MAT 102 - Discrete Mathematics

Claudiu C. Remsing

*Mathematics is not about calculations but about ideas. [...] Calculations are merely a means to an end. [...] Not all ideas are mathematics; but all good mathematics must contain an idea. [...] There are [...] at least five distinct sources of mathematical ideas. They are **number**, **shape**, **arrangement**, **movement**, and **chance**. [...] The driving force of mathematics is **problems**. [...] Another important source of mathematical inspiration is **examples**.*

<div align="right">

IAN STEWART

</div>

It is not easy to say what mathematics is, but "I know it when I see it" is the most likely response of anyone to whom this question is put. The most striking thing about mathematics is that it is very different to science, and this compounds the problem of why it should be found so useful in describing and predicting how the Universe works. Whereas science is like a long text that is constantly being redrafted, updated, and edited, mathematics is entirely cumulative. Contemporary science is going to be proven wrong, but mathematics is not. The scientists of the past were well justified in holding naïve and erroneous views about physical phenomena in the context of the civilizations in which they lived, but there can never be any justification for establishing erroneous mathematical results. The mechanics of ARISTOTEL is wrong, but the geometry of EUCLID is, was, and always will be correct. Right and wrong mean different things in science and mathematics. In the former, "right" means correspondence with reality; in mathematics it means logical consistency.

<div align="right">

JOHN D. BARROW

</div>

Mathematics is a way of representing and explaining the Universe in a symbolic way.

<div align="right">John D. Barrow</div>

Mathematics may be defined as the subject in which we never know what are we talking about, nor whether what we are saying is true.

<div align="right">Bertrand Russell</div>

What is mathematics, anyway ?

In a broad sense, mathematics include all the related areas which touch on *quantitative, geometric*, and *logical themes.* This includes Statistics, Computer Science, Logic, Applied Mathematics, and other fields which are frequently considered distinct from mathematics, as well as fields which study the study of mathematics (!) – History of Mathematics, Mathematics Education, and so on. We draw the line only at experimental sciences, philosophy, and computer applications. Personal perspectives vary widely, of course. Probably the only absolute definition of mathematics is : *that which mathematicians do.*

Contrary to common perception, mathematics does not consists of "crunching numbers" or "solving equations". There are branches of mathematics concerned with *setting up* equations, or *analyze* their solutions, and there are

parts of mathematics devoted to *creating methods* for doing computations. But there are also parts of mathematics which have nothing at all to do with numbers and equations.

The current mathematics literature can be divided, roughly, into two parts : *"pure" mathematics* (i.e. mathematics for mathematics) and *"applied" mathematics* (i.e. mathematics for something else).
The first group divides roughly into just a few broad overlapping areas :

- **Foundations** : considers questions in logic or set theory – the very language of mathematics.

- **Algebra** : is principally concerned with symmetry, patterns, discrete sets, and the rules for manipulating arithmetic operations (one might think of this as the outgrowth of arithmetic and algebra classes in primary and secondary school).

- **Geometry** : is concerned with shapes and sets, and the properties of them which are preserved under various kinds of transformations (this is related to elementary geometry and analytic geometry).

- **Analysis** : studies functions, the real number line, and the ideas of continuity and limit (this is the natural succesor to courses in graphing, trigonometry, and calculus).

The second broad part of mathematics literature includes those areas which could be considered either independent disciplines or central parts of mathematics, as well as areas which clearly use mathematics but are interested in non-mathematical ideas too :

- **Probability and Statistics** : has a dual nature – mathematical and experimental.

- **Computer Sciences** : consider algorithms and information handling.

- **Application to Sciences** : significant mathematics must be developed to formulate ideas in the **physical sciences** (e.g. mechanics, optics, electromagnetism, relativity, astronomy, etc.), **engineering** (e.g. control, robotics, etc.), and other branches of **science** (e.g. biology, economics, social sciences).

The division between mathematics and its applications is of course vague.

Contents

Chapter 1

Propositions and Predicates

Topics :

1. PROPOSITIONS AND CONNECTIVES

2. PROPOSITIONAL EQUIVALENCES

3. PREDICATES AND QUANTIFIERS

Logic is the basis of all mathematical reasoning. The rules of logic specify the precise meaning of mathematical statements. Most of the definitions of formal logic have been developed so that they agree with the natural or intuitive logic used by people who have been educated to think clearly and use language carefully. The difference that exists between formal and intuitive logic are necessary to avoid ambiguity and obtain consistency.

1.1 Propositions and connectives

In any *mathematical theory*, new terms are defined by using those that have been previously defined. However, this process has to start somewhere. A few initial terms necessarily remain *undefined*. In logic, the words **sentence, true,** and **false** are initial undefined terms.

Propositions

1.1.1 Definition.   A **proposition** (or **statement**) is a sentence that is either TRUE or FALSE (but *not* both).

1.1.2 Examples.   All the following sentences are propositions.

   (1)   Pretoria is the capital of South Africa.

   (2) $3 + 3 = 5$.

   (3)   If x is a real number, then $x^2 < 0$. (FALSE)

   (4)   All kings of the United States are bald. (TRUE)

   (5)   There is intelligent life outside our solar system.

1.1.3 Examples.   The following are *not* propositions.

   (6)   Is this concept important ?

   (7)   Wow, what a day !

   (8) $x + 1 = 7$.

   (9)   When the swallows return to Capistrano.

  (10)   This sentence is false.

A proposition ends in a period, not a question mark or an exclamation point. Thus (6) and (7) are *not* propositions. (8) is *not* a proposition, even though it has the proper *form*, until the variable x is replaced by meaningful terms. Because (9) *makes no sense*, it cannot be TRUE or FALSE.

Sentence (10) is deceiving; it looks like a proposition. If it is a proposition, then it is either TRUE or FALSE, but not both. Suppose it is TRUE. Then what it says is TRUE, and it is FALSE. But it cannot be both TRUE and FALSE. Hence (10) cannot be TRUE. Well, suppose (10) is FALSE. Then what it says is FALSE, and (10) is not FALSE, it is TRUE. Again, it cannot be both TRUE and FALSE. Therefore, (10) *cannot be classified* as either TRUE or FALSE. Hence it is not a proposition.

We will use lower case letters, such as $p, q, r, s, \ldots$ to denote propositions. Any proposition symbolized by a single letter is called a **primitive proposition**. If p is a (primitive) proposition we define its **truth value** by

$$\tau(p) := \begin{cases} 1 & \text{if } p \text{ is TRUE} \\ 0 & \text{if } p \text{ is FALSE.} \end{cases}$$

Thus the symbol 1 stands for TRUE and the symbol 0 for FALSE.

Logical operators

New propositions, called **compound propositions**, may be constructed from existing propositions using **logical operators** (or **connectives**). We define here five such connectives : $\neg$, $\wedge$, $\vee$, $\rightarrow$, and $\leftrightarrow$. Three more connectives – $\oplus$, $\downarrow$, and $\mid$ – are defined in the exercises.

1.1.4 DEFINITION. Let p be a proposition. The proposition "not p", denoted by $\neg p$, is TRUE when p is FALSE and is FALSE when p is TRUE. The proposition $\neg p$ is called the **negation** of p.

We use a **truth table** to display the relationship between the truth values.

NOT	
p	$\neg p$
1	0
0	1

1.1.5 EXAMPLE.   Find the negation of the proposition "Today is Monday".

SOLUTION : The negation is "Today is not Monday".

1.1.6 DEFINITION.   Let p and q be propositions. The proposition "p and q",
denoted by $p \wedge q$, is TRUE when both p and q are TRUE, and is FALSE oth-
erwise. The proposition $p \wedge q$ is called the **conjunction** of p and q.

We can use a truth table to illustrate how conjunction works.

AND		
p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

1.1.7 EXAMPLE.   Find the conjunction of the propositions p and q, where
p is the proposition "Today is Sunday" and q is the proposition "The moon
is made of cheese".

SOLUTION : The conjunction of these propositions is the proposition "Today
is Sunday and the moon is made of cheese". This proposition is always FALSE.

1.1.8 DEFINITION.   Let p and q be propositions. The proposition "p or q",
denoted by $p \vee q$, is the proposition that is FALSE when p and q are FALSE,

and is TRUE otherwise. The proposition $p \vee q$ is called the **disjunction** of p and q.

We can again use a truth table to illustrate how disjunction works.

OR		
p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

1.1.9 EXAMPLE.   Find the disjunction of the propositions p and q, where p is the proposition "Today is Sunday" and q is the proposition "The moon is made of cheese".

SOLUTION : The disjunction of these propositions is the proposition "Today is Sunday or the moon is made of cheese". This proposition is TRUE only on Sundays.

1.1.10 DEFINITION.   Let p and q be propositions. The proposition "p implies q", denoted by $p \rightarrow q$, is FALSE when p is TRUE and q is FALSE, and is TRUE otherwise. The proposition $p \rightarrow q$ is called an **implication** (or **conditional**). In this implication p is called the **antecedent** (or **hypothesis**), whereas q is called the **consequent** (or **consequence**).

A truth table for the conditional is :

IMPLIES		
p	q	$p \rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

1.1.11 EXAMPLE.   Consider the propositions

(1) p : 7 is a positive integer.

(2) q : $2 < 3$.

(3) r : 5 is an even integer.

(4) s : No one will pass this course.

Then the conditional propositions $p \rightarrow q$, $r \rightarrow q$, $r \rightarrow s$ are all TRUE.

NOTE :   The proposition $r \rightarrow s$ is TRUE since the hypothesis is FALSE. Even though this proposition is TRUE, it does not say that no one will pass this course.

It is worth noting certain synonyms for $p \rightarrow q$ which occur in mathematical literature. They are as follows :

- "if p, then q"

- "p, only if q"

- "p is sufficient for q"

- "q is implied by p"

- "q, if p"

- "q, whenever p"

- "q is necessary for p".

NOTE : (1) The mathematical concept of an implication is independent of a cause-and-effect relationship between antecedent and consequent.

(2) The if-then construction used in many programming languages is different from that in logic. Most programming languages contain statements such as "if p then S", where p is a proposition and S is a program segment (one or more statements to be executed). When execution of a program encounters such a statement, S is executed if p is TRUE, whereas S is not executed if p is FALSE.

There are some related implications that can be formed from $p \to q$. We call

- $q \to p$ the **converse**

- $\neg q \to \neg p$ the **contrapositive**

- $\neg p \to \neg q$ the **inverse**

of the implication $p \to q$.

1.1.12 EXAMPLE. Find the converse, the contrapositive, and the inverse of the implication "If today is Friday, then I will party tonight."

SOLUTION : The converse is "If I will party tonight, then today is Friday." The contrapositive of this implication is "If I will not party tonight, then today is not Friday." And the inverse is "If today is not Friday, then I will not party tonight."

Observe that the given implication and its contrapositive are either both TRUE or both FALSE.

NOTE : When one says "If it rains, then I will stay home" the meaning usually includes the inverse statement "If it does not rain, then I will not stay home". This is *not* the case in an implication. As an implication, this statement gives absolutely no information for the case when it does not rain.

1.1.13 DEFINITION.   Let p and q be propositions. The proposition "p if and only if q", denoted by $p \leftrightarrow q$, is the proposition that is TRUE when p and q have the same truth values, and is FALSE otherwise. The proposition $p \leftrightarrow q$ is called an **equivalence** (or **biconditional**).

The truth table for the biconditional is :

IF AND ONLY IF		
p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

The biconditional is the conjunction of two conditional propositions (see the appropriate logical equivalence from the list on page 11). This leads to the terminology "if and only if". Other ways of expressing this connective are

- "if p, then q and conversely"

- "p is necessary and sufficient for q".

1.1.14 EXAMPLE.   Find the truth value of the biconditional "The moon is made of cheese if and only if 1=2".

SOLUTION : The proposition is TRUE, since it is composed of two propositions each of which is FALSE.

NOTE :   (Remark on punctuation) For symbolized statements, punctuation is accomplished by using parentheses. To lessen the use of parentheses, we agree that in the absence of parentheses the logical operator NOT takes precedence over AND and OR, and the logical operators AND and OR take precedence over the conditional (IMPLIES) and biconditional (IF AND ONLY IF). Thus

- $\neg p \wedge q$ stands for $(\neg p) \wedge q$, not for $\neg(p \wedge q)$.

- $\neg p \rightarrow q$ stands for $(\neg p) \rightarrow q$, not for $\neg (p \rightarrow q)$.

- $\neg p \vee \neg q$ stands for $(\neg p) \vee (\neg q)$, not for $\neg (p \vee (\neg q))$.

- $p \wedge q \rightarrow r$ stands for $(p \wedge q) \rightarrow r$, not for $p \wedge (q \rightarrow r)$.

- $\neg p \vee q \rightarrow r \wedge q$ stands for $((\neg p) \vee q) \rightarrow (r \wedge q)$.

- $\neg p \leftrightarrow p \rightarrow q \wedge r$ stands for $(\neg p) \leftrightarrow (p \rightarrow (q \wedge r))$.

A basic principle of (propositional) logic is that *the truth values of a proposition composed of other propositions and the connectives* $\neg, \wedge, \vee, \rightarrow,$ *and* $\leftrightarrow$ *are determined by the truth values of the constituent propositions and by the way in which those propositions are combined with the connectives.*

1.1.15 EXAMPLE. Construct the truth table for the proposition $(\neg p \rightarrow q) \wedge r$.

SOLUTION : The truth table is

p	q	r	$\neg p \rightarrow q$	$(\neg p \rightarrow q) \wedge r$
1	1	1	1	1
1	1	0	1	0
1	0	1	1	1
1	0	0	1	0
0	1	1	1	1
0	1	0	1	0
0	0	1	0	0
0	0	0	0	0

It is often desirable that we translate English (or any other human language) sentences into expressions involving propositional variables and logical connectives in order to remove the ambiguity.

NOTE : This may involve making certain reasonable assumptions based on the intended meaning of the sentence.

Once we have translated sentences from English into logical expressions we can analyze them (i.e. determine their truth values), as well as manipulate and reason about them.

1.1.16 EXAMPLE.   Let p, q, and r be the propositions

  p : You get an A on the final exam.

  q : You do every prescribed exercise.

  r : You get an A in this class.

Write the following propositions using p, q, and r and logical operators.

(1)   You get an A on the final, but you don't do every prescribed exercise; nevertheless, you get an A in this class.

(2)   Getting an A on the final and doing every prescribed exercise is sufficient for getting an A in this class.

SOLUTION :   The answer is : $p \wedge \neg q \wedge r$ and $p \wedge q \rightarrow r$.

1.2   Propositional equivalences

Methods that produce propositions with the same truth value as a given compound proposition are used extensively in the construction of mathematical arguments.

1.2.1 DEFINITION.   A compound proposition that is always TRUE, no matter what the truth values of the propositions that occur in it, is called a **tautology**.

1.2.2 EXAMPLES.   All the following propositions are tautologies.

(1) $p \vee \neg p$.

(2) $p \rightarrow p \vee q$.

(3) $p \wedge (p \rightarrow q) \rightarrow q.$

In each case, the truth value of the compound proposition is 1 for every one of the lines in the truth table. For example, the truth table for the proposition $p \wedge (p \rightarrow q) \rightarrow q$ is :

p	q	$p \wedge (p \rightarrow q)$	$p \wedge (p \rightarrow q) \rightarrow q$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	1

1.2.3 DEFINITION.   A compound proposition that is always FALSE, no matter what the truth values of the propositions that occur in it, is called a **contradiction**.

1.2.4 EXAMPLES.   All the following propositions are contradictions.

(1) $p \wedge \neg p.$

(2) $p \wedge \neg (p \vee q).$

(3) $(p \rightarrow q) \wedge (p \wedge \neg q).$

1.2.5 DEFINITION.   The propositions p and q are called **logically equivalent**, denoted $p \iff q$, provided $p \leftrightarrow q$ is a tautology.

In other words, two compound propositions are logically equivalent provided that they have the same truth values for all possible assignments of truth values to the constituent propositions. Thus *all tautologies are logically equivalent, as are all contradictions.*

NOTE :   Although one proposition may be easier to read than the other, insofar as the truth values of any propositions which depend on one or the other of the two propositions, it makes no difference which of the two is used. Logical equivalence may allow us to replace a complex proposition with a much simpler one.

1.2.6 EXAMPLE.   Show that the propositions $\neg(p \wedge q)$ and $\neg p \vee \neg q$ are logically equivalent.

SOLUTION : We construct the truth table for these propositions.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

Since the truth values of $\neg(p \wedge q)$ and $\neg p \vee \neg q$ agree, these propositions are logically equivalent.

NOTE :   It is important to understand the difference between $\leftrightarrow$ and $\iff$. $p \leftrightarrow q$ is a statement which may or may not be TRUE. In other words, the truth value of $\tau(p \leftrightarrow q)$ may be 1 or 0. But $p \iff q$ is a statement about the statement (proposition) $p \leftrightarrow q$: it says that "$p \leftrightarrow q$ is always TRUE".

1.2.7 DEFINITION.   Let p and q be propositions. We say that p **logically implies** q, denoted $p \Rightarrow q$, provided $p \rightarrow q$ is a tautology.

In other words, q is true whenever p is TRUE. For example, we have seen that

$$p \wedge (p \rightarrow q) \rightarrow q \quad \text{is a tautology}$$

and so

$$p \wedge (p \rightarrow q) \Rightarrow q.$$

NOTE :   (1)   Again, we emphasize the difference between $\rightarrow$ and $\Rightarrow$. $p \rightarrow q$ is is just a proposition, whereas $p \Rightarrow q$ is a statement about the statement (proposition) $p \rightarrow q$: it says that "$p \rightarrow q$ is always TRUE".

(2)   Also, we note that, in order to show that $p \Rightarrow q$ it is sufficient to show that $p \rightarrow q$ is never FALSE. For example, to show that

$$p \wedge q \Rightarrow p$$

we need only show that we cannot have $\tau(p \wedge q) = 1$ and $\tau(p) = 0$. This is immediate since if $\tau(p \wedge q) = 1$ then $\tau(p) = 1$.

We list some important logical equivalences and logical implications. In this, we let $\mathbf{T}$ denote any tautology and we let $\mathbf{C}$ denote any contradiction.

(1) $p \wedge \mathbf{T} \iff p$ (identity) ;

(2) $p \vee \mathbf{C} \iff p$ (identity) ;

(3) $p \wedge \mathbf{C} \iff \mathbf{C}$ (domination) ;

(4) $p \vee \mathbf{T} \iff \mathbf{T}$ (domination) ;

(5) $\neg\neg p \iff p$ (double negation) ;

(6) $p \wedge p \iff p$ (idempotency) ;

(7) $p \vee p \iff p$ (idempotency) ;

(8) $p \wedge q \iff q \wedge p$ (commutativity) ;

(9) $p \vee q \iff q \vee p$ (commutativity) ;

(10) $p \wedge (q \wedge r) \iff (p \wedge q) \wedge r$ (associativity) ;

(11) $p \vee (q \vee r) \iff (p \vee q) \vee r$ (associativity) ;

(12) $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$ (distributivity) ;

(13) $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$ (distributivity) ;

(14) $\neg(p \wedge q) \iff \neg p \vee \neg q$ (De Morgan's law) ;

(15) $\neg(p \vee q) \iff \neg p \wedge \neg q$ (De Morgan's law) ;

(16) $p \to q \iff \neg p \vee q$ (OR form of a conditional) ;

(17) $\neg(p \to q) \iff p \wedge \neg q$ (negation of a conditional) ;

(18) $p \to q \iff \neg q \to \neg p$ (contraposition) ;

(19) $p \leftrightarrow q \iff (p \to q) \wedge (q \to p)$ (biconditional) ;

(20) $p \Rightarrow p \vee q$ (addition) ;

(21)　$p \wedge q \Rightarrow p$　(simplification) ;

(22)　$p \wedge (p \to q) \Rightarrow q$　(detachment) ;

(23)　$\neg p \wedge (p \vee q) \Rightarrow q$　(disjunction) ;

(24)　$(p \to q) \wedge (q \to r) \Rightarrow p \to r$　(syllogism).

The logical equivalences above, as well as any others (like $p \wedge \neg p \iff \mathbf{C}$ or $p \vee \neg p \iff \mathbf{T}$), can be used to construct additional logical equivalences. The reason for this is that *a proposition in a compound proposition can be replaced by one that is logically equivalent to it without changing the truth value of the compound proposition.*

1.2.8 EXAMPLE.　　Show that the propositions $p \wedge q \to r$ and $p \to (q \to r)$ are logically equivalent.

SOLUTION : To show these compound propositions are logically equivalent, we will developing a sequence of logical equivalences starting with $p \wedge q \to r$ and ending with $p \to (q \to r)$. We have

$$p \wedge q \to r \iff \neg(p \wedge q) \vee r \iff (\neg p \vee \neg q) \vee r \iff$$
$$\neg p \vee (\neg q \vee r) \iff \neg p \vee (q \to r) \iff p \to (q \to r).$$

1.2.9 EXAMPLE.　　Show that the proposition $\neg(p \to q) \to p$ is a tautology.

SOLUTION : To show this proposition is a tautology, we will use logical equivalences to demonstrate that it is logically equivalent to $\mathbf{T}$. We have

$$\neg(p \to q) \to p \iff (p \wedge \neg q) \to p \iff \neg(p \wedge \neg q) \vee p \iff$$
$$(\neg p \vee q) \vee p \iff (\neg p \vee p) \vee q \iff \mathbf{T} \vee q \iff \mathbf{T}.$$

1.3　Predicates and quantifiers

Propositions are sentences that are either TRUE or FALSE (but *not* both). The sentence "He is a student at Rhodes University" is not a proposition because it may be either true or false depending on the value of the pronoun

he. Similarly, the sentence "$x + y > 0$" is not a proposition because its truth value depends on the values of the *variables* x and y.

NOTE : In grammar, the word *predicate* refers to the part of a sentence that gives information about the subject. In the sentence "James is a student at Rhodes University", the word *James* is the subject and the phrase "is a student at Rhodes University" is the predicate.

In logic, predicates can be obtain by removing some or all nouns from a statement. For instance, the sentences "x is a student at Rhodes University" and "x is a student at y" are predicates ; here x and y are *predicate variables* that take values in appropriate sets.

Predicates

We make the following definition.

1.3.1 DEFINITION. A sentence that contains a finite number of variables and becomes a proposition when specific values are substituted for the variables is called a **predicate** (or **open sentence**).

Predicates are sometimes referred to as **propositional functions**.

1.3.2 EXAMPLES. The following are all predicates.

(1) $x + 3 = 4$.

(2) The sum of the first n odd integers is n^2.

(3) $x > 2$.

(4) If $x < y$, then $x^2 < y^2$.

(5) $x + y = z$.

(6) x is the capital of France.

We generally denote predicates by capital letters such as $P, Q, R, \ldots$, and following the name of the predicate we list in parentheses the variables which are used by the predicate. Thus in the example above we might describe the predicates as $P(x), Q(n), R(x), S(x,y), T(x,y,z), U(x)$.

NOTE : The predicate $S(x,y)$: "If $x < y$, then $x^2 < y^2$" is actually a *compound predicate*, consisting of predicates which are combined by the same kind of logical connectives that are used in propositional logic. This means that we can write $S(x,y)$ as $A(x,y) \rightarrow B(x,y)$, where $A(x,y)$ is the predicate "$x < y$" and $B(x,y)$ is the predicate "$x^2 < y^2$".

1.3.3 EXAMPLE. Consider the predicate

$$P(x,y) : \quad \text{"} y = x + 3 \text{"}.$$

What are the truth values of the propositions $P(1,2)$ and $P(0,3)$?

SOLUTION : $P(1,2)$ is the proposition "$2 = 1 + 3$" which is false. The statement $P(0,3)$ is the proposition "$3 = 0 + 3$" which is true.

When all the variables in a predicate are assigned values, the resulting sentence is a proposition. The set of all values that may be substituted in place of a variable constitutes the **universe of discourse**. If $P(x)$ is a predicate, where the universe of discourse is $\mathcal{U}$, the **truth set** of $P(x)$ is the set of all elements in $\mathcal{U}$ that make $P(x)$ true when substituted for x.

However, there is another important way to change predicates into propositions, namely **quantification**.

Quantifiers

1.3.4 DEFINITION. The proposition "$P(x)$ is true for all values of x belonging to the universe of discourse $\mathcal{U}$", denoted $\forall x\, P(x)$ ($x \in \mathcal{U}$), is called the **universal quantification** of the predicate $P(x)$.

The proposition $\forall x\, P(x)$ (or $\forall x \in \mathcal{U},\ P(x)$) is also expressed as

- "For all x (in $\mathcal{U}$) $P(x)$".

- "For every x (in $\mathcal{U}$) $P(x)$".

1.3.5 EXAMPLE. Express the statement "Every student in this class has seen a computer" as a universal quantification.

SOLUTION : Let $Q(x)$ be the predicate "x has seen a computer". Then the statement "Every student in this class has seen a computer" can be written as $\forall x\, Q(x)$, where the universe of discourse consists of all students in this class. Also, this statement can be expressed as $\forall x\, (P(x) \to Q(x))$, where $P(x)$ is the predicate "x is in this class" and the universe of discourse consists of all students.

NOTE : There is often more than one good way to express a quantification.

1.3.6 EXAMPLE. Let $P(x)$ be the predicate "$x^2 > x$". What is the truth value of the universal quantification $\forall x\, P(x)$, where the universe of discourse is the set of real numbers ?

SOLUTION : $P(x)$ is not true for all real numbers x; for instance, $P(\frac{1}{2})$ is false. Thus, the proposition $\forall x\, P(x)$ is false.

When all the elements of the universe of discourse can be listed, say $x_1, x_2, \ldots, x_n$, it follows that the universal quantification $\forall x\, P(x)$ is the same as the conjunction

$$P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n).$$

1.3.7 EXAMPLE. What is the truth value of the proposition "$\forall x\, P(x)$", where $P(x)$ is the predicate "$x^{10} < 50\,000$", and the universe of discourse consists of the positive integers not exceeding 3 ?

SOLUTION : The proposition $\forall x\, P(x)$ is the same as the conjunction

$$P(1) \wedge P(2) \wedge P(3).$$

Since the proposition $P(3)$: "$3^{10} < 50\,000$" is false, it follows that the universal quantification $\forall x \, P(x)$ is false.

Statements such as "there exists an x in U such that $P(x)$" are also common.

1.3.8 DEFINITION.   The proposition "There exists an x in the universe of discourse $\mathcal{U}$ such that $P(x)$ is TRUE", denoted $\exists x \, P(x)$ ($x \in \mathcal{U}$), is called the **existential quantification** of the predicate $P(x)$.

The proposition $\exists x \, P(x)$ (or $\exists x \in \mathcal{U}, \, P(x)$) is also expressed as

- "There exists at least one x (in $\mathcal{U}$) such that $P(x)$".

- "For some x (in $\mathcal{U}$) $P(x)$".

1.3.9 EXAMPLE.   Let $Q(n)$ be the predicate "$n^2 + n + 1$ is a prime number". What is the truth value of the existential quantification $\exists n \, Q(n)$, where the universe of discourse is the set of positive integers ?

SOLUTION : Since the proposition $Q(1)$: "3 is a prime number" is TRUE, it follows that the existential quantification $\exists n \, Q(n)$ is TRUE.

When all the elements in the universe of discourse can be listed, say $x_1, x_2, \ldots, x_n$, the existential quantification $\exists x \, P(x)$ is the same as the disjunction

$$P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n).$$

1.3.10 EXAMPLE.   What is the truth value of the proposition $\exists x \, P(x)$, where $P(x)$ is the predicate "$x^3 = 15x + 4$", and the universe of discourse consists of all positive integers not exeeding 4 ?

SOLUTION : The proposition $\exists x \, P(x)$ is the same as the disjunction

$$P(1) \vee P(2) \vee P(3) \vee P(4).$$

Since the proposition $P(4)$: "$4^3 = 60 + 4$" is TRUE, it follows that the existential quantification $\exists x \, P(x)$ is TRUE.

1.3.11 EXAMPLE.   Rewrite the formal statement

$$\forall x \in \mathbb{R}, \ x^2 \geq 0$$

in several equivalent but more informal ways. Do not use the symbol (universal quantifier) $\forall$.

SOLUTION :

All real numbers have nonnegative squares.

Every real number has a nonnegative square.

Any real number has a nonnegative suare.

x has a nonnegative square, for each real number x.

The square of any real number is nonnegative.

1.3.12 EXAMPLE.   Rewrite the statement "No dogs have wings" formally. Use quantifiers and variables.

SOLUTION :

$\forall$ dogs d, d does not have wings.

$\forall d \in D$, d does not have wings (where D is the set of dogs).

$\forall d \ P(d)$, where D is the set of dogs and $P(d)$ is the predicate " d does not have wings".

$\forall d \ \neg Q(d)$, where D is the set of dogs and $Q(d)$ is the predicate " d has wings".

Many mathematical statements involve multiple quantifications of predicates involving more than one variable. It is important to note that *the order of the quantifiers is important, unless all the quantifiers are universal quantifiers or all are existential quantifiers.*

1.3.13 EXAMPLE.   Express the statement "If somebody is female and is a parent, then this person is someone's mother" formally. Use quantifiers and variables.

SOLUTION :   Consider the predicates

$F(x)$: "x is female".

$P(x)$: "x is parent".

$M(x,y)$: "x is the mother of y".

Here, the universe of discourse can be taken to be the set of all people. We can write the statement symbolically as

$$\forall x \, (F(x) \wedge P(x) \to \exists y \, M(x,y)).$$

1.3.14 EXAMPLE.   Let $P(x,y)$ be the predicate "$x+y=3$". What are the truth values of the quantifications

$$\forall x \forall y \, P(x,y), \quad \forall x \exists y \, P(x,y), \quad \exists x \forall y \, P(x,y) \quad \text{and} \quad \exists x \exists y \, P(x,y) \, ?$$

SOLUTION : The quantification $\forall x \forall y \, P(x,y)$ denotes the proposition "For every pair $x,y \, P(x,y)$ is TRUE". Clearly, this proposition is FALSE.

The quantification $\forall x \exists y \, P(x,y)$ denotes the proposition "For every x there is an y such that $P(x,y)$ is TRUE". Given a real number x, there is a real number y such that $x+y=3$, namely $y=3-x$. Hence, the proposition $\forall x \exists y \, P(x,y)$ is TRUE.

We can see that $\exists x \forall y \, P(x,y)$ is FALSE and $\exists x \exists y \, P(x,y)$ is TRUE.

NOTE :   The order in which quantifiers appear makes a difference. For instance, the propositions $\exists x \forall y \, P(x,y)$ and $\forall y \exists x \, P(x,y)$ are *not* logically equivalent. However,

$$\exists x \forall y \, P(x,y) \; \Rightarrow \; \forall y \exists x \, P(x,y).$$

We will often want to consider the negation of a quantification. In this regard, the following logical equivalences are useful.

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

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

(3) $\neg \forall x \forall y\, P(x,y) \iff \exists x \exists y\, \neg P(x,y)$;

(4) $\neg \forall x \exists y\, P(x,y) \iff \exists x \forall y\, \neg P(x,y)$;

(5) $\neg \exists x \forall y\, P(x,y) \iff \forall x \exists y\, \neg P(x,y)$;

(6) $\neg \exists x \exists y\, P(x,y) \iff \forall x \forall y\, \neg P(x,y)$.

1.3.15 EXAMPLE.   Express the negations of the following propositions using quantifiers. Also, express these negations in English.

(1) "Every student in this class likes mathematics".

(2) "There is a student in this class who has been in at least one room of every building on campus".

SOLUTION :   (1)   Let $L(x)$ be the predicate "x likes mathematics", where the universe of discourse is the set of students in this class. The original statement is $\forall x\, L(x)$ and its negation is $\exists x\, \neg L(x)$. In English, it reads "Some student in this class does not like mathematics".

  (2)   Consider the predicates $P(z,y)$: "room z is in building y" and $Q(x,z)$: "student x has been in room z". Then the original statement is

$$\exists x\, \forall y\, \exists z\, (P(z,y) \wedge Q(x,z)) \,.$$

To form the negation, we change all the quantifiers and put the negation on the inside, then apply De Morgan's law. The negation is therefore

$$\forall x\, \exists y\, \forall z\, (\neg P(z,y) \vee \neg Q(x,z)) \,,$$

which is also equivalent to

$$\forall x\, \exists y\, \forall z\, (P(z,y) \rightarrow \neg Q(x,z)).$$

In English, this could be read "For every student there is a building on the campus such that for every room in that building, the student has not been in that room".

1.3.16 EXAMPLE.   Rewrite the statement "No politicians are honest" formally. Then write formal and informal negations.

SOLUTION :

> *formal version* : $\forall$ politicians x, x is not honest.
>
> *formal negation* : $\exists$ a politician x such that x is honest.
>
> *informal negation* :   "Some politicians are honest".

1.3.17 EXAMPLE.   Write informal negations for each of the following statements:

(1) "All computer programs are finite".

(2) "Some computer hackers are over 40".

(3) "Every polynomial function is continuous".

SOLUTION :   The informal negations are :

(1) "Some computer programs are not finite".

(2) "No computer hackers are over 40" (or "All computer hackers are 40 or under").

(3) "There is a non-continuous polynomial function".

1.4   Exercises

Exercise 1 TRUE or FALSE? The negation of "If Tom is Ann's father, then Jim is her uncle and Sue is her aunt" is "If Tom is Ann's father, then either Jim is not her uncle or Sue is not her aunt".

Exercise 2 Assume that "Joe is a girl" is a FALSE proposition and that "Mary is ten years old" is a TRUE proposition. Which of the following are TRUE ?

> (a) Joe is a girl and Mary is ten years old.

(b) Joe is a girl or Mary is ten years old.

(c) If Joe is a girl, then Mary is ten years old.

(d) If Mary is ten years old, then Joe is a girl.

(e) Joe is a girl if and only if Mary is ten years old.

Exercise 3 Suppose that p and q are propositions so that $p \rightarrow q$ is FALSE. Find the truth value of the following propositions.

(a) $\neg p \rightarrow q$.

(b) $p \vee q$.

(c) $q \rightarrow p$.

Exercise 4 Construct truth tables for each of the following propositions.

(a) $p \wedge \neg p$.

(b) $p \vee \neg p$.

(c) $p \wedge q \rightarrow p$.

(d) $p \rightarrow p \vee q$.

(e) $p \vee q \rightarrow p \wedge q$.

(f) $(p \rightarrow q) \rightarrow (q \rightarrow p)$.

(g) $p \wedge (p \rightarrow q) \rightarrow q$.

(h) $(p \rightarrow q) \vee (\neg p \rightarrow r)$.

(i) $(p \vee q) \wedge r \rightarrow \neg p \vee q$.

(j) $\neg p \wedge \neg q \vee (r \rightarrow q)$.

Exercise 5 Let p and q be propositions. The proposition "p exclusive or q", denoted by $p \oplus q$, is the proposition that is TRUE when exactly one of p and q is TRUE, and is FALSE otherwise. Construct the truth table for this logical operator (XOR), and then show that

$$\tau(p \oplus q) = \tau((p \wedge \neg q) \vee (\neg p \wedge q)).$$

Exercise 6 Verify that each of the following propositions is a tautology.

(a) $p \wedge q \rightarrow p$.

(b) $p \to p \lor q$.

(c) $\neg p \to (p \to q)$.

(d) $p \land q \to (p \to q)$.

(e) $p \land (p \to q) \to q$.

(f) $(p \to q) \to (p \lor r \to q \lor r)$.

Exercise 7 Verify each of the following logical equivalences.

(a) $p \land r \to q \iff p \to (r \to q)$.

(b) $p \lor q \to r \iff (p \to r) \land (q \to r)$.

(c) $\neg(p \oplus q) \iff p \leftrightarrow q$.

(d) $\neg(p \leftrightarrow q) \iff \neg p \leftrightarrow q$.

Exercise 8 Show that $(p \to q) \to r$ and $p \to (q \to r)$ are *not* logically equivalent.

Exercise 9 Which of the following expressions are logically equivalent to $p \to q$?

(a) $p \to q$.

(b) $p \lor q$.

(c) $\neg q \to \neg p$.

(d) $\neg q \to p$.

(e) $\neg p \land q$.

(f) $p \land \neg q$.

(g) $\neg p \to q$.

(h) $p \land q$.

(i) $p \lor \neg q$.

(j) $\neg p \to \neg q$.

(k) $\neg p \lor q$.

(l) $q \to p$.

Exercise 10 Suppose that "John is smart", "John or Mary is ten years old", and "If Mary is ten years old, then John is not smart" are each TRUE propositions. Which of the following propositions are TRUE ?

    (a) John is not smart.

    (b) Mary is ten years old.

    (c) John is ten years old.

    (d) Either John or Mary is not ten years old.

Exercise 11 Let p and q be propositions. The proposition "p NOR q", denoted by $p \downarrow q$, is TRUE when both p and q are FALSE, and it is FALSE otherwise.

    (a) Construct the truth table for the logical operator $\downarrow$ (also known as the **Peirce arrow**).

    (b) Show that :

        i. $p \downarrow q \iff \neg(p \vee q)$.

        ii. $p \downarrow p \iff \neg p$.

        iii. $(p \downarrow q) \downarrow (p \downarrow q) \iff p \vee q$.

        iv. $(p \downarrow p) \downarrow (q \downarrow q) \iff p \wedge q$.

Exercise 12 Let p and q be propositions. The proposition "p NAND q", denoted by $p \mid q$, is TRUE when either p and q, or both, are FALSE, and is FALSE when both p and q are TRUE.

    (a) Construct the truth table for the logical operator $\mid$ (also known as the **Scheffer stroke**).

    (b) Show that :

        i. $p \mid q \iff \neg(p \wedge q)$.

        ii. $p \mid p \iff \neg p$.

        iii. $(p \mid p) \mid (q \mid q) \iff p \vee q$.

        iv. $(p \mid q) \mid (p \mid q) \iff p \wedge q$.

Exercise 13 Let $F(x, y)$ be the predicate "x can fool y", where the universe of discourse is the set of all people in the world. Use quantifiers to express each of the following statements.

    (a) Everybody can fool Bob.

    (b) Kate can fool everybody.

    (c) Everybody can fool somebody.

(d) There is no one who can fool everybody.

(e) Everyone can be fooled by somebody.

(f) No one can fool Fred and Jerry.

(g) No one can fool himself or herself.

Exercise 14 Let $P(x, y)$ be the predicate "$x + y = x - y$". If the universe of discourse is the set of integers, what are the truth values of the following propositions?

(a) $P(1, 1)$.

(b) $P(2, 0)$.

(c) $\forall y\, P(1, y)$.

(d) $\exists x\, P(x, 2)$.

(e) $\exists x \exists y\, P(x, y)$.

(f) $\forall x \exists y\, P(x, y)$.

(g) $\exists y \forall x\, P(x, y)$.

(h) $\forall x \forall y\, P(x, y)$.

(i) $\forall y \exists x\, P(x, y)$.

Exercise 15 Write the negation for each of the following propositions. Determine whether the resulting proposition is TRUE or FALSE; let $\mathcal{U} = \mathbb{R}$.

(a) $\forall x\, (x^2 + 2x - 3 = 0)$.

(b) $\exists x\, (x^2 - 2x + 5 \leq 0)$.

(c) $\forall x\, \exists r\, (xr = 1)$.

(d) $\forall x \exists m\, (x^2 < m)$.

(e) $\exists m \forall x\, (x^2 < m)$.

(f) $\exists m \forall x\, \left(\frac{x}{|x|+1} < m \right)$.

(g) $\forall x\, \forall y\, (x^2 + y^2 \geq xy)$.

Chapter 2

Sets and Numbers

Topics :

1. SETS

2. OPERATIONS ON SETS

3. THE INTEGERS AND DIVISION

Almost all mathematical objects (even numbers !) can be defined in terms of sets. In any mathematical study, one considers a set or sets of certain objects; sets of numbers are quite common. The theory that results from the intuitive definition of a set – the so-called *naive* set theory – leads to *paradoxes* (i.e., logical inconsistencies). These logical inconsistencies can be avoided by building the *axiomatic* set theory. However, all the sets considered in this course can be treated consistently from the "naive" point of view.

2.1   Sets

We think of a *set* as a collection of objects; these objects are called the *elements* (or *members*) of the set. We DO NOT attempt to define the words **collection** or **object** (and hence the term **set**), but we assume that if we have a set S, then there is some "rule" that determines whether a given object x is a member of S. We say that *a set is completely determined by its elements.*

NOTE :   Membership in a set is an all-or-nothing situation. We cannot have a set S and an object x that belongs only partially to S. A given object is either a member of a set or it is not.

If A is a set and x is an object that belongs to A, we write $x \in A$. If x is not an element of A, then we write $x \notin A$.

NOTE :   It is important to know that a set itself may also be an element of some other set. Mathematics is full of examples of sets of sets. A *line*, for instance, is a set of *points*; the set of all lines in the *plane* is a natural example of a set of sets (of points).

A basic relation between sets is that of *containment* (or *subsethood*).

2.1.1 DEFINITION.   Let A and B be sets. We say that A is a **subset** of B, written $A \subseteq B$, provided every element of A is also an element of B. Simbolically:

$$\boxed{A \subseteq B \iff \forall x, \text{ if } x \in A \text{ then } x \in B.}$$

The phrases "A is contained in B" and "B contains A" are alternative ways of saying that "A is a subset of B".

NOTE :   (1)   We see that $A \subseteq B$ if and only if the quantification

$$\forall x \, (x \in A \rightarrow x \in B)$$

is TRUE.

(2)   It follows from the definition of a subset that a set A is *not* a subset of a set B, written $A \nsubseteq B$, if and only if there is at least one element of A that is not an element of B. Simbolically :

$$\boxed{A \nsubseteq B \iff \exists x \text{ such that } x \in A \text{ and } x \notin B.}$$

(3)   When we wish to emphasize that a set A is a subset of B but that $A \neq B$, we write $A \subset B$ and say that A is a **proper subset** of B.

2.1.2 DEFINITION.   Let A and B be sets. We say that the sets A and B are **equal**, written $A = B$, provided every element of A is in B and every element of B is in A. Symbolically :

$$\boxed{A = B \iff A \subseteq B \text{ and } B \subseteq A.}$$

NOTE :   (1)   *Two sets are equal if and only if they have the same elements.* More formally, $A = B$ if and only if the quantification

$$\forall x \ (x \in A \leftrightarrow x \in B)$$

is TRUE.

(2)   To know that a set A equals a set B, we must know that $A \subseteq B$ and we must also know that $B \subseteq A$.

There are several ways to describe sets.

(i)   One way is to *list* all the elements of the set, when it is possible. We use a notation where all elements of the set are listed between braces.

2.1.3 EXAMPLE.   The set V of all vowels in the English alphabet can be written as

$$V = \{a,\, e,\, i,\, o,\, u\}.$$

2.1.4 EXAMPLE.   The sets $\{a, b, c\}$, $\{a, c, b\}$ and $\{a, a, b, c\}$ are equal, since they have exactly the same elements, namely the symbols a, b and c.

NOTE :   It does not matter in what order we list the objects nor does it matter if we repeat an object. All that matters is what objects are members of the set and what objects are not.

The unique set that has no members is called the **empty set**, and is denoted by the symbol $\emptyset$.

NOTE :   The symbol $\emptyset$ is *not* the same as the Greek letter phi : ϕ or Φ.

Observe that

$$\emptyset \in \{\emptyset\} \quad \text{and} \quad \emptyset \subseteq \{\emptyset\}, \quad \text{but} \quad \emptyset \notin \emptyset.$$

It is important to distinguish clearly between the concepts of *set membership* ($\in$) and *set containment* ($\subseteq$). The notation $x \in A$ means that x is an element (member) of A. The notation $A \subseteq B$ means that every element of A is an element of B. Thus $\emptyset \subseteq \{1, 2, 3\}$ is TRUE, but $\emptyset \in \{1, 2, 3\}$ is FALSE.

NOTE :   The difference between $\in$ and $\subseteq$ is analogous to the difference between x and $\{x\}$. The symbol x refers to some object (a number or whatever), and the notation $\{x\}$ means the set whose one and only one element is the object x. It is always *correct* to write $x \in \{x\}$, but it is *incorrect* to write $x = \{x\}$ or $x \subseteq \{x\}$.

Uppercase letters are usually used to denote sets. We have special symbols to denote sets of *numbers* :

$\mathbb{N}$ denotes the set of *natural* numbers $\{0, 1, 2, 3, \dots\}$;

$\mathbb{Z}$ denotes the set of *integers* ;

$\mathbb{Q}$ denotes the set of *rational* numbers ;

$\mathbb{R}$ denotes the set of *real* numbers.

We will occasionally use the notation $\mathbb{Z}^+$ to denote the set of *positive integers* $\{1, 2, 3, \dots\}$. A natural number may be referred to as a *non-negative integer*.

We have

$$\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

There are two popular ways of thinking about the set $\mathbb{R}$ of *real numbers* :

- as a *geometric* object, with its *points* as positions on a straight line – the **real line**;

- as an *algebraic* object, with its elements as numbers (expressed as *decimal expansions*, where if a number is irrational we think of longer and longer decimal expansions approximating it more and more closely) – the **real number system**.

Each of these intuitive ideas can be made precise (and actually lead to ways of constructing the real numbers from the rational numbers).

NOTE :   (1)   Although sets are usually used to group together elements with common properties, there is nothing that prevents a set from having seemingly unrelated elements. For instance, $\{\alpha, \text{Paris}, \text{Mike}, 102\}$ is the set containing the elements α, Paris, Mike, and 102.

(2)   Sometimes the brace notation is used to describe a set without listing *all* its elements: some elements are listed, and then *ellipses* (. . .) are used when the general pattern of the elements is obvious. For instance, the set of positive integers less than 102 can be denoted by $\{1, 2, 3, \ldots, 102\}$.

(*ii*)   Whenever we are given a set S, we can use **set-builder notation** to describe a subset of S. The form of this notation is

$$\{\, \text{dummy variable} \, \in S \,|\, \text{conditions} \,\}.$$

This is the set of all objects drawn from the set S and subject to the conditions specified. For example, we could write

$$A = \{n \in \mathbb{N} \,|\, n \text{ is prime and } n < 15\}$$

which would be read "A equals the set of all n belonging to $\mathbb{N}$ *such that* n is prime and n is less than 15". Thus $\{n \in \mathbb{N} \,|\, n \text{ is prime and } n < 15\}$ describes the set $\{2, 3, 5, 7, 11, 13\}$.

NOTE :   In set-builder notation $\{x \in S \,|\, \ldots\}$ is always read "The set of *all* x belonging to S *such that* . . . ".

We have notation for certain special subsets of $\mathbb{R}$. We agree as usual that among real numbers

$\boxed{a < b}$ means "a is (strictly) less than b" or "$b - a$ is positive"

$\boxed{a \leq b}$ means "a is less than or equal to b" or "$b - a$ is non-negative".

Note that for any $a \in \mathbb{R}$, $a \leq a$. Then we define the **intervals** :

$$
\begin{aligned}
[a, b] &:= \{x \in \mathbb{R} \mid a \leq x \leq b\}; \\
(a, b) &:= \{x \in \mathbb{R} \mid a \leq x < b\}; \\
(a, b] &:= \{x \in \mathbb{R} \mid a < x \leq b\}; \\
(a, b) &:= \{x \in \mathbb{R} \mid a < x < b\}.
\end{aligned}
$$

When $b < a$, the definitions imply that all these sets equal $\emptyset$; if $a = b$, then $[a, b] = \{a\} = \{b\}$ and the rest are empty. By convention, the *half-unbounded* intervals are written similarly : if $a, b \in \mathbb{R}$, then

$$
\begin{aligned}
[a, \infty) &:= \{x \in \mathbb{R} \mid a \leq x\}; \\
(-\infty, b] &:= \{x \in \mathbb{R} \mid x \leq b\}; \\
(a, \infty) &:= \{x \in \mathbb{R} \mid a < x\}; \\
(-\infty, b) &:= \{x \in \mathbb{R} \mid x < b\}
\end{aligned}
$$

by definition, without thereby allowing the symbols $-\infty$ or ∞ as "numbers".

2.1.5 Example.   Let $a, b \in \mathbb{R}$ such that $0 < a \leq b$. Then

$$
a \leq \sqrt{ab} \leq \frac{a + b}{2} \leq b
$$

with equality if and only if $a = b$.

Solution :   Let $0 < a \leq b$. We have to prove three inequalities :

(1) $\sqrt{ab} - a = \sqrt{a}\left(\sqrt{b} - \sqrt{a}\right) \geq 0 \Rightarrow a \leq \sqrt{ab}$.

(2) $\frac{a+b}{2} - \sqrt{ab} = \frac{1}{2}\left(a + b - 2\sqrt{a} \cdot \sqrt{b}\right) = \frac{1}{2}\left(\sqrt{a} - \sqrt{b}\right)^2 \geq 0 \Rightarrow \sqrt{ab} \leq \frac{a+b}{2}$.

(3) $b - \frac{a+b}{2} = \frac{1}{2}(b - a) \geq 0 \Rightarrow \frac{a+b}{2} \leq b$.

The expressions $\sqrt{ab}$ and $\frac{a+b}{2}$ are called the **geometric mean** and the **arithmetic mean** (of the positive real numbers a and b), respectively.

NOTE : Inequality (2) has an interesting geometrical interpretation : *Among all rectangles with prescribed perimeter, the square is the one with largest area* (if $a+b = p$, then $ab \leq \left(\frac{p}{2}\right)^2$).

2.1.6 EXAMPLE. Let $a, b \in \mathbb{R}$ such that $a + b \geq 0$. Then the following inequality holds

$$\left(\frac{a+b}{2}\right)^3 \leq \frac{a^3 + b^3}{2}$$

with equality if and only if $a = \pm b$.

SOLUTION : We have

$$
\begin{aligned}
\frac{a^3 + b^3}{2} - \left(\frac{a+b}{2}\right)^3 &= \frac{1}{8}\left[4(a^3 + b^3) - (a+b)^3\right] \\
&= \frac{1}{8}\left(4a^3 + 4b^3 - a^3 - b^3 - 3a^2b - 3ab^2\right) \\
&= \frac{3}{8}\left(a^3 - a^2b + b^3 - ab^2\right) \\
&= \frac{3}{8}(a^2 - b^2)(a - b) \\
&= \frac{3}{8}(a - b)^2(a + b) \geq 0
\end{aligned}
$$

and hence

$$\left(\frac{a+b}{2}\right)^3 \leq \frac{a^3 + b^3}{2}.$$

Clearly, we have equality if and only if $a - b = 0$ or $a + b = 0$; that is, $a = \pm b$.

(*iii*) Sets can also be represented graphically using **Venn diagrams**. In Venn diagrams the **universal set** $\mathcal{U}$, which contains all the objects under consideration, is represented by a rectangle. Inside this rectangle, circles or other geometrical figures are used to represent sets. Sometimes points are used to represent the particular elements of a set.
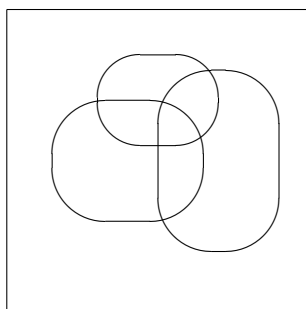
Venn diagram with three sets

Sets are used extensively in counting problems, and for such applications we need to discuss the "size" of sets.

2.1.7 DEFINITION.   Let S be a set. If there are exactly n distinct elements in S, where n is a natural number, we say that S is a **finite set** and that n is the **cardinality** of S. The cardinality of S is denoted by $|S|$.

2.1.8 EXAMPLE.   Let S be the set of letters in the English alphabet. Then $|S| = 26$.

2.1.9 EXAMPLE.   Since the empty set has no elements, it follows that $|\emptyset| = 0$.

2.1.10 DEFINITION.   A set is said to be **infinite** if it is not finite.

2.1.11 EXAMPLE.   The set $\mathbb{Z}^+$ of positive integers is infinite.

2.2   Operations on sets

Just as statements can be combined with logical connectives to produce new (compound) statements, and numbers can be added and multiplied to obtain new numbers, there are various operations we perform on sets. The most

basic set operations are *union* and *intersection*. Other operations are *difference*, *Cartesian product*, and *symmetric difference*; the latter is defined in the exercises.

It is safe to assume that all the sets under consideration are subsets of a fixed (large) *universal set* $\mathcal{U}$. Thus, for any set A,

$$\emptyset \subseteq A \subseteq \mathcal{U}.$$

2.2.1 DEFINITION.   Let A and B be sets. The **union** of A and B, denoted by $A \cup B$, is the set of all objects that belong either to A or to B, or to both.

In set-builder notation,

$$\boxed{A \cup B := \{x \,|\, x \in A \ \text{or} \ x \in B\}.}$$

2.2.2 EXAMPLE.   What is the union of the sets $A = \{1, 2, 5\}$ and $B = \{1, 2, 4\}$?

SOLUTION :   The union is $A \cup B = \{1, 2, 4, 5\}$.

2.2.3 DEFINITION.   Let A and B be sets. The **intersection** of A and B, denoted by $A \cap B$, is the set of all objects that belong to both A and B.

In set-builder notation,

$$\boxed{A \cap B := \{x \,|\, x \in A \ \text{and} \ x \in B\}.}$$

2.2.4 EXAMPLE.   What is the intersection of the sets $A = \{1, 2, 5\}$ and $B = \{1, 2, 4\}$?

SOLUTION :   The intersection is $A \cap B = \{1, 2\}$.

2.2.5 DEFINITION.   Let A and B be sets. The **difference** of A and B, denoted by $A \setminus B$, is the set of all objects belonging to A, but not to B. The diference of A and B is also called the **complement of B relative to A**.

The complement of B relative to the universal set $\mathcal{U}$, denoted by B^c, is called the **complement** of B.

In set-builder notation,

$$A \setminus B := \{x \mid x \in A \ \text{ and } \ x \notin B\}.$$

It followes that

$$\emptyset^c = \mathcal{U} \quad \text{and} \quad \mathcal{U}^c = \emptyset.$$

Also, observe that (for any sets A and B)

$$A \setminus B = A \cap B^c.$$

2.2.6 EXAMPLE. What is the difference of the sets $A = \{1, 2, 5\}$ and $B = \{1, 2, 4\}$?

SOLUTION : The difference is $A \setminus B = \{5\}$. This is different from the difference $B \setminus A$, which is $\{4\}$.

We list now some important set identities. In this, A, B, and C are subsets of a universal set $\mathcal{U}$.

(1) $A \cap \mathcal{U} = A$ (identity) ;

(2) $A \cup \emptyset = A$ (identity) ;

(3) $A \cap \emptyset = \emptyset$ (domination) ;

(4) $A \cup \mathcal{U} = \mathcal{U}$ (domination) ;

(5) $(A^c)^c = A$ (complementation) ;

(6) $A \cap A = A$ (idempotency) ;

(7) $A \cup A = A$ (idempotency) ;

(8) $A \cap B = B \cap A$ (commutativity) ;

(9) $A \cup B = B \cup A$ (commutativity) ;

(10) $A \cap (B \cap C) = (A \cap B) \cap C$ (associativity) ;

(11) $A \cup (B \cup C) = (A \cup B) \cup C$ (associativity) ;

(12) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributivity) ;

(13) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributivity) ;

(14) $(A \cap B)^c = A^c \cup B^c$ (De Morgan's law) ;

(15) $(A \cup B)^c = A^c \cap B^c$ (De Morgan's law).

NOTE :   There is a similarity between these set identities and the logical equivalences discussed in section **1.2**. In fact, the set identities given can be proved directly from the corresponding logical equivalences.

2.2.7 EXAMPLE.   Prove that for any sets A and B

$$(A \cup B)^c = A^c \cap B^c.$$

SOLUTION :   We have

$x \in (A \cup B)^c \iff x \notin A \cup B \iff \neg(x \in A \cup B) \iff \neg(x \in A \vee x \in B) \iff$

$\neg(x \in A) \wedge \neg(x \in B) \iff x \notin A \wedge x \notin B \iff x \in A^c \wedge x \in B^c \iff x \in A^c \cap B^c.$

Once a certain number of set properties have been established, new properties can be derived from them *algebraically*.

2.2.8 EXAMPLE.   For all sets $A, B,$ and C,

$$(A \cup B) \setminus (C \setminus A) = A \cup (B \setminus C).$$

SOLUTION :   We have

$$
\begin{aligned}
(A \cup B) \setminus (C \setminus A) &= (A \cup B) \cap (C \setminus A)^c \\
&= (A \cup B) \cap (C \cap A^c)^c \\
&= (A \cup B) \cap ((A^c)^c \cup C^c) \\
&= (A \cup B) \cap (A \cup C^c) \\
&= A \cup (B \cap C^c) \\
&= A \cup (B \setminus C).
\end{aligned}
$$

Set identities can also be proved using **membership tables**: we consider each combination of sets that an element can belong to and verify that elements in the same combinations of sets belong to both the sets in the identity; to indicate that an element *is* in an a set, the symbol **1** is used, whereas to indicate that an element is *not* in a set, the symbol **0** is used. (Note the similarity between the membership tables and truth tables; this is no coincidence !)

2.2.9 EXAMPLE.   Use a membership table to show that (for all sets A, B, and C)

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

SOLUTION :   The membership table is given below (it has eight rows).

A	B	C	$B \cap C$	$A \cup (B \cap C)$	$A \cup B$	$A \cup C$	$(A \cup B) \cap (A \cup C)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

It follows that the identity is valid.

Since the union and intersection of sets are associative operations, the sets $A \cup B \cup C$ and $A \cap B \cap C$ are well defined. We note that $A \cup B \cup C$ contains those objects that belong to at least one of the sets A, B, and C, and that $A \cap B \cap C$ contains those objects that belong to all of A, B, and C.

We can extend the union and intersection to n sets.

2.2.10 DEFINITION.   Let $A_1, A_2, \ldots, A_n$ be a *collection* of sets. The **union** of A_1,

$A_2, \ldots, A_n$, denoted by $A_1 \cup A_2 \cup \cdots \cup A_n$, is the set that contains those elements that are members of at least one set in the collection.

In set-builder notation,

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i := \{x \mid \exists i \text{ such that } x \in A_i\}.$$

2.2.11 DEFINITION. Let $A_1, A_2, \ldots, A_n$ be a *collection* of sets. The **intersection** of $A_1, A_2, \ldots, A_n$, denoted by $A_1 \cap A_2 \cap \cdots \cap A_n$, is the set that contains those elements that are members of all sets in the collection.

In set-builder notation,

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i := \{x \mid \forall i, \ x \in A_i\}.$$

2.2.12 EXAMPLE. Let $A_i = \{i, i+1, i+2, \ldots\}$, $i \in \{1, 2, \ldots, n\}$. Then

$$\bigcup_{i=1}^{n} A_i = \{1, 2, 3, \ldots\} \quad \text{and} \quad \bigcap_{i=1}^{n} A_i = \{n, n+1, n+2, \ldots\}.$$

2.2.13 DEFINITION. Let A and B be sets. The **Cartesian product** of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

In set-builder notation,

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

2.2.14 EXAMPLE. What is the Cartesian product of the sets $A = \{1, 2, 3\}$ and $B = \{\alpha, \beta\}$?

SOLUTION : The Cartesian product is

$$A \times B = \{(1, \alpha), (1, \beta), (2, \alpha), (2, \beta), (3, \alpha), (3, \beta)\}.$$

NOTE : (1) The Cartesian products $A \times B$ and $B \times A$ are *not* equal, unless $A = \emptyset$ or $B = \emptyset$ (so that $A \times B = \emptyset$) or unless $A = B$.

(2) Since

$$(a, b) \in A \times B \quad \Longleftrightarrow \quad a \in A \text{ and } b \in B$$

we can use the Cartesian product set to describe the set of outcomes of performing one operation *and* then another. For example, an object has to be coloured by choosing one of the colours from the set $C = \{c_1, c_2, c_3\}$ and then numbered by choosing one of the numbers from the set $N = \{n_1, n_2\}$ then the set of all possible objects which result is represented by the set

$$C \times N = \{(c_i, n_j) \mid i \in \{1, 2, 3\}, \ j \in \{1, 2\}\}.$$

The Cartesian product can easily be extended to n sets.

2.2.15 DEFINITION. Let $A_1, A_2, \ldots, A_n$ be sets. The **Cartesian product** of $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of all ordered n-**tuples** $(a_1, a_2, \ldots, a_n)$, where a_i belongs to A_i for $i \in \{1, 2, \ldots, n\}$.

In set-builder notation,

$$\boxed{A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i := \{(a_1, a_2, \ldots, a_n) \mid \forall i, \ a_i \in A_i\}.}$$

We write

$$A^2 := A \times A$$

and, in general,

$$A^n := \underbrace{A \times A \times \cdots \times A}_{n \text{ factors}}.$$

2.2.16 DEFINITION. Let S be a set. The **power set** of S, denoted by 2^S (or $\mathcal{P}(S)$), is the set of all subsets of S.

In set-builder notation,

$$\boxed{2^S := \{A \mid A \subseteq S\}.}$$

2.2.17 EXAMPLE.   What is the power set of $S = \{1, 2, 3\}$?

SOLUTION : $2^S = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

2.3   The integers and division

The set of all *integers* is denoted by $\mathbb{Z}$. The mathematical theory of integers and their properties is called *number theory* (or sometimes, on traditional grounds, *arithmetic*).

Any two integers $a, b \in \mathbb{Z}$ can be *added* and *multiplied* : their *sum* $a + b$ and their *product* ab are well-defined integers. Addition and multiplication of integers are governed by certain laws. The most basic ones are the following :

$$a + b = b + a; \qquad\qquad\qquad ab = ba;$$
$$a + (b + c) = (a + b) + c; \qquad\qquad a(bc) = (ab)c;$$
$$a(b + c) = ab + ac.$$

NOTE :   These fundamental arithmetic laws are very simple, and may seem obvious. But they might not be applicable to entities other than integers. However, these laws resemble some (but not all !) properties (laws) regarding logical propositions (w.r.t. disjuction and conjuction) or sets (w.r.t. union and intersection). For example, the addition of integers does not distributes w.r.t. the multiplication : in general, $a + bc \neq (a + b)(a + c)$.

The notion of *divisibility* is the central concept of number theory. Based on this concept, many important ideas (with far reaching applications) can be developed.

Divisibility

When one integer is devided by a second (nonzero) integer, the quotient may or may not be an integer. For example, $16 \div 4$ is an integer, whereas $15 \div 4$ is not.

We make the following definition.

2.3.1 DEFINITION.   If $a, b \in \mathbb{Z}$ and $b \neq 0$, we say that a is **divisible** by b, denoted $a \vdots b$, provided there is an integer k such that $a = bk$. Simbolically,

$$\boxed{a \vdots b \iff a = bk \quad \text{for some } k \in \mathbb{Z}.}$$

Alternatively, we say that

- a is a **multiple** of b;

- b is a **divisor** of a;

- b is a **factor** of a;

- b **divides** a.

The (alternative) notation $b \,|\, a$ is read "b divides a".

2.3.2 EXAMPLE.

(a) Is 40 divisible by 8 ?

(b) Does 5 divide 120 ?

(c) Is 48 a multiple of -16 ?

(d) Does $7 \,|\, (-7)$?

SOLUTION :   (a)   Yes, $40 = 8 \cdot 5$. (b) Yes, $120 = 5 \cdot 24$. (c) Yes, $48 = 16 \cdot (-3)$. (d) Yes, $-7 = 7 \cdot (-1)$.

2.3.3 EXAMPLE.   If m is a nonzero integer, does m divide 0 ?

SOLUTION :   Yes, because $0 = m \cdot 0$.

NOTE :   We may express the fact that m is a nonzero integer, by writing $m \in \mathbb{Z}^*$: $= \mathbb{Z} \setminus \{0\}$.

2.3.4 EXAMPLE.   Which integers divide 1 ?

SOLUTION :   The only divisors of 1 are 1 and -1.

The following result is easy to prove.

2.3.5 PROPOSITION. *Let* $a, b, c \in \mathbb{Z}$. *Then*

1. *If* $a \vdots c$ *and* $b \vdots c$, *then* $(a + b) \vdots c$.

2. *If* $a \vdots b$, *then* $ac \vdots b$.

3. *If* $a \vdots b$ *and* $b \vdots c$, *then* $a \vdots c$.

Every positive integer greater than 1 is divisible by *at least* two integers, since a positive integer is divisible by 1 and by itself. Integers that have exactly two (different) positive integer factors are called *prime*.

2.3.6 DEFINITION. A positive integer $p > 1$ is called **prime** if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called **composite**.

2.3.7 EXAMPLE. The first few prime numbers are :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \cdots$$

They become progresively more sparse and are rather irregularly distributed.

NOTE : Attempts have been made to find simple arithmetical formulas that yield only primes, even though they may not give all of them. PIERRE DE FERMAT (1601-1665) made the fameous *conjecture* that *all numbers of the form*

$$F(n) = 2^{2^n} + 1$$

are prime. Indeed, for $n = 1, 2, 3, 4$ we obtain

$$
\begin{aligned}
F(1) &= 2^2 + 1 = 5 \\
F(2) &= 2^{2^2} + 1 = 17 \\
F(3) &= 2^{2^3} + 1 = 257 \\
F(4) &= 2^{2^4} + 1 = 65\,537
\end{aligned}
$$

all prime numbers. But in 1732 LEONHARD EULER (1707-1783) discovered the factorization $2^{2^5} + 1 = 641 \cdot 6\,700\,417$; hence $F(5)$ is *not* prime.

Another remarkable and simple expression which produces many primes is

$$f(n) = n^2 - n + 41.$$

For $n = 1, 2, 3, \cdots, 40$, $f(n)$ is a prime number; but for $n = 41$, we have $f(n) = 41^2$, which is no longer a prime number.

On the whole, it has been a futile task to seek expressions of a simple type which produce only prime numbers. Even less promising is the attempt to find an algebraic formula which shall yield *all* the prime numbers.

Is the set of all such numbers *infinite*, or is there a largest prime number ? The answer was known to EUCLID and a proof (that the set of all prime numbers is infinite) will be given now. Only one additional fact is required.

2.3.8 LEMMA.   *For any integer a and prime number p, if $p \,|\, a$, then $p \,/\! | \,(a + 1)$.*

PROOF :   Suppose not. Suppose there exists an integer a and a prime number p such that

$$p \,|\, a \quad \text{and} \quad p \,|\, (a + 1).$$

Then, by definition of divisibility, there exist integers k and ℓ so that

$$a = pk \quad \text{and} \quad a + 1 = p\ell.$$

It follows that

$$1 = (a + 1) - a = pk - p\ell = p(k - \ell)$$

and so (since $k - \ell$ is an integer) $p \,|\, 1$. But the only divisors of 1 are 1 and -1. But p is prime, hence $p > 1$. This is a contradiction. (Hence the supposition is FALSE, and the proposition is TRUE.)   □

NOTE :   An implication $p \to q$ can be *proved* by showing that if p is TRUE, then q must also be TRUE. (This shows that the combination p TRUE and q FALSE never occurs.) A *proof* of this kind is called a **direct proof**.

Suppose that a contradiction can be *deduced* by assuming that q is not TRUE : the proposition $p \wedge \neg q \to \mathbf{C}$ is TRUE. We can see that

$$p \to q \iff (p \wedge \neg q \to \mathbf{C}).$$

It follows that if p is TRUE, then q must also be TRUE. An *argument* of this type (for proving the implication $p \to q$) is called a **proof by contradiction**.

2.3.9 THEOREM. *The set of all prime numbers is infinite.*

PROOF : Suppose not. Suppose the set of all prime numbers is finite. (We must deduce a contradiction.) Then all the prime numbers can be listed, say, in ascending order :

$$p_1 = 2, \; p_2 = 3, \; p_3 = 5, \; \cdots, \; p_n.$$

Consider the integer

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1.$$

Then $n > 1$ and so n is divisible by some prime number p : $p \,|\, n$. Also, since p is prime, p must equal one of the prime numbers $p_1, p_2, \cdots, p_n$. Thus

$$p \,|\, (p_1 \cdot p_2 \cdot p_3 \cdots p_n).$$

Then, by LEMMA 2.3.8, $p \,\nmid\, (p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1)$. So $p \,\nmid\, n$. This is a contradiction. (Hence the supposition is FALSE, and the theorem is TRUE.) $\square$

The prime numbers are the building blocks of positive integers, as the following result shows. This result (also referred to as the *Unique Factorization Theorem*) says that any positive integer $n > 1$ is either a prime number or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order of the factors.

2.3.10 THEOREM. (THE FUNDAMENTAL THEOREM OF ARITHMETIC) *Every positive integer $n > 1$ can be written uniquely as a product of prime numbers, where the prime factors are written in order of increasing size.*

Thus, for $n > 1$, there exist unique prime numbers $p_1 < p_2 < \cdots < p_k$ and unique positive integers $\alpha_1, \alpha_2 \cdots, \alpha_k$ such that

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k}.$$

2.3.11 EXAMPLE.   Find the prime factorizations of the numbers $100, 999,$ and $2005.$

SOLUTION :   We have

$$
\begin{aligned}
100 &= 2 \cdot 50 \\
&= 2 \cdot 2 \cdot 25 \\
&= 2^2 \cdot 5^2. \\
999 &= 9 \cdot 111 \\
&= 3^2 \cdot 3 \cdot 37 \\
&= 3^3 \cdot 37. \\
2005 &= 5 \cdot 401.
\end{aligned}
$$

NOTE :   It is often important to know whether a given positive integer is prime. It can be shown that *a positive integer is a prime number if it is not divisible by any prime number less than or equal to its square root.* For example, the number 401 is prime because it is not divisible by any of the prime numbers 2,3,5,7,11,13,17 or 19.

An important *corollary* of THE FUNDAMENTAL THEOREM OF ARITHMETIC is the following :

2.3.12 PROPOSITION.   *If a, b, p are positive integers and p is prime such that $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

SOLUTION :   If p were a factor of neither a nor b, then then the product of the prime factorizations of a and b would yield a prime factorization of the integer ab *not containing p*. On the other hand, since p is assumed to be a factor of ab, there exists an integer k such that $ab = pk$. Hence the product of p by a prime factorization of k would yield a prime factorization of the

integer *ab containing p*, contrary to the fact that the prime factorization of
ab is unique. □

2.3.13 EXAMPLE. If one has verified the fact that 13 is a divisor of $2\,652$,
and the fact that $2\,652 = 6 \cdot 442$, one may conclude that 13 is a divisor of
442.

On the other hand, 6 is a factor of 240, and $240 = 15 \cdot 16$, but 6 is *not*
a factor of either 15 or 16.

(This shows that the assumption that p is a prime number is an essential
one.)

In order to find all the divisors (or factors) of any (positive integer) a we
need only its prime decomposition

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}.$$

All the divisors of a are the numbers

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where the β's are any integers satisfying the inequalities

$$0 \leq \beta_1 \leq \alpha_1, \quad 0 \leq \beta_2 \leq \alpha_2, \quad \cdots, \quad 0 \leq \beta_n \leq \alpha_n.$$

It follows that *the number of all different divisors of a (including the divisors
1 and a) is given by the product*

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1).$$

2.3.14 EXAMPLE. The positive integer $144 = 2^4 \cdot 3^2$ has $5 \cdot 3 = 15$ divisors.
They are

$$1, \ 2, \ 4, \ 8, \ 16, \ 3, \ 6, \ 12, \ 24, \ 48, \ 9, \ 18, \ 36, \ 72, \ 144.$$

GCDs and LCMs

An integer may or may not be divisible by another. However, when an integer is divided by a positive integer, there always is a *quotient* and a *remainder*. The following result holds.

2.3.15 THEOREM.   (THE QUOTIENT-REMAINDER THEOREM) *Given any integer* a *and positive integer* d, *there are unique integers* q *and* r *such that*

$$a = d \cdot q + r \quad and \quad 0 \leq r < d.$$

In the equality above, d is called the **divisor**, a is called the **dividend**, q is called the **quotient**, and r is called the **remainder**.

2.3.16 EXAMPLE.   What are the quotient and the remainder when 82 is divided by 11 ?

SOLUTION :   We have

$$82 = 11 \cdot 7 + 5.$$

Hence the quotient (when 82 is divided by 11) is 7 and the remainder is 5.

2.3.17 EXAMPLE.   What are the quotient and the remainder when -43 is divided by 8 ?

SOLUTION :   We have

$$-43 = 8 \cdot (-6) + 5.$$

Hence the quotient (when -43 is divided by 8) is -6 and the remainder is 5. (Note that the remainder cannot be negative.)

2.3.18 DEFINITION.   Let a and b be two nonzero integers. The largest integer d such that $d \,|\, a$ and $d \,|\, b$ is called the **greatest common divisor** of a and b.

The greatest common divisor of a and b is denoted by $\mathsf{GCD}\,(a, b)$.

The GCD of two nonzero integers always exists because the set of common divisors of these integers is finite. One way to find the GCD of two integers is to find all the positive common divisors of both integers and then take the largest divisor.

2.3.19 EXAMPLE. Find the greatest common divisor of 48 and 64.

SOLUTION : The positive common divisors of 48 and 64 are

$$1, 2, 4, 8, \quad \text{and} \quad 16.$$

Hence $\mathsf{GCD}\,(48, 64) = 16$.

2.3.20 EXAMPLE. What is the GCD of 16 and 81 ?

SOLUTION : The integers 16 and 81 have no positive common divisors other than 1, so that $\mathsf{GCD}\,(16, 81) = 1$.

NOTE : Two integers who have no common positive divisors other than 1 are said to be **relatively prime**. Clearly, any two prime numbers are relatively prime.

Another way to find the GCD of two integers is to use the *prime factorizations* of these integers. Suppose that the prime factorizations of the nonzero integers a and b are :

$$a = p_1^{\alpha_1} \cdot p_1^{\alpha_2} \cdots p_n^{\alpha_n} \quad \text{and} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where each exponent is a *nonnegative* integer and where all prime factors occuring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then $\mathsf{GCD}\,(a, b)$ is given by

$$\mathsf{GCD}\,(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_n^{\min(\alpha_n, \beta_n)}$$

where $\min(r, s)$ represents the *minimum* of the two numbers r and s.

2.3.21 EXAMPLE.   Find the GCD of 200 and 360.

SOLUTION :   The prime factorizations of 200 and 360 are

$$
\begin{aligned}
200 &= 8 \cdot 25 \\
&= 2^3 \cdot 5^2, \\
360 &= 4 \cdot 9 \cdot 10 \\
&= 2^3 \cdot 3^2 \cdot 5.
\end{aligned}
$$

Hence

$$\mathsf{GCD}\,(200, 360) = 2^{\min(3,3)} \cdot 3^{\min(0,2)} \cdot 5^{\min(2,1)} = 2^3 \cdot 3^0 \cdot 5^1 = 40.$$

Prime factorizations can also be used to find the *least commun multiple* of two integers.

2.3.22 DEFINITION.   Let a and b be two positive integers. The smallest positive integer m such that $m \,\vdots\, a$ and $m \,\vdots\, b$ is called the **least common multiple** of a and b.

The least common multiple of a and b is denoted by $\mathsf{LCM}\,(a, b)$.

The LCM of two integers always exists because the set of integers divisible by both a and b is nonempty, and *every nonempty set of positive integers has a least element*. Suppose that the prime factorizations of a and b are as before. Then $\mathsf{LCM}\,(a, b)$ is given by

$$\mathsf{LCM}\,(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdots p_n^{\max(\alpha_n, \beta_n)}$$

where $\max(r, s)$ represents the *maximum* of the two numbers r and s.

2.3.23 EXAMPLE.   What is the least common multiple of $a = 2^2 \cdot 3^4 \cdot 5$ and $b = 2 \cdot 3^2 \cdot 7^2$?

SOLUTION :   We have

$$\mathsf{LCM}\,(a, b) = 2^{\max(2,1)} \cdot 3^{\max(4,2)} \cdot 5^{\max(1,0)} \cdot 7^{\max(0,2)} = 2^2 \cdot 3^4 \cdot 5 \cdot 7^2.$$

There is an interesting relationship between the GCD and the LCM of two integers.

2.3.24 PROPOSITION. *Let a and b be positive integers. Then*

$$a \cdot b = \mathsf{GCD}\,(a,b) \cdot \mathsf{LCM}\,(a,b).$$

The Euclidean algorithm

The method for computing the GCD of two integers, using the prime factorization, is very inefficient. (The reason is that finding prime factorizations is a time-consuming process.) More efficient methods exist. The following *algorithm*, called the **Euclidean algorithm**, has been known since ancient times. It is based on the following facts :

- If r is a positive integer, then $\mathsf{GCD}\,(r,0) = r$.

- If a, b, q, r are integers such that $a = b \cdot q + r$, then $\mathsf{GCD}\,(a,b) = \mathsf{GCD}\,(b,r)$.

The Euclid algorithm can be described as follows :

1. Let a and b be integers with $a > b \geq 0$.

2. To find the GCD of a and b, first check whether $b = 0$. If it is, then $\mathsf{GCD}\,(a,b) = a$. If it isn't, then put $r_0 = a$ and $r_1 = b$, and then apply successively the *Quotient-Remainder Theorem* :

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 & (0 \leq r_2 < r_1)\\
r_1 &= r_2 q_2 + r_3 & (0 \leq r_3 < r_2)\\
&\ \ \vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & (0 \leq r_n < r_{n-1})\\
r_{n-1} &= r_n q_n.
\end{aligned}
$$

Eventually *a remainder of zero occurs in this sequence of successive divisions* (since a sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms).

3. It follows that

$$
\begin{aligned}
\mathsf{GCD}\,(a,b) &= \mathsf{GCD}\,(r_0, r_1) \\
&= \mathsf{GCD}\,(r_1, r_2) \\
&\ \ \vdots \\
&= \mathsf{GCD}\,(r_n, 0) \\
&= r_n.
\end{aligned}
$$

Hence *the* $\mathsf{GCD}\,(a,b)$ *is the last nonzero remainder in the sequence of divisions.*

NOTE : It is always the case that the number of steps required in the Euclidean algorithm is at most five times the number of digits in the small number.

2.3.25 EXAMPLE. Calculate the GCD of 330 and 156 using the Euclidean algorithm.

SOLUTION : We have

$$
\begin{aligned}
330 &= 156 \cdot 2 + 18 \\
156 &= 18 \cdot 8 + 12 \\
18 &= 12 \cdot 1 + 6 \\
12 &= 6 \cdot 1 + 0.
\end{aligned}
$$

Hence

$$
\mathsf{GCD}\,(330, 156) = 6.
$$

An extremely important property of $\mathsf{GCD}\,(a,b)$ can be derived from the Euclidean algorithm.

2.3.26 PROPOSITION. *If a and b are positive integers, then there exist integers k and ℓ such that*

$$
\mathsf{GCD}\,(a,b) = ka + \ell b.
$$

SOLUTION : As before, consider the sequence of successive divisions :

$$r_0 = r_1 q_1 + r_2$$
$$r_1 = r_2 q_2 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$
$$r_{n-1} = r_n q_n.$$

From the first equation

$$r_2 = a - q_1 b$$

so that r_2 can be written in the form $k_1 a + \ell_1 b$ (in this case $k_1 = 1$ and $\ell_1 = -q_1$).

From the next equation,

$$
\begin{aligned}
r_3 &= b - q_2 r_2 \\
&= b - q_2(k_1 a + \ell_1 b) \\
&= (-q_2 k_1)a + (1 - q_2 \ell_1)b \\
&= k_2 a + \ell_2 b.
\end{aligned}
$$

Clearly this process can be repeated through the successive remainders $r_4, r_5, \cdots$ until we arrive at the representation

$$r_n = ka + \ell b$$

as was to be proved. $\qquad \square$

2.3.27 EXAMPLE. Express $\mathsf{GCD}\,(61, 24)$ as a *linear combination* of 61 and 24 (i.e. in the form $k \cdot 61 + \ell \cdot 24$).

SOLUTION :   We have

$$
\begin{aligned}
61 &= 2 \cdot 24 + 13 \\
24 &= 1 \cdot 13 + 11 \\
13 &= 1 \cdot 11 + 2 \\
11 &= 5 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0.
\end{aligned}
$$

We have, from the first of these equations,

$$13 = 61 - 2 \cdot 24,$$

from the second,

$$11 = 24 - 13 = 24 - (61 - 2 \cdot 24) = -61 + 3 \cdot 24,$$

from the third,

$$2 = 13 - 11 = (61 - 2 \cdot 24) - (-61 + 3 \cdot 24) = 2 \cdot 61 - 5 \cdot 24,$$

and from the fourth,

$$1 = (-61 + 3 \cdot 24) - 5 \cdot (2 \cdot 61 - 5 \cdot 24) = -11 \cdot 61 + 28 \cdot 24.$$

NOTE :   The fact that $d = \mathsf{GCD}\,(a, b)$ can always be written in the form

$$d = k \cdot a + \ell \cdot b$$

may be used to prove the FUNDAMENTAL THEOREM OF ARITHMETIC.

2.4   Exercises

Exercise 16 TRUE or FALSE ?

   (a) $\emptyset = \{\emptyset\}$.

   (b) $4 \in \{4\}$.

(c) $\{4\} \subseteq \{\{4\}\}$.

(d) $\emptyset \in \{4\}$.

(e) $\emptyset \subseteq \{4\}$.

(f) $[2, 4] \subseteq \mathbb{N}$.

(g) $\{2, 3, 4\} \subseteq \mathbb{Z}$.

(h) $\frac{1}{2} \in \{0, 1\}$.

Exercise 17 Let $a, b, c \in \mathbb{R}$. Prove that

$$a^2 + b^2 + c^2 \geq ab + bc + ca$$

with equality if and only if $a = b = c$.

Exercise 18 Let $a, b, a_1, a_2, b_1, b_2 \in \mathbb{R}$. Prove that :

(a) (**Mean inequalities**)   If $0 < a \leq b$, then

$$a \leq \frac{2}{\frac{1}{a} + \frac{1}{b}} \leq \sqrt{ab} \leq \frac{a + b}{2} \leq \sqrt{\frac{a^2 + b^2}{2}} \leq b$$

with equality if and only if $a = b$.

(b) (**Cauchy-Schwarz inequality**)

$$(a_1 b_1 + a_2 b_2)^2 \leq (a_1^2 + a_2^2)(b_1^2 + b_2^2)$$

with equality if and only if $a_1 = r b_1$ and $a_2 = r b_2$ $(r \in \mathbb{R})$.

(c) (**Chebyshev inequality**)   If $a_1 \leq a_2$ and $b_1 \leq b_2$, then

$$(a_1 + a_2)(b_1 + b_2) \leq 2(a_1 b_1 + a_2 b_2)$$

with equality if and only if $a_1 = a_2$ and $b_1 = b_2$.

NOTE :   (1)   The expressions $\frac{2}{\frac{1}{a} + \frac{1}{b}}$ and $\sqrt{\frac{a^2 + b^2}{2}}$ are called the **harmonic mean** and the **quadratic mean** (of the positive real numbers a and b), respectively.

(2)   All these inequalities (given here for the case $n = 2$) can be generalized.

Exercise 19 Find conditions on sets A and B to make each of the following propositions TRUE.

(a) $A \cup B = A$.

(b) $A \cap B = B$.

(c) $A \cup B = A \cap B$.

(d) $A \setminus B = \emptyset$.

(e) $A \setminus B = A$.

(f) $A \setminus B = B$.

(g) $A \setminus B = B \setminus A$.

Exercise 20 Can you conclude that $A = B$ if A, B and C are sets such that

(a) $A \cup C = B \cup C$?

(b) $A \cap C = B \cap C$?

(c) $A \cup C = B \cup C$ and $A \cap C = B \cap C$?

Exercise 21 The **symmetric difference** of A and B, denoted by $A \triangle B$, is the set containing those elements in either A or B, but not in both A and B; that is,

$$A \triangle B := (A \cup B) \setminus (A \cap B).$$

(a) Find the symmetric difference of $\{1, 2, 3\}$ and $\{2, 3, 4\}$.

(b) Show that

  i. $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

  ii. $A \triangle A = \emptyset$.

  iii. $A \triangle \emptyset = A$.

  iv. $A \triangle B = B \triangle A$.

  v. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$

(c) What can you say about the sets A and B if $A \triangle B = A$?

Exercise 22 TRUE or FALSE ?

(a) If A, B are finite sets, then $\mid A \times B \mid = \mid A \mid \cdot \mid B \mid$.

(b) If A, B are finite sets, then $\mid A \setminus B \mid = \mid A \mid - \mid B \mid$.

(c) If A, B are finite sets, then $\mid A \cup B \mid = \mid A \mid + \mid B \mid$.

(d) If A, B are finite sets, then $\mid 2^A \mid = 2^{\mid A \mid}$.

(e) If A, B are sets, and $(5,6) \notin A \times B$, then $5 \notin A$ and $6 \notin B$.

(f) If A, B are sets, and $5 \notin A$, then $(5,6) \notin A \times B$.

(g) If A, B are sets, and $(A \times B) \cap (B \times A) \neq \emptyset$, then $A \cap B \neq \emptyset$.

(h) If A, B are sets, and $A \cap B \neq \emptyset$, then $(A \times B) \cap (B \times A) \neq \emptyset$.

If the statement is FALSE, give a counterexample.

Exercise 23 Let A, B, and C be sets. Show that :

(a) $(A \setminus B) \cap (A \cap B) = \emptyset$.

(b) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

(c) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

(d) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

(e) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.

Exercise 24 Prove the following statements.

(a) If a is a nonzero integer, then

$$1 \mid a \quad \text{and} \quad a \mid 0.$$

(b) If a, b, and c are integers such that $a \mid b$, then $a \mid bc$.

(c) If a, b, and c are integers such that $a \mid b$ and $b \mid c$, then $a \mid c$.

(d) If a, b, c, and d are integers such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.

(e) If a, b, and c are integers such that $ac \mid bc$, then $a \mid b$.

Exercise 25 Are the following integers prime ?

(a) 93.

(b) 101.

(c) 301.

(d) 1001.

Exercise 26 In each of the following cases, what are the quotient and remainder ?

(a) 19 is divided by 7.

(b) -101 is divided by 11.

(c) 1001 is divided by 13.

(d) 0 is divided by 23.

(e) -1 is divided by 5.

Exercise 27 Find the prime factorization of each of the following.

(a) 39.

(b) 81.

(c) 101.

(d) 289.

(e) 899.

Exercise 28 Use the Euclidean algorithm to find

(a) $\mathsf{GCD}\,(12, 18)$.

(b) $\mathsf{GCD}\,(111, 201)$.

(c) $\mathsf{GCD}\,(1001, 1331)$.

(d) $\mathsf{GCD}\,(123, 4321)$.

Exercise 29 Express the GCD of each of the following pairs of integers as a linear combination of these integers.

(a) 10, 11.

(b) 21, 44.

(c) 36, 48.

(d) 34, 55.

(e) 117, 213.

(f) 0, 223.

Exercise 30 TRUE or FALSE ?

(a) If a and b are integers such that $a \vdots b$ and $b \vdots a$, then $a = b$.

(b) If a, b, and c are positive integers such that $a \mid bc$, then $a \mid c$.

(c) The integers which leave a remainder 1 when divided by 2 and also leave a remainder 1 when divided by 3 are those and only those of the form $6k + 1$, where $k \in \mathbb{Z}$.

Chapter 3

Functions

Topics :

1. GENERAL FUNCTIONS

2. SPECIFIC FUNCTIONS

3. PERMUTATIONS

The concept of *function* is central to mathematics. (The words *map* and *mapping* are synonims for function.) This fundamental notion is the modern extension of the classical concept of a (numerical) function of one or several numerical "variables".

The idea of *symmetry* can be formalized and studied using *permutations*; the related notion of invariance plays an important role in modern geometry and physics. Sets of permutations on finite sets appear naturally (as groups of substitutions) in the study of algebraic equations.

3.1 General functions

In everyday language the word *function* indicates dependence of one varying quantity on another. Intuitively, a function is a "mechanism" that transforms one quantity into another. We shall make this idea more precise.

3.1.1 DEFINITION.　Let A and B be sets. A **function** f from A to B, denoted by $f : A \to B$, is a *rule* which associates with each element $x \in A$ a unique element $y \in B$. We write $y = f(x)$ to denote the element y assigned to x by the rule f; we say that y is the **image** of x under f (or the **value** of f at x), and x is a **preimage** of y under f.

We may think of a function as an "abstract machine" that processes an **input** x, in a certain way, to produce *the* **output** $f(x)$. If f is a function from A to B, we often write

$$f : A \to B, \quad x \mapsto f(x).$$

We also say that F is a *mapping* (or *map*) from A to B; it is customary to say that f maps the element x to (the element) $f(x)$. The set of all functions (or mappings) from A to B is denoted by B^A.

NOTE :　We have used $\to$ to specify the sets a function is between and $\mapsto$ to specify its "rule". This distinction between $\to$ and $\mapsto$ will be consistent throughout these notes.

　A function may be specified by a *list*, such as

$$f : \{a, b, c\} \to \mathbb{R}, \quad a \mapsto 1, \ b \mapsto 10 \quad \text{and} \quad c \mapsto 100$$

or by an *algebraic expression*, such as

$$g : \mathbb{Z} \to \mathbb{Z}, \quad x \mapsto x^2 + 4.$$

NOTE :　The "mechanism" of a function need not be dictated by an algebraic formula. All that is required is that we carefully specify the allowable inputs and, for each allowable input, the corresponding output.

3.1.2 EXAMPLES.   Let A be the set of people in a class.

1. There is a function $e : A \to [0, 100]$, which assigns to each person $x \in A$ an examination mark $e(x) \in [0, 100]$.

2. There is a function $g : A \to \{0, 1\}$, where

$$g(x) := \begin{cases} 1, & \text{if } x \text{ is male} \\ 0, & \text{if } x \text{ is female} \end{cases}$$

3. There is a function $b : A \to \{1, 2, 3, \ldots, 366\}$, where $b(x)$ is the unique number which encodes the birthday of x.

We can associate a set of ordered pairs in $A \times B$ to each function from A to B. This set is called the *graph* of the function and is often displayed pictorially to aid in understanding the behaviour of the function.

3.1.3 DEFINITION.   Let $f : A \to B$ be a function. The **graph** of the function f is the set of ordered pairs $\{(x, f(x)) \mid x \in A\}$.

If A and B are finite sets, we can represent a function f from A to B by making a list of elements in A and a list of elements in B and drawing an arrow from each element in A to the corresponding element in B. Such a drawing is called an **arrow diagram**.
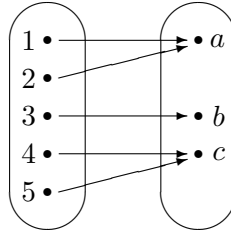
3.1.4 EXAMPLE.   Consider the function

$$f : \{1, 2, 3, 4, 5\} \to \{a, b, c\}$$

given by

$$1 \mapsto a, \ 2 \mapsto a, \ 3 \mapsto b, \ 4 \mapsto c, \ 5 \mapsto c.$$
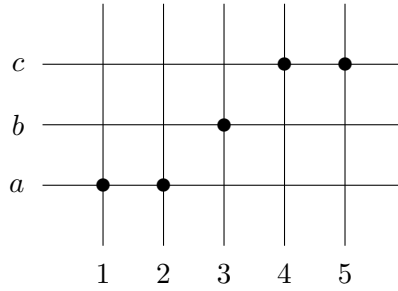
The function f can be represented by the following *arrow diagram* :

Alternatively, the graph of f,

$$G_f = \{(1,a),\ (2,a),\ (3,b),\ (4,c),\ (5,c)\},$$

can be exhibited as follows :

NOTE : It is customary to *identify* a function $f : A \to B$ and its graph $G_f \subseteq A \times B$; that is, to think of a function as *a set of ordered pairs* of elements. In this case, we call – by abuse of language – the exhibition of the set G_f the *graphical representation* (or even the *graph*) of the function f.

3.1.5 DEFINITION.   Let f be a function from A to B. We say that the set A is the **domain** of f and the set B is the **codomain** of f. The set $\{f(x) \,|\, x \in A\}$ is called the **range** (or **image**) of f.

NOTE : (1) Although the range $\operatorname{im}(f)$ of a function f is always a subset of the codomain, there is no requirement that the range equals the codomain. Thus $\operatorname{im}(f) \subseteq B$.

(2) If the domain $\operatorname{dom}(f)$ and codomain $\operatorname{codom}(f)$ of a function f are understood, we will write simply
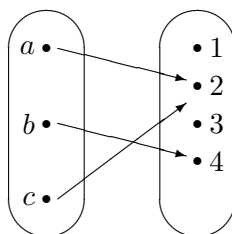
$$y = f(x).$$

As a matter of convention, if we write

$$y = f(x) \quad \text{or} \quad x \mapsto f(x)$$

without defining the domain of f, then we will *always* assume that the domain of f is the set of *all* x for which $f(x)$ is meaningful. For example, $y = \frac{1}{x}$ will have, by this convention, the domain $\text{dom}(f) = \{x \in \mathbb{R} \mid x \neq 0\}$.

3.1.6 EXAMPLE.   Let $A = \{a, b, c\}$ and $B = \{1, 2, 3, 4\}$. Define a function f from A to B by the arrow diagram

(a) Write the domain and the codomain of f.

(b) Find $f(a)$, $f(b)$ and $f(c)$.

(c) What is the range (image) of f ?

(d) Find the preimages of 2, 4, and 1. [If $y \in \text{codom}(f)$, then the *preimage* of y under f is the set $f^{-1}(y) := \{x \in \text{dom}(f) \mid f(x) = y\}$.]

(e) Represent f as a set of ordered pairs.

SOLUTION :

(a) $\text{dom}(f) = \{a, b, c\}$ and $\text{codom}(f) = \{1, 2, 3, 4\}$.

(b) $f(a) = 2$, $f(b) = 4$, and $f(c) = 2$.

(c) $\text{im}(f) = \{2, 4\}$.

(d) $f^{-1}(2) = \{a, c\}$, $f^{-1}(4) = \{b\}$, and $f^{-1}(1) = \emptyset$.

(e) $f = \{(a, 2), (b, 4), (c, 2)\}$.

3.1.7 DEFINITION.   Suppose f and g are functions from A to B. Then f **equals** g, written $f = g$, provided

$$f(x) = g(x) \quad \text{for all} \ \ x \in A.$$

3.1.8 EXAMPLE.   Define $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ by the following formulas (for all $x \in \mathbb{R}$) :

$$\begin{aligned} f(x) &= |x| \\ g(x) &= \sqrt{x^2}. \end{aligned}$$

Does $f = g$?

SOLUTION :   Yes. Since the *absolute value* of a (real) number equals the square root of its square, $|x| = \sqrt{x^2}$ for all $x \in \mathbb{R}$. Hence $f = g$.

<div align="center">

Injective and surjective functions

</div>

A function may send several elements of its domain (inputs) to the same element of its codomain (output). In terms of arrow diagrams, this means means that two or more arrows that start in the domain can point to the same element in the codomain. On the other hand, a function may associate a different element of its codomain to each element of its domain, which would mean that no two arrows that start in the domain would point to the same element in the codomain. A function with this property is called *one-to-one*.

3.1.9 DEFINITION.   Let $f : A \to B$ be a function. We say that f is **one-to-one** (or **injective**) provided $f(x_1) \neq f(x_2)$, whenever $x_1 \neq x_2$. Simbolically :

$$\boxed{f \text{ is injective} \iff (\forall x_1, x_2 \in A, \text{ if } x_1 \neq x_2 \text{ then } f(x_1) \neq f(x_2)).}$$

In other words, every element of the codomain of a one-to-one function has *at most* one preimage. A one-to-one function is also called an **injection**.

NOTE :   (1)   We see that a function $f : A \to B$ is one-to-one if and only if the quantification

$$\forall x_1 \forall x_2 \, (x_1 \neq x_2 \; \to \; f(x_1) \neq f(x_2))$$

is TRUE.

(2)   Equivalently,

$$\boxed{f \text{ is injective } \Longleftrightarrow \; (\forall x_1, x_2 \in A, \text{ if } \; f(x_1) = f(x_2) \; \text{ then } \; x_1 = x_2).}$$

(3)   For a one-to-one function $f : A \to B$, any two distinct elements of the domain A are sent to two distinct elements of the codomain. It follows that the function f is *not* one-to-one if and only if at least two elements of the domain are taken to the same element of the codomain. Symbolically :

$$\boxed{f \text{ is } not \text{ injective } \Longleftrightarrow \; (\exists x_1, x_2 \in A, \; \text{ such that } \; x_1 \neq x_2 \; \text{ and } \; f(x_1) = f(x_2)).}$$

3.1.10 EXAMPLE.   Let $f : \{a, b, c\} \to \{1, 2, 3, 4\}$ defined by $f(a) = 2$, $f(b) = 3$ and $f(c) = 2$. The function f is *not* one-to-one since $f(a) = f(c)$ and $a \neq c$.

3.1.11 EXAMPLE.   Let $A = [0, \infty)$ and let $f : A \to A$ be defined by $f(x) = \frac{5x^2 + 3}{3x^2 + 5}$. Is this function one-to-one ?

SOLUTION :   To show that f is an injection, we must show that, if $f(a) = f(b)$, then $a = b$. Suppose that $f(a) = f(b)$. Then

$$\frac{5a^2 + 3}{3a^2 + 5} = \frac{5b^2 + 3}{3b^2 + 5}$$

and so

$$15a^2 b^2 + 9b^2 + 25a^2 + 15 = 15a^2 b^2 = 9a^2 + 25b^2 + 15 \,.$$

This relation simplifies to $16a^2 = 16b^2$, or $a^2 = b^2$. Since $a \geq 0$ and $b \geq 0$, it follows that $a = b$.

There may be an element of the codomain of a function that is not the image of any element in the domain. On the other hand, a function may have the property that *every* element of its codomain is the image of some element of its domain. Such a function is called *onto*.

3.1.12 DEFINITION. Let $f : A \to B$ be a function. We say that f is **onto** (or **surjective**) provided for every element $y \in B$ there is an element $x \in A$ so that $f(x) = y$. Symbolically :

$$\boxed{f \text{ is surjective} \iff \forall y \in B, \exists x \in A \text{ such that } f(x) = y.}$$

In other words, every element of the codomain of an onto function has *at least* one preimage. An onto function is also called a **surjection**.

NOTE : (1) We see that a function $f : A \to B$ is onto if and only if the quantification

$$\forall y \, \exists x \, (y = f(x))$$

is TRUE.

(2) A function $f : A \to B$ is onto if and only if its range $\text{im}(f)$ equals the codomain B. It follows that the function f is *not* onto if and only if $\text{im}(f) \subset B$. That is, there is at least one element of B that is not an element of $\text{im}(f)$. Symbolically :

$$\boxed{f \text{ is } not \text{ surjective} \iff \exists y \in B \text{ such that } \forall x \in A, \; f(x) \neq y.}$$

3.1.13 EXAMPLE. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{7, 8, 9, 10\}$. Let $f, g : A \to B$ be defined by

$$f : \quad 1 \mapsto 7, \; 2 \mapsto 7, \; 3 \mapsto 8, \; 4 \mapsto 9, \; 5 \mapsto 9, \; 6 \mapsto 10$$

and

$$g : \quad 1 \mapsto 7, \; 2 \mapsto 7, \; 3 \mapsto 7, \; 4 \mapsto 9, \; 5 \mapsto 9, \; 6 \mapsto 10 \, ,$$

respectively. Investigate for surjectivity these two functions.

SOLUTION : The function f is onto because for each element $b \in B$ we can find one or more elements $a \in A$ such that $f(a) = b$. It is also easy to check that $\text{im}(f) = B$.

However, the function g is *not* onto. Observe that $8 \in B$ but there is no $a \in A$ with $g(a) = 8$. Also, $\text{im}(g) = \{7, 9, 10\} \neq B$.

3.1.14 EXAMPLE.   Let $f : \mathbb{Q} \to \mathbb{Q}$ defined by $x \mapsto 3x + 4$. Prove that f is onto.

SOLUTION :   Let $b \in \mathbb{Q}$ be arbitrary. We seek an $a \in \mathbb{Q}$ so that $f(a) = b$.

Let $a = \frac{1}{3}(b - 4)$. (Since b is a rational number, so is a.) Notice that

$$f(a) = 3\left[\frac{1}{3}(b - 4)\right] + 4 = (b - 4) + 4 = b.$$

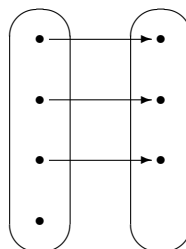Therefore the function $f : \mathbb{Q} \to \mathbb{Q}$ is onto.

How did we ever "guess" that we should take $a = \frac{1}{3}(b - 4)$? We did not guess, we worked backward ! That is, we solved for a the *equation* $f(a) = b$.

3.1.15 EXAMPLE.   Let S be a finite set, with at least one element, and let $f : 2^S \to \mathbb{Z}^+$ be defined by $f(A) = |A|$ (cardinality of A). This function is not a surjection.
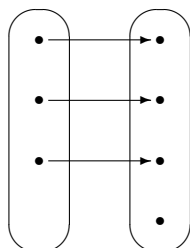
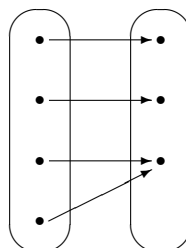We can use arrow diagrams to exhibit various specific situations.
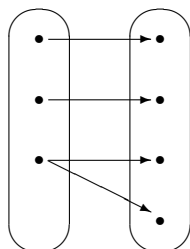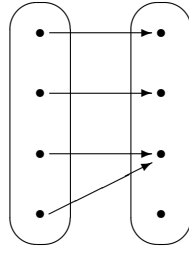

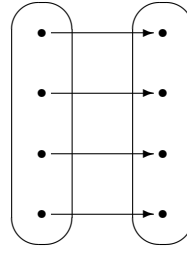not a function   not a function

1-1 but not onto   onto but not 1-1

neither 1-1 nor onto   1-1 and onto

3.1.16 DEFINITION.   A function f is **bijective** if f is both one-to-one and onto.

Every element of the codomain of a bijective function has *exactly* one preimage. A bijective function is also called a **one-to-one correspondence** (or **bijection**).

3.1.17 DEFINITION.   Let A be a (nonempty) set. The **identity function** on A is the function $id_A : A \to A$ defined by

$$id_A(x) := x, \quad x \in A.$$

Every identity function is bijective.

3.1.18 EXAMPLES.   (1)   The function $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ is neither injective nor surjective, since $f(-1) = f(1)$ and for $y < 0$ there is no $x \in \mathbb{R}$ such that $y = f(x)$.

(2)   The function $g : \mathbb{R} \to [0, \infty)$, $x \mapsto x^2$ is not injective but is surjective.

(3)   The function $h : [0, \infty) \to \mathbb{R}$, $x \mapsto x^2$ is injective but is not surjective.

(4)   The function $k : [0, \infty) \to [0, \infty)$, $x \mapsto x^2$ is bijective.

The inverse of a function

If f is a one-to-one correspondence from A to B, then there is a function from B to A that "undoes" the action of f; that is, it sends each element of B back to the element of A that it came from. This function is called the *inverse* of f.

3.1.19 DEFINITION.   Let $f : A \to B$ be a bijection. The **inverse function** of the given function is the function $f^{-1} : B \to A$ defined by

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

NOTE : f^{-1} does *not* denote the reciprocal $1/f$.

3.1.20 EXAMPLE.   Find the inverse of the bijective function $f : \{1, 2, 4, 8\} \to \{0, 1, 2, 3\}$ given by

$$1 \mapsto 0, \ 2 \mapsto 1, \ 4 \mapsto 2, \ 8 \mapsto 3\,.$$

SOLUTION :   We have (by reversing the arrows) :

$$f^{-1} : \quad 0 \mapsto 1, \ 1 \mapsto 2, \ 2 \mapsto 4, \ 3 \mapsto 8\,.$$

3.1.21 EXAMPLE.   Let $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 3x + 4$. Find the inverse function f^{-1}.

SOLUTION :   The given function is a one-to-one correspondence (why ?), and so it makes sense to ask for the inverse function $f^{-1} : \mathbb{R} \to \mathbb{R}$. Let $x \in \mathbb{R}$. Then $f(f^{-1}(x)) = x \iff 3f^{-1}(x) + 4 = x$. Solving for $f^{-1}(x)$, we find that $f^{-1}(x) = \frac{x-4}{3}$. Thus $f^{-1} : \mathbb{R} \to \mathbb{R}, \quad x \mapsto \frac{x-4}{3}$.

Composition of functions

The notion of performing first one function and then another can be defined precisely.

3.1.22 DEFINITION.   Let $f : A \to B$ and $g : C \to D$, where $B \subseteq C$. Then the **composition** of g and f, denoted by $g \circ f$, is the function from A to D defined by

$$(g \circ f)(x) := g(f(x)), \quad x \in A.$$

(The symbol $g \circ f$ is read "g composite f").

In other words, $g \circ f$ is the function that assigns to the element $x \in A$ the element assigned by g to $f(x)$.

NOTE : (1) The notation $g \circ f$ means that we do f first and then g. It may seem strange that, although we evaluate f first, we write its symbol after g. Why? When we apply the function $g \circ f$ to an element $a \in A$, as in $(g \circ f)(a)$, the letter f is closer to a and "hits" it first :

$$a \mapsto g(f(a)).$$

(2) The domain of $g \circ f$ is the same as the domain of f :

$$\mathrm{dom}\,(g \circ f) = \mathrm{dom}\,(f).$$

(3) For the composition $g \circ f$ to make sense, every output of f must be an acceptable input to g. Properly said, we need $\mathrm{im}\,(f) \subseteq \mathrm{dom}\,(g)$.

(4) It is possible that $g \circ f$ and $f \circ g$ both make sense (are defined). It this situation, it may be the case that $g \circ f \neq f \circ g$ (are different functions).

3.1.23 EXAMPLE. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d\}$, $C = \{b, c, d\}$, and $D = \{\square, \diamond, \triangle, \bowtie, \heartsuit\}$. Let $f : A \to B$ and $g : C \to D$ be defined by

$$f : \quad 1 \mapsto b,\ 2 \mapsto b,\ 3 \mapsto c,\ 4 \mapsto d,\ 5 \mapsto d,$$

and

$$g : \quad b \mapsto \diamond,\ c \mapsto \bowtie,\ d \mapsto \heartsuit.$$

We can identify these functions with their graphs, and write them as sets of ordered pairs of elements :

$$f = \{(1, b),\ (2, b),\ (3, c),\ (4, d),\ (5, d)\}$$

and

$$g = \{(b, \diamond),\ (c, \bowtie),\ (d, \heartsuit)\}.$$

Then $g \circ f$ is the function

$$g \circ f = \{(1, \diamond),\ (2, \diamond),\ (3, \bowtie),\ (4, \heartsuit),\ (5, \heartsuit)\}.$$

For example,

$$(g \circ f)(2) = g(f(2)) = g(b) = \diamond.$$

So $(2, \diamond) \in g \circ f$.

3.1.24 EXAMPLE.   Let $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^2 + 2$ and let $g : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 3x + 4$. Then $g \circ f : \mathbb{R} \to \mathbb{R}$ is the function defined by

$$(g \circ f)(x) = g(f(x)) = g(x^2 + 2) = 3(x^2 + 2) + 4 = 3x^3 + 10$$

and $f \circ g : \mathbb{R} \to \mathbb{R}$ is the function defined by

$$(f \circ g)(x) = f(g(x)) = f(3x + 4) = (3x + 4)^2 + 2 = 9x^2 + 24x + 18.$$

We can see clearly that $g \circ f \neq f \circ g$.

We have seen that composition of functions does not satisfy the *commutativity property*. It does, however, satisfy the *associativity property*.

3.1.25 PROPOSITION.   *Let $f : A \to B$, $g : B' \to C$, and $h : C' \to D$, where $B \subseteq B'$, $C \subseteq C'$. Then*

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

SOLUTION :   We need to show that the functions $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are the same. First, we see that the domains of the functions are the same, namely the set A. Second, we check that for any $a \in A$, the functions produce the same value. We have

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

Hence $h \circ (g \circ f) = (h \circ g) \circ f$. $\square$

It is often important to decide whether a function is one-to-one or onto. In this regard, the following results concerning the composition of functions are useful.

3.1.26 PROPOSITION. *Let $f : A \to B$ and $g : C \to D$, where $B \subseteq C$.*

    (a) If f and g are injections, then $g \circ f$ is also an injection.

    (b) If f and g are surjections, then $g \circ f$ is also a surjection.

    (c) If $g \circ f$ is an injection, then f is an injection.

    (d) If $g \circ f$ is a surjection, then g is a surjection.

3.1.27 EXAMPLE. Let $f : A \to B$ and $g : B \to A$. Show that if $f \circ g : B \to B$ is the identity function on B and $g \circ f : A \to A$ is the identity function on A, then f and g are bijections, f is the inverse function of g, and g is the inverse function of f.

SOLUTION : We first note that it follows from PROPOSITION 2.3.29 (c) and (d) that both f and g are bijections. We show that g is the inverse function of f, and a similar argument shows that f is the inverse function of g. Let $y \in B$ and let $x = g(y)$. We must show that x is the element of A for which $f(x) = y$. But

$$f(x) = f(g(y)) = f \circ g(y) = id_B(y) = y.$$

3.1.28 DEFINITION. A function $f : A \to B$ is **invertible** provided there is a function $g : B \to A$ such that $f \circ g : B \to B$ is the identity function on B and $g \circ f : A \to A$ is the identity function on A.

NOTE : A function $f : A \to B$ is invertible if and only if it is a bijection.

3.1.29 EXAMPLE. Show that the function $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 3x + 4$ is a bijection.

SOLUTION : Define $g : \mathbb{R} \to \mathbb{R}, \quad x \mapsto (x - 4)/3$. Let $x \in \mathbb{R}$. Then

$$(g \circ f)(x) = g(f(x)) = g(3x + 4) = \frac{(3x + 4) - 4}{3} = x$$

and

$$(f \circ g)(x) = f(g(x)) = f\left(\frac{x - 4}{3}\right) = 3\left(\frac{x - 4}{3}\right) + 4 = (x - 4) + 4 = x.$$

Therefore, $f : \mathbb{R} \to \mathbb{R}$ is invertible, and thus it is a bijection.

NOTE : Alternatively, one can show that the function f is both one-to-one and onto. This can be done, for instance, by showing that for any given $y \in \mathbb{R}$, the *equation* (in x) $y = 3x + 4$ has a *unique* solution.

3.2 Specific functions

Let $f : A \to B$ be a function. In the general case, the domain A and the codomain B of such a function are completely arbitrary sets. However, important classes of functions exist for specific sets A, B. We shall describe briefly some of these *specific* functions.

(i) $B = \mathbb{R}$. Functions $f : A \to \mathbb{R}$ are referred to as **real-valued functions**. The domain A of f is an arbitrary set; in other words, the inputs of a real-valued function are *not* necessary numbers : they could be any type of objects (e.g. people, books, triangles, sets or even sets of sets).

Two real-valued functions f and g can be combined to form new functions $f + g$, $f - g$, fg, and f/g in a manner similar to the way we add, subtract, multiply, and divide real numbers.

3.2.1 DEFINITION. Let $f : A_1 \to \mathbb{R}$ and $g : A_2 \to \mathbb{R}$, where $A_1 \cap A_2 \neq \emptyset$. Then

$f + g : A_1 \cap A_2 \to \mathbb{R}$ is defined by $(f + g)(x) := f(x) + g(x)$;

$f - g : A_1 \cap A_2 \to \mathbb{R}$ is defined by $(f - g)(x) := f(x) - g(x)$;

$f \cdot g : A_1 \cap A_2 \to \mathbb{R}$ is defined by $(f \cdot g)(x) := f(x) \cdot g(x)$;

$\dfrac{f}{g} : A_1 \cap A_2 \setminus \{x \in A_1 \cap A_2 \mid g(x) \neq 0\} \to \mathbb{R}$ is defined by $\left(\dfrac{f}{g}\right)(x) := \dfrac{f(x)}{g(x)}$.

3.2.2 EXAMPLE. Let $f : [0, \infty) \to \mathbb{R}$, $x \mapsto \sqrt{x} + 3$ and let $g : (-\infty, 4] \to \mathbb{R}$, $x \mapsto \sqrt{4 - x} - 1$. Then $(-\infty, 4] \cap [0, \infty) = [0, 4]$ and

$f + g : [0, 4] \to \mathbb{R}$ is defined by $(f + g)(x) = \sqrt{x} + \sqrt{4 - x} + 2$;

$f - g : [0, 4] \to \mathbb{R}$ is defined by $(f - g)(x) = \sqrt{x} - \sqrt{4 - x} + 4$;

$f \cdot g : [0, 4] \to \mathbb{R}$ is defined by $(f \cdot g)(x) = \sqrt{x(4 - x)} + 3\sqrt{4 - x} - \sqrt{x} - 3$;

$\dfrac{f}{g} : [0, 3) \cup (3, 4] \to \mathbb{R}$ is defined by $\left(\dfrac{f}{g}\right)(x) = \dfrac{\sqrt{x} + 3}{\sqrt{4 - x} - 1}$.

Real-valued functions $f : A \to \mathbb{R}$ where $A \subseteq \mathbb{R}$ are usually called *real-valued functions of one real variable* (or **real functions**, for short). The simplest types of real functions are the **polynomials**, of the form

$$x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

with *coefficients* $a_0, a_1, \ldots, a_n$. Next come the **rational functions**, such as

$$x \mapsto \frac{1}{x}, \quad x \mapsto \frac{1}{1 + x^2}, \quad x \mapsto \frac{2x + 1}{x^4 + 3x^2 + 5}$$

which are quotients of polynomials, and the *trigonometric functions* sin, cos, tan. Other basic real functions are the *exponential function* $\exp_a$, the *power function* $(\cdot)^a$, the *logarithmic function* $\log_a$, and the *inverse trigonometric functions* arcsin, arccos, arctan.

NOTE : These real functions (which are commonly referred to as **elementary functions**) are formally defined and their remarkable properties are studied in *Calculus* courses.

The **absolute value** (or **modulus**) **function** is the real function

$$| \cdot | : \mathbb{R} \to \mathbb{R}, \quad x \mapsto |x| := \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

For example, $|1.5| = 1.5$, $|-0.7| = 0.7$, $|0| = 0$.

NOTE :   Geometrically, the absolute value of (the number) x represents the *distance* from the origin of the real line to the point (on the real line) with *coordinate* x.

The absolute value function has some remarkable properties (see APPENDIX B).

3.2.3 EXAMPLE.   There is a function $\{\cdot\}_* : \mathbb{R} \to \mathbb{R}$ which associates to each real number x the *distance to the closest integer* (on the real line); that is,

$$\{x\}_* := \min\{|x - n| \mid n \in \mathbb{Z}\}.$$

(ii) $B = \mathbb{Z}$.   Functions $f : A \to \mathbb{Z}$ are special cases of real-valued functions. Some of these functions play important roles in discrete mathematics. The *floor* and *ceiling functions* are fundamental.

3.2.4 DEFINITION.   The **floor function** is the function

$$\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}.$$

$\lfloor x \rfloor$ is the greatest integer which is less than or equal to x; for example, $\lfloor 1.5 \rfloor = 1$, $\lfloor -0.7 \rfloor = -1$, $\lfloor \pi \rfloor = 3$.

3.2.5 DEFINITION.   The **ceiling function** is the function

$$\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lceil x \rceil := \min\{n \in \mathbb{Z} \mid n \geq x\}.$$

$\lceil x \rceil$ is the least integer which is greater than or equal to x; for example, $\lceil 1.5 \rceil = 2$, $\lceil -0.7 \rceil = 0$, $\lceil \pi \rceil = 4$.

Both these functions have some remarkable properties (see APPENDIX B). Other interesting (and useful) examples are given in what follows.

3.2.6 EXAMPLES.

1. The **signum function** is the function

$$\text{sgn} : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \begin{cases} \dfrac{x}{|x|} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

2. The **Dirichlet function** is the function

$$\delta : \mathbb{R} \to \{0, 1\}, \quad x \mapsto \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q}. \end{cases}$$

3. The **unit-step function** (at $a \in \mathbb{R}$) is the function

$$u_a : \mathbb{R} \to \{0, 1\}, \quad x \mapsto u_a(x) := \begin{cases} 1 & \text{if } x \geq a \\ 0 & \text{if } x < a. \end{cases}$$

NOTE : Both the Dirichlet function and the unit-step function are examples of *characteristic functions*. The general concept can be described as follows. Let X be a (fixed) set and let 2^X denote the power set (i.e. the set consisting of all the subsets, including the empty set) of X. Given $A \in 2^X$, the **characteristic function** of A is the function

$$\varphi_A : X \to \{0, 1\}, \quad x \mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

Equal subsets (of X) have, by definition, equal corresponding characteristic functions. It turns out that there is a one-to-one correspondence between the power set 2^X and the set $\{0, 1\}^X$ (of all functions $X \to \{0, 1\}$) : the function

$$\Phi : 2^X \to \{0, 1\}^X, \quad A \mapsto \varphi_A$$

is a *bijection*. In other words, each (sub)set may be viewed as a function, its characteristic function, and any such function determines uniquely the (sub)set; this allows us to *identify*, whenever appropriate, a (sub)set with its characteristic function. We can see that $\delta = \varphi_{\mathbb{Q}}$ (the Dirichlet function δ is the characteristic function of the set

of rational numbers) and $u_a = \varphi_{[a,\infty)}$ (the unit-step function u_a is the characteristic function of the interval $[a, \infty)$ of real numbers).

(iii) $A \subseteq \mathbb{N}$ Functions $f : A \to B$ where A is an infinite subset of $\mathbb{N}$ (usually either the set $\mathbb{N}$ or the set of positive integers $\mathbb{Z}^+$) are called **sequences** (of elements of B).

3.2.7 EXAMPLE.   The *sequence*

$$1, \; -\frac{1}{2}, \; \frac{1}{3}, \; -\frac{1}{4}, \; \cdots, \; \frac{(-1)^n}{n+1}, \; \cdots$$

can be thought of as the function

$$f : \mathbb{N} \to \mathbb{R}, \quad n \mapsto f(n) := \frac{(-1)^n}{n+1}.$$

Sequences of numbers will be encountered later (see chapters 4-6).

(iv) $A = B$.   *Bijective* functions $f : A \to A$ where A is an arbitrary set are called **permutations** (or **symmetries**) of A. The set $\mathsf{Sym}\,(A)$ of all permutations of A has a remarkable algebraic structure and plays a major role in many areas of mathematics.

NOTE :   When the set A (usually infinite) is equipped with some "geometric structure", it is customary to refer to a permutation (of A) as a *transformation* on the "space" A.

The case when A is a *finite* set will be considered in the following section.

3.3   Permutations

When dealing with *discrete* (usually finite) objects, a permutation is best viewed as a *rearrangement* of objects. This simple idea can be made precise.

Let X be a finite, *ordered* set with n elements. These are our distinct objects we want to "rearrange". We may assume that $X = \{1, 2, 3, \cdots, n\}$. (We identify each object with its "position" in the ordered set : the first, second, third, etc.)

3.3.1 DEFINITION.   A bijection $\alpha : \{1, 2, 3, \cdots, n\} \rightarrow \{1, 2, 3, \cdots, n\}$ is called a **permutation on n elements**.

The set of all permutations on n elements is denoted by S_n; it is usually referred to as the *symmetric group* of order n.

3.3.2 EXAMPLE.   Let $X = \{1, 2, 3, 4, 5\}$ and let $\alpha : X \rightarrow X$ be defined by

$$\alpha = \{(1, 2),\ (2, 4),\ (3, 1),\ (4, 3),\ (5, 5)\}.$$

Since α is a one-to-one and onto function (i.e. a bijection) from X to X, it is a permutation (on 5 elements); we write $\alpha \in S_5$.

Let α be an arbitrary permutation on n elements (or a permutation of *degree n*). We can express α as a $2 \times n$ array of integers. The top row contains the integers 1 through n in their usual order, and the bottom row contains $\alpha(1)$ through $\alpha(n)$:

$$\alpha = \begin{bmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{bmatrix}.$$

NOTE :   (1)   The numbers $\alpha(1)$, $\alpha(2)$, ..., $\alpha(n)$ are the numbers $1, 2, \ldots, n$ in some order.

(2)   The top row in the *array notation* is not strictly necessary. We could express the permutation α simply by reporting the bottom row; all the information we need is there. We could write $\alpha = \begin{bmatrix} \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{bmatrix}$. This notation is reasonable only when n is small. On the other hand, this is a reasonable way to store a permutation into a computer.

3.3.3 EXAMPLE.   For the permutation (on 5 elements)

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix}$$

$\alpha(1) = 2$, $\alpha(2) = 4$, $\alpha(3) = 1$, $\alpha(4) = 3$ and $\alpha(5) = 5$.

3.3.4 EXAMPLE.   The identity function $id_{\{1,2,\ldots,n\}}$ is a permutation (on n elements) and therefore in S_n. We usually denote the **identity permutation** by the lowercase Greek letter ι (iota). Thus

$$\iota := \begin{bmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{bmatrix} \in S_n.$$

Permutations (on the same number of elements) can be *multiplied* by consecutive application. Let $\alpha, \beta \in S_n$. The function

$$\beta\alpha : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}, \quad k \mapsto \beta\left(\alpha(k)\right)$$

is the **product** (or **composition**) of the permutations α and β.

NOTE :   Permutations are functions and $\beta\alpha$ is just the composite function $\beta \circ \alpha$. Permutation α acts first and then permutation β acts on the result of α.

The following result lists important properties of S_n.

3.3.5 PROPOSITION.   *Consider the set S_n. Then (for $\alpha, \beta, \gamma \in S_n$) :*

(G1) $\beta\alpha \in S_n$.

(G2) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

(G3) $\alpha\iota = \iota\alpha$.

(G4) $\alpha^{-1} \in S_n$ *and* $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \iota$.

NOTE :   The properties listed above may be summarized by saying that S_n is a *group* (with respect to the composition of permutations).

3.3.6 EXAMPLE.   The product of permutations

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

is

$$\begin{aligned} \beta\alpha &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}. \end{aligned}$$

Also

$$\begin{aligned} \alpha\beta &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}. \end{aligned}$$

NOTE :   The product of permutations is, in general, *not* commutative. More precisely, the symmetric group S_n is not commutative for $n \geq 3$.

If a permutation maps $a \mapsto b$, then its inverse maps $b \mapsto a$. Thus the inverse of the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{bmatrix}$$

is simply

$$\alpha^{-1} = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \\ 1 & 2 & \ldots & n \end{bmatrix}.$$

3.3.7 EXAMPLE.   Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 3 & 2 & 7 & 6 \end{bmatrix} \in S_7.$$

Find α^{-1}.

SOLUTION :   We have

$$\begin{aligned} \alpha^{-1} &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 3 & 2 & 7 & 6 \end{bmatrix}^{-1} = \begin{bmatrix} 4 & 5 & 1 & 3 & 2 & 7 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 1 & 2 & 7 & 6 \end{bmatrix}. \end{aligned}$$

Cycle notation

For another look at permutations we consider the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix}$, an element of S_5. The **cycle notation** for α is as follows :

$$\alpha = (1, 2, 4, 3)(5).$$

Let us explain what this notation means. The two lists in parentheses, $(1, 2, 4, 3)$ and (5), are called **cycles**. The cycle $(1, 2, 4, 3)$ means that

$$1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1 \,.$$

In other words,

$$\alpha(1) = 2, \ \alpha(2) = 4, \ \alpha(4) = 3, \quad \text{and} \quad \alpha(3) = 1.$$

Each number k is followed by $\alpha(k)$. Taken literally, if we began the cycle with 1, we would go on for ever :

$$(1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, \dots).$$

Instead, when we reach the first 3, we write a close parentheses meaning "return to the start of the cycle". Thus $(1, \ \dots, \ 3)$ means that $\alpha(3) = 1$.

What does the lonely (5) mean ? It means $\alpha(5) = 5$.

NOTE :   (1)   A cycle is a permutation. For example,

$$(1, 2, 4, 3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix} \quad \text{and} \quad (5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix} .$$

(2)   A cycle may be written starting with *any* of its elements. For example,

$$(1, 2, 4, 3) = (2, 4, 3, 1) = (4, 3, 1, 2) = (3, 1, 2, 4).$$

However, the *cyclic order* must be kept. For example,

$$(1, 2, 4, 3) \neq (2, 1, 4, 3).$$

(3)   A cycle $(a_1, a_2, \dots, a_k)$ is called a cycle of length k (or an k-cycle).

3.3.8 EXAMPLE.   Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 6 & 3 & 8 & 1 & 4 & 9 \end{bmatrix} \in S_9.$$

Express α in cycle notation.

SOLUTION :   Note that $\alpha(1) = 2$, $\alpha(2) = 7$, and $\alpha(7) = 1$. So far we have

$$\alpha = (1, 2, 7) \cdots .$$

The first element we have not considered is 3. Restarting from 3, we have $\alpha(3) = 5$ and $\alpha(5) = 3$, so the next cycle is $(3, 5)$. So far we have

$$\alpha = (1, 2, 7)(3, 5) \cdots .$$

The next element we have yet to consider is 4. We have $\alpha(4) = 6$, $\alpha(6) = 8$, and $\alpha(8) = 4$ to complete the cycle. The next cycle is $(4, 6, 8)$. Thus far we have

$$\alpha = (1, 2, 7)(3, 5)(4, 6, 8) \cdots .$$

Finally, we have $\alpha(9) = 9$, so the last cycle is just (9). The permutation α in cyclic notation is

$$\alpha = (1, 2, 7)(3, 5)(4, 6, 8)(9).$$

NOTE :   Since a cycle of length 1 is just the identity permutation, it can be dropped (as long as the degree of the permutation is remembered). For example,

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{bmatrix} = (1, 3)(2)(4)(5) = (1, 3) \in S_5.$$

Does the cycle notation method work for all permutations (on n elements) ? The answer is *yes*. More precisely, *we can write any permutation $\alpha \in S_n$ as a product of pairwise disjoint cycles*; that is, no two cycles have common elements.

NOTE :   Any two disjoint cycles commute.

3.3.9 EXAMPLE.   Consider the cycles $(1, 2)$, $(1, 3)$, $(3, 4) \in S_4$. Then

$$(1, 2)(3, 4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = (3, 4)(1, 2).$$

Does $(1, 2)(1, 3) = (1, 3)(1, 2)$?

SOLUTION :   The answer is *no*. Indeed,

$$(1, 2)(1, 3) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} = (1, 3)(1, 2).$$

We can say more. Is it possible to write the same permutation as a product of disjoint cycles in two different ways ? At first glance, the answer is *yes*. For example,

$$\alpha = (1, 2, 7)(3, 5)(4, 6, 8)(9) = (5, 3)(6, 8, 4)(9)(7, 1, 2) \,;$$

both represent the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 6 & 3 & 8 & 1 & 4 & 9 \end{bmatrix}$. However, on closer inspection, we see that the two representations of α have the same cycles; the cycles $(1, 2, 7)$ and $(7, 1, 2)$ both say the same thing, namely, $\alpha(1) = 2$, $\alpha(2) = 7$, and $\alpha(7) = 1$. One can prove that *there is only one way to write* α *as a product of disjoint cycles*. The following general result holds.

3.3.10 PROPOSITION.   *Every permutation on a finite set can be decomposed into pairwise disjoint cycles. Furthermore, this decomposition is unique up to rearranging the cycles and the cyclic order of the elements within cycles.*

The cycle notation is handy for doing calculations with permutations (on a finite set). The most basic operations are taking the inverse of a permutation and the composition of two permutations.

Let us begin with calculating the inverse of a permutation. An important observation is the following : if $(a, b, c, \dots)$ is a cycle, then its inverse is

$(\ldots, c, b, a)$. Since any permutation $a \in S_n$ decomposes into pairwise disjoint cycles, we get a simple rule for calculating the inverse of α :

$$\alpha = \alpha_1 \alpha_2 \cdots \alpha_r \quad \Rightarrow \quad \alpha^{-1} = \alpha_1^{-1} \alpha_2^{-1} \cdots \alpha_r^{-1}.$$

3.3.11 EXAMPLE.   Let $\alpha = (1, 2, 7, 9, 8)(5, 6, 3)(4) \in S_9$. Calculate α^{-1}.

SOLUTION :   We have

$$\alpha^{-1} = (8, 9, 7, 2, 1)(3, 6, 5)(4) = (8, 9, 7, 2, 1)(3, 6, 5).$$

Let us explore how to compute the composition of two permuations.

3.3.12 EXAMPLE.   Let $\alpha, \beta \in S_9$ be given by

$$\alpha = (1, 3, 5)(4, 6)(2, 7, 8, 9) \quad \text{and} \quad \beta = (1, 4, 7, 9)(2, 3)(6, 8).$$

Compute $\alpha\beta$.

SOLUTION :   We calculate $\alpha\beta(k)$ for all $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. We begin with $\alpha\beta(1)$. We have $\alpha\beta(1) = \alpha(4) = 6$. Thus far we can write

$$\alpha\beta = (1, 6, \ldots$$

To continue the cycle, we calculate $\alpha\beta(6)$. We have $\alpha\beta(6) = \alpha(8) = 9$. Now we have

$$\alpha\beta = (1, 6, 9, \ldots$$

Continuing in this fashion, we get

$$1 \mapsto 6 \mapsto 9 \mapsto 3 \mapsto 7 \mapsto 2 \mapsto 5 \mapsto 1$$

and we have completed a cycle ! Thus $(1, 6, 9, 3, 7, 2, 5)$ is a cycle of $\alpha\beta$. Notice that 4 is not on this cycle, so we start over computing $\alpha\beta(4)$. We get

$$4 \mapsto 8 \mapsto 4.$$

The two cycles $(1, 6, 9, 3, 7, 2, 5)$ and $(4, 8)$ exhaust all the elements of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and so we are finished. We have found

$$\alpha\beta = (1, 6, 9, 3, 7, 2, 5)(4, 8).$$

Transpositions

The simplest permutation is the identity permutation. The identity permutation ι maps every element into itself.

The next simplest type of permutation is a *transposition.* Transpositions map almost all elements to themselves, except that they exchange one pair of elements. For example,

$$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{bmatrix} = (2,5)$$

is a transposition (of degree 5). Thus

3.3.13 DEFINITION.   A **transposition** is a cycle of length 2.

We explore the expression of permutations as products of transpositions. There is a nice trick for converting a cycle into a composition of transpositions.

3.3.14 EXAMPLE.   Let $\pi = (1,2,3,4,5)$. Write π as a composition of transpositions.

SOLUTION :   We have

$$\pi = (1,2,3,4,5) = (1,5)(1,4)(1,3)(1,2).$$

3.3.15 EXAMPLE.   Let $\sigma = (1,2,3,4,5)(6,7,8)(10,11) \in S_{11}$. Write σ as a product of transpositions.

SOLUTION :   We have

$$\sigma = (1,5)(1,4)(1,3)(1,2)(6,8)(6,7)(10,11).$$

Let α be any permutation (on a finite set). Write α as a product of cycles. Using the technique from EXAMPLE 3.3.2, we can rewrite each of its cycles as a composition of transpositions. Because the cycles are pairwise disjoint, there is no effect of one cycle on another. Thus we can simply string together the transpositions for the various cycles into one long product of transpositions.

What about the identity permutation ι ? Can it also be represented as a product of transpositions ? Yes. We can write, for instance,

$$\iota = (1, 2)(1, 2).$$

Let us summarize what we have shown here.

3.3.16 PROPOSITION.   *Every permutation on a finite set can be decomposed into transpositions.*

The decomposition of permutations into transpositions is *not* unique ! For example, we can write

$$
\begin{aligned}
(1, 2, 3, 4) &= (1, 4)(1, 3)(1, 2) \\
&= (1, 2)(2, 3)(3, 4) \\
&= (1, 2)(1, 4)(2, 3)(1, 4)(3, 4).
\end{aligned}
$$

These ways of writing $(1, 2, 3, 4)$ are *not* simple rearrangements of one another. We see that they do not even have the same number of transpositions. However, they do have something in common. In all three cases, we used an odd number of transpositions.

The following important general result holds.

3.3.17 PROPOSITION.   *Let $\alpha \in S_n$. Let α be decomposed into transpositions as*

$$
\begin{aligned}
\alpha &= \tau_1 \tau_2 \cdots \tau_a \\
\alpha &= \sigma_1 \sigma_2 \cdots \sigma_b.
\end{aligned}
$$

Then a and b have the same parity; that is, they are both odd or even.

The key to proving this result is the following fact, given without proof (the proof, however, takes a little work !) : *If the identity permutation is written as a composition of transpositions, then that composition must use an even number of transpositions.*

PROOF (OF PROPOSITION 3.3.5) : Let α be a permutation decomposed (into transpositions) as

$$\begin{aligned} \alpha &= \tau_1 \tau_2 \cdots \tau_a \\ \alpha &= \sigma_1 \sigma_2 \cdots \sigma_b. \end{aligned}$$

Then we can write

$$\alpha^{-1} = \sigma_b \sigma_{b-1} \cdots \sigma_2 \sigma_1$$

and so

$$\iota = \alpha \alpha^{-1} = \tau_1 \tau_2 \cdots \tau_a \sigma_b \cdots \sigma_2 \sigma_1.$$

This is a decomposition of ι into $a + b$ transpositions, hence $a + b$ is even, and so a and b have the same parity. $\qquad\square$

The signature of a permutation

The foregoing result enables us to separate permutations into two disjoint categories: those that can be expressed as the composition of an even number of transpositions and those that can be expressed as the composition of an odd number of transpositions.

3.3.18 DEFINITION. Let α be a permutation on a finite set. We call α **even** provided it can be written as the composition of an even number of transpositions. Otherwise it can be written as the composition of an odd number of transpositions, in which case we call α **odd**.

The **signature** of a permutation $\alpha \in S_n$, denoted by $\operatorname{sgn}(\alpha)$, is $+1$ for even permutations and -1 for odd permutations.

3.3.19 EXAMPLE. What is the signature of $(1,2,3,4)$?

SOLUTION : We have

$$\operatorname{sgn}(1,2,3,4) = \operatorname{sgn}(1,4)(1,3)(1,2) = -1.$$

The function

$$h : S_n \to \{-1, 1\}, \qquad \alpha \mapsto \mathrm{sgn}(\alpha)$$

is clearly a surjection. Moreover, it preserves the "group structure"; that is, (for $\alpha, \beta \in S_n$)

$$h(\alpha\beta) = h(\alpha) \cdot h(\beta).$$

NOTE :   The set (in fact, *subgroup*) $A_n = h^{-1}(1)$ (of all even permutations on n elements) is referred to as the *alternating group* on n elements.

3.4   Exercises

Exercise 31 Recall the definitions of the floor function, the ceiling function, the absolute value function, and of the unit-step function. Then sketch the graph of

(a) $y = \lfloor x \rfloor$.

(b) $y = \lceil x \rceil$.

(c) $y = \lfloor x - 1 \rfloor$.

(d) $y = \lceil x - 1 \rceil$.

(e) $y = 1 + \lfloor x \rfloor$.

(f) $y = 2 - \lceil x \rceil$.

(g) $y = |\, x \,|$.

(h) $y = |\, x - 2 \,|$.

(i) $y = |\, x + 2 \,|$.

(j) $y = 1 - |\, x \,|$.

(k) $y = u_2(x)$.

(l) $y = u_0(x)$.

(m) $y = u_{-1}(x)$.

(n) $y = x^2 u_3(x)$.

(o) $y = 1 - u_1(x)$.

(p) $y = (1 - u_3(x))u_2(x)$.

Exercise 32 Investigate the following functions for injectivity, surjectivity, and bijectivity. If the function is bijective, find its inverse.

(a) $f : \mathbb{N} \to \mathbb{N}, \quad n \mapsto n^2 + 1$.

(b) $g : \mathbb{Z} \to \mathbb{Z}, \quad n \mapsto n^3$.

(c) $h : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lfloor x \rfloor$.

(d) $i : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lceil x \rceil$.

(e) $j : \mathbb{R} \to \mathbb{R}, \quad x \mapsto |x|$.

(f) $k : [0, \infty) \to [0, \infty), \quad x \mapsto |x|$.

(g) $l : (-\infty, 0] \to [0, \infty), \quad x \mapsto |x|$.

(h) $m : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^4$.

(i) $n : [0, \infty) \to [0, \infty), \quad x \mapsto x^4$.

(j) $u : \mathbb{R} \to \mathbb{R}, \quad x \mapsto \begin{cases} x^2, & \text{if } x \geq 0 \\ 2x, & \text{if } x < 0. \end{cases}$

(k) $v : (0, \infty) \to (0, \infty), \quad x \mapsto \dfrac{7x + 8}{8x + 7}$.

(l) $w : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{2\}, \quad x \mapsto \dfrac{2x + 1}{x - 2}$.

Exercise 33 Write down *all* functions $f : A \to B$ and then indicate which are one-to-one and which are onto.

(a) $A = \{1, 2, 3\}$ and $B = \{4, 5\}$.

(b) $A = \{1, 2\}$ and $B = \{3, 4, 5\}$.

(c) $A = \{1, 2\}$ and $B = \{3, 4\}$.

Exercise 34 Give an example of a function from $\mathbb{N}$ to $\mathbb{N}$ that is

(a) one-to-one but not onto ;

(b) onto but not one-to-one ;

(c) both one-to-one and onto (but different from the identity function) ;

(d) neither one-to-one nor onto.

Exercise 35 Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be two functions.

(a) If f and g are both one-to-one, is $f + g$ also one-to-one ?

(b) If f and g are both one-to-one, is $f \cdot g$ also one-to-one ?

(c) If f and g are both one-to-one, is $f \circ g$ also one-to-one ?

(d) If f and g are both onto, is $f + g$ also onto ?

(e) If f and g are both onto, is $f \cdot g$ also onto ?

(f) If f and g are both onto, is $f \circ g$ also onto ?

Justify your answers.

Exercise 36 Let

$$f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto ax + b \quad \text{and} \quad g : \mathbb{R} \to \mathbb{R}, \quad x \mapsto cx + d$$

where $a, b, c,$ and d are constants. Determine for which constants $a, b, c,$ and d it is true that $f \circ g = g \circ f$.

Exercise 37 Express the following permutations in cycle notation.

(a) $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{bmatrix}$.

(b) $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{bmatrix}$.

(c) $\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{bmatrix}$.

(d) $\gamma^2 := \gamma\gamma$, where γ is the permutation from part (c).

(e) γ^{-1}, where γ is the permutation from part (c).

(f) $\iota \in S_5$.

(g) $\delta = (1, 2)(2, 3)(3, 4)(4, 5)(5, 1)$.

Exercise 38 Let $\pi, \sigma, \tau \in S_9$ be given by

$$\begin{aligned} \pi &= (1)(2, 3, 4, 5)(6, 7, 8, 9), \\ \sigma &= (1, 3, 5, 7, 9, 2, 4, 6, 8), \\ \tau &= (1, 9)(2, 8)(3, 5)(4, 6)(7). \end{aligned}$$

Calculate :

(a) $\pi\sigma$; (b) $\sigma\pi$; (c) π^2; (d) π^{-1}; (e) σ^{-1}; (f) τ^2; (g) τ^{-1}.

Exercise 39 Find

    (a) $a, b, c, d,$ and e when

$$(1,3,4)(2,5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{bmatrix}.$$

    (b) $a, b,$ and c when

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{bmatrix} = (1, a, b)(3, c).$$

Exercise 40 Exhibit

    (a) the 6 elements of S_3 in cycle notation.

    (b) the 24 elements of S_4 in cycle notation.

Exercise 41 Prove or disprove :

    (a) For all $\alpha, \beta \in S_n,$ $\alpha\beta = \beta\alpha.$

    (b) If τ and σ are transpositions, then $\tau\sigma = \sigma\tau.$

    (c) For all $\alpha, \beta \in S_n,$ $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}.$

    (d) For all $\alpha, \beta \in S_n,$ $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}.$

Exercise 42 Let $\alpha, \beta, \gamma \in S_n.$

    (a) Prove that if $\alpha\beta = \beta,$ then $\alpha = \iota.$

    (b) Prove that if $\alpha\beta = \alpha\gamma,$ then $\beta = \gamma.$

Exercise 43 Write out the following products in cycle notation :

$$(1,2)(1,3), \quad (1,2)(1,3)(1,4), \quad (1,2)(1,3)(1,4)(1,5), \quad (1,2)(1,3)\cdots(1,n).$$

Exercise 44 Express each of the following permutations as products of transpositions :

$$(2,3,4), \quad (2,4,6,8), \quad (1,2)(3,4,5)(6,7,8,9), \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 8 & 3 & 1 & 5 & 7 & 4 & 2 \end{bmatrix}.$$

Exercise 45 For each of the permutations listed, write the permutation as a composition of transpositions, and then determine if the permutation is even or odd.

(a) $(1, 2, 3, 4, 5)$.

(b) $(1, 3)(2, 4, 5)$.

(c) $[(1, 3)(2, 4, 5)]^{-1}$.

(d) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix}$.

Chapter 4

Mathematical Induction

Topics :

1. SEQUENCES OF NUMBERS

2. SUMMATIONS

3. MATHEMATICAL INDUCTION

One of the tasks of mathematics is to discover and characterize patterns, such as those associated with processes that are repeated. The main mathematical structure used to study repeated processes is the *sequences*. An important mathematical tool used to verify conjectures about patterns is *mathematical induction*.

4.1 Sequences of numbers

Sequences are used to represent ordered collections, finite or infinite, of elements. To say that a collection of objects is *ordered* means that the collection has an identified first element, second element, third element, and so on. For the sake of simplicity, we may assume that the objects involved are all *numbers*. (Here, by number is meant any real number; that is, an element of the set $\mathbb{R}$.) A formal definition is given below.

4.1.1 DEFINITION.   A **sequence** (of numbers) is a real-valued function whose domain is an infinite subset of $\mathbb{N}$ (usually either the set $\mathbb{N}$ or $\mathbb{Z}^+$).

Let $a : N \subseteq \mathbb{N} \to \mathbb{R}, \quad n \mapsto a(n)$ be a sequence. It is customary to use the notation $(a_n)_{n \in \mathbb{N}}$ (or $(a_n)_{n \geq n_0}$ or, simply, (a_n)) to denote such a sequence, where a_n is called the nth **term** of the sequence.

4.1.2 EXAMPLE.   The terms of the sequence $(a_n)_{n \geq 1}$, where $a_n = 3 + (-1)^n$ are

$$3 + (-1)^1, \; 3 + (-1)^2, \; 3 + (-1)^3, \; 3 + (-1)^4, \; \ldots;$$

that is,

$$2, \; 4, \; 2, \; 4, \; \ldots.$$

4.1.3 EXAMPLE.   The terms of the sequence $\left(\frac{2n}{n+1}\right)_{n \geq 1}$ are

$$\frac{2 \cdot 1}{1 + 1}, \; \frac{2 \cdot 2}{2 + 1}, \; \frac{2 \cdot 3}{1 + 3}, \; \frac{2 \cdot 4}{1 + 4}, \; \ldots;$$

that is,

$$1, \; \frac{4}{3}, \; \frac{3}{2}, \; \frac{8}{5}, \; \ldots \ldots.$$

Sometimes the terms of a sequence are generated by some rule that does not explicitly identify the nth term of the sequence. In such cases, you may be required to discover a *pattern* in the sequence and to describe the nth term.

4.1.4 EXAMPLE.   Find a sequence $(a_n)_{n \in \mathbb{N}}$ whose first five terms are

$$\frac{1}{1}, \frac{2}{3}, \frac{4}{5}, \frac{8}{7}, \frac{16}{9}, \ldots$$

SOLUTION :   First, note that the numerators are successive powers of 2, and the denominators form the sequence of positive odd integers. By comparing a_n with n, we have the following pattern

$$\frac{2^0}{1}, \frac{2^1}{3}, \frac{2^2}{5}, \frac{2^3}{7}, \frac{2^4}{9}, \ldots, \frac{2^n}{2n+1}, \ldots$$

4.1.5 EXAMPLE.   Determine the nth term for a sequence whose first five terms are

$$-\frac{2}{1}, \frac{8}{2}, -\frac{26}{6}, \frac{80}{24}, -\frac{242}{120}, \ldots$$

SOLUTION :   Note that the numerators are 1 less than 3^n. Hence, we can reason that the numerators are given by the rule $3^n - 1$. Factoring the denominators produces

$$
\begin{aligned}
1 &= 1 \\
2 &= 1 \cdot 2 \\
6 &= 1 \cdot 2 \cdot 3 \\
24 &= 1 \cdot 2 \cdot 3 \cdot 4 \\
120 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 .
\end{aligned}
$$

This suggests that the denominators are represented by $n!$. Finally, because the signs alternate, we can write the nth term as

$$a_n = (-1)^n \left(\frac{3^n - 1}{n!} \right).$$

Finite sequences

An ordered collection of finitely many objects is usually referred to as a **list** (of terms) or a **string** (of symbols). We write lists (strings) by starting with an open paranthesis, followed by the elements of the list (string) separated by

commas, and finishing with a close parenthesis. For example, $(1, \emptyset, \mathbb{Z})$ is a list whose first term is number 1, whose second term is the empty set, and whose third term is the set of integers.

NOTE :   The order in which elements appear in a list (string) is significant. The string (a, b, c) is *not* the same as the string (b, c, a). Elements in a (list) string might be repeated.

The number of elements in a list (string) is called its **length**. For example, the string $(1, 0, 1, 0)$ is a string of length four (or a 4-string). Another term used for strings is *tuple*.

NOTE :   The string $s = (s_1, s_2, \ldots, s_n)$ is also denoted simply by $s_1 s_2 \cdots s_n$. Strings constructed only with the symbols 0 and 1 are called **bit strings**. For example, 00, 01, 10, 11 are (all the) bit strings of length two. Bit strings are widely used in discrete mathematics as well as in computer science.

It is clear that lists (strings or tuples) are in fact *finite* sequences of objects. The formal definition is given below.

4.1.6 DEFINITION.   For each positive integer n, the set $[n] := \{1, 2, 3, \ldots n\}$ is called an **initial segment** of $\mathbb{Z}^+$. A **finite sequence** is a function whose domain is an initial segment of $\mathbb{Z}^+$.

4.2   Summations

Consider a sequence (of numbers) $(a_n)_{n \in \mathbb{N}}$. In order to express the sum of the terms

$$a_p, a_{p+1}, a_{p+2}, \ldots, a_q \quad (p \leq q)$$

it is often convenient to use the *summation notation*; we write

$$\sum_{i=p}^{q} a_i$$

to represent

$$a_p + a_{p+1} + a_{p+2} + \cdots + a_q.$$

NOTE :   The variable i is called the **index of summation**, and the choice of the letter i is arbitrary; thus, for instance,

$$\sum_{i=p}^{q} a_i = \sum_{j=p}^{q} a_j = \sum_{k=p}^{q} a_k.$$

The uppercase Greek letter *sigma* (Σ) is used to denote summation.

Here, the index of summation runs through *all* integers starting with the **lower limit** p and ending with the **upper limit** q. (There are $q - p + 1$ terms in the summation.)

4.2.1 EXAMPLE.   Find the value of the sum

$$S_1 = \sum_{i=0}^{4} (-2)^i.$$

SOLUTION :   We have

$$\begin{aligned}
S_1 = \sum_{i=0}^{4} (-2)^i &= (-2)^0 + (-2)^1 + (-2)^2 + (-2)^3 + (-2)^4 \\
&= 1 + (-2) + 4 + (-8) + 16 \\
&= 11.
\end{aligned}$$

4.2.2 EXAMPLE.   Compute the sum

$$S_2 = \sum_{j=0}^{4} (2j + 1)^2.$$

SOLUTION :   We have

$$\begin{aligned}
S_2 = \sum_{j=0}^{4} (2j + 1)^2 &= 1^2 + 3^2 + 5^2 + 7^2 + 9^2 \\
&= 1 + 9 + 25 + 49 + 81 \\
&= 165.
\end{aligned}$$

4.2.3 EXAMPLE. Evaluate the following *double* sum

$$\sum_{i=1}^{3}\sum_{j=1}^{4} ij.$$

SOLUTION : We have

$$
\begin{aligned}
\sum_{i=1}^{3}\sum_{j=1}^{4} ij &= \sum_{i=1}^{3}(i + 2i + 3i + 4i) \\
&= \sum_{i=1}^{3} 10i \\
&= 10 + 20 + 30 \\
&= 60.
\end{aligned}
$$

Some useful identities (formulas)

4.2.4 EXAMPLE. Find explicit formulas for the sums

$$S_n^{(k)} = \sum_{i=1}^{n} i^k \quad \text{for} \ \ k = 1, 2.$$

SOLUTION : We calculate first

$$S_n^{(1)} = \sum_{i=1}^{n} i = 1 + 2 + \cdots + n.$$

We write the sum in two ways

$$
\begin{aligned}
S_n^{(1)} &= 1 + 2 + \cdots + (n-1) + n \\
S_n^{(1)} &= n + (n-1) + \cdots + 2 + 1.
\end{aligned}
$$

On adding, we see that each pair of numbers in the same column yields the sum $n + 1$ and since there are n columns in all, it follows that

$$2S_n^{(1)} = n(n+1),$$

and hence

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

We have obtained the formula (the sum of the first n natural numbers) :

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

Next, we calculate

$$S_n^{(2)} = \sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \cdots + n^2.$$

Consider the identity

$$(i+1)^3 = i^3 + 3i^2 + 3i + 1.$$

By making $i = n, n-1, n-2, \ldots, 2, 1$ we get

$$\begin{aligned}
(n+1)^3 &= n^3 + 3n^2 + 3n + 1 \\
n^3 &= (n-1)^3 + 3(n-1)^2 + 3(n-1) + 1 \\
(n-1)^3 &= (n-2)^3 + 3(n-2)^2 + 3(n-2) + 1 \\
&\vdots \\
3^3 &= 2^3 + 3 \cdot 2^2 + 3 \cdot 2 + 1 \\
2^3 &= 1^3 + 3 \cdot 1^2 + 3 \cdot 1 + 1.
\end{aligned}$$

Adding up, we have

$$(n+1)^3 + S_n^{(3)} - 1 = S_n^{(3)} + 3S_n^{(2)} + 3S_n^{(1)} + n$$

or

$$3S_n^{(2)} = (n+1)^3 - (n+1) - \frac{3n(n+1)}{2}$$

and hence

$$\begin{aligned}
S_n^{(2)} &= \frac{(n+1)\left[2(n+1)^2 - 2 - 3n\right]}{6} \\
&= \frac{(n+1)(2n^2 + n)}{6} \\
&= \frac{n(n+1)(2n+1)}{6} \, .
\end{aligned}$$

We have obtained the formula (the sum of the first n squares) :

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

NOTE : Similarly, using the identity

$$(i+1)^4 = i^4 + 4i^3 + 6i^2 + 4i + 1 \, ,$$

we can derive an explicit formula for $S_n^{(3)}$; that is, the formula (the sum of the first n cubes) :

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

4.2.5 EXAMPLE.   Find an explicit formula for

$$A = a + (a+r) + (a+2r) + \cdots + (a+nr) = \sum_{i=0}^{n}(a+ir)$$

(the sum of the first $n+1$ terms of a **arithmetic progression** with initial term a and *ratio* r).

SOLUTION :   We have

$$
\begin{aligned}
A &= \sum_{i=0}^{n}(a+ir) \\
&= \sum_{i=0}^{n} a + r \sum_{i=0}^{n} i \\
&= (n+1)a + r\frac{n(n+1)}{2} \\
&= \frac{(n+1)(2a+rn)}{2} \\
&= \frac{n+1}{2}\left[a + (a+rn)\right].
\end{aligned}
$$

Thus

$$a + (a+r) + (a+2r) + \cdots + (a+nr) = \frac{n+1}{2}\left[a + (a+rn)\right].$$

4.2.6 EXAMPLE. Find an explicit formula for

$$G = a + ar + ar^2 + \cdots + ar^n = \sum_{i=0}^{n} ar^i, \quad r \neq 1$$

(the sum of the first $n + 1$ terms of a **geometric progression** with initial term a and *ratio r*).

SOLUTION : We have

$$
\begin{aligned}
rG & = r \sum_{i=0}^{n} ar^i \\
& = \sum_{i=0}^{n} ar^{i+1} \\
& = \sum_{k=1}^{n+1} ar^k \\
& = \sum_{k=0}^{n} ar^k + (ar^{n+1} - a) \\
& = G + (ar^{n+1} - a).
\end{aligned}
$$

Thus

$$rG = G + (ar^{n+1} - a),$$

and by solving for G we get

$$\boxed{a + ar + ar^2 + \cdots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1}, \quad r \neq 1.}$$

4.3 Mathematical induction

Mathematical induction is an important proof technique that can be used to prove statements of the form $\forall n \; P(n)$, where the universe of discourse (of the predicate $P(n)$) is the set of natural numbers. It is based on a principle, called the **principle of mathematical induction**.

Principle of Mathematical Induction : *Let S be a subset of $\mathbb{N}$ such that*

- *$0 \in S$;*

- *for all n, if $n \in S$ then $n + 1 \in S$.*

Then $S = \mathbb{N}$.

To visualize the idea of mathematical induction, imagine a collection of dominoes positioned one behind the other in such a way that if any given domino falls backward, it makes the one behind him fall backward also. Then imagine that the first domino falls backward. What happens ? ... They all fall down !

NOTE : Strictly speaking, the validity of the principle of mathematical induction is an *axiom.* This is why it is referred to as the *principle* of mathematical induction rather than as a theorem.

Let $P(n)$ be a predicate whose universe of discourse is $\mathbb{N}$, and let S be the *truth set* of $P(n)$, that is $S := \{n \in \mathbb{N} \,|\, P(n) \text{ is true}\}$. Based on the principle of mathematical induction, a **proof by mathematical induction** that $P(n)$ is true for every natural number n (that is, $S = \mathbb{N}$) consists of two steps :

1. *Basis step.* The property $P(0)$ is shown to be true.

2. *Inductive step.* The implication $P(n) \to P(n+1)$ is shown to be true for every $n \in \mathbb{N}$.

When we complete both steps of a proof by mathematical induction, we have proved that $P(n)$ is true for all natural numbers n; that is, we have shown that the proposition $\forall n \, P(n)$ is true.

NOTE : (1) This proof technique is based on the tautology

$$P(0) \wedge \forall n \, (P(n) \to P(n + 1)) \to \forall n \, P(n).$$

(2)   To prove the implication $P(n) \to P(n+1)$ is true for every $n \in \mathbb{N}$, we need to show that $P(n+1)$ *cannot* be false when $P(n)$ is true ; this can be accomplished by assuming that $P(n)$ is true and showing that *under this premise* $P(n+1)$ must also be true.

(3)   The principle of mathematical induction is equally valid if, instead of starting with 0, we (1) start with a given natural number a, (2) show that $a \in S$, and (3) show that, if $a \in S$ and $n \geq a$, then $n+1 \in S$. When we do this we will know that every natural number greater than or equal to a belongs to the set S.

4.3.1 EXAMPLE.   Use mathematical induction to prove that

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

for each positive integer n.

SOLUTION :   Let $P(n)$ be the predicate

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

We shall prove by induction that the proposition $\forall n\ P(n)$ is true.

BASIS STEP : $P(1)$ is true, since $1 = \frac{1(1+1)}{2}$.

INDUCTIVE STEP :   Assume that $P(n)$ is true. That is, assume that

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

Under this assumption, we must show that $P(n+1)$ is true, namely, that

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

Adding $n+1$ to both sides of the equality in $P(n)$, it follows that

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

The last equality shows that $P(n+1)$ is true.

This completes the proof by induction.

4.3.2 EXAMPLE.   Use mathematical induction to prove that, for each natural number $n \geq 5$, $n^2 < 2^n$.

SOLUTION :   Let $P(n)$ denote the predicate "$n^2 < 2^n$", where the universe of discourse is the set $\{n \in \mathbb{N} \,|\, n \geq 5\}$. We shall prove by induction that the proposition $\forall n \, P(n)$ is true.

BASIS STEP : $P(5)$ is true, since $5^2 < 2^5$.

INDUCTIVE STEP :   Assume that $P(n)$ is true. That is, assume that

$$n^2 < 2^n.$$

Under this assumption, we want to show that

$$(n+1)^2 < 2^{n+1}.$$

Now

$$(n+1)^2 = n^2 + 2n + 1 \quad \text{and} \quad 2^{n+1} = 2 \cdot 2^n$$

so we want to show that

$$n^2 + 2n + 1 < 2 \cdot 2^n.$$

Since $n^2 < 2^n$, $2n^2 < 2 \cdot 2^n$. Hence, it is sufficient to show that

$$n^2 + 2n + 1 < 2n^2.$$

But this inequality is equivalent to

$$1 < n(n-2)$$

which is obviously true, since $n \geq 5$. This completes the proof by induction.

4.3.3 EXAMPLE.   Prove by induction that, for each positive integer n, $7^n - 3^n$ is divisible by 4.

SOLUTION :   Let $P(n)$ denote the predicate "$7^n - 3^n$ is divisible by 4", where the universe of discourse is the set of positive integers. We shall prove by induction that the proposition $\forall n \, P(n)$ is true.

BASIS STEP : $P(1)$ is true, since $7 - 3$ is divisible by 4.

INDUCTIVE STEP :   We assume that

$$7^n - 3^n \quad \text{is divisible by 4}$$

and want to show that

$$7^{n+1} - 3^{n+1} \quad \text{is divisible by 4.}$$

We write

$$
\begin{aligned}
7^{n+1} - 3^{n+1} &= 7 \cdot 7^n - 3 \cdot 3^n \\
&= 7 \cdot 7^n - 7 \cdot 3^n + 7 \cdot 3^n - 3 \cdot 3^n \\
&= 7(7^n - 3^n) + 4 \cdot 3^n.
\end{aligned}
$$

Since $7(7^n - 3^n)$ and $4 \cdot 3^n$ are divisible by 4 (why ?), $7^{n+1} - 3^{n+1}$ is divisible by 4. This completes the proof by induction.

4.3.4 EXAMPLE.   Define a sequence $(a_n)_{n \geq 1}$ as follows :

$$a_1 = 2 \quad \text{and} \quad a_n = 5a_{n-1} \ \text{ for all } n \geq 1.$$

1. Write the first four terms of the sequence.

2. Use mathematical induction to show that the terms of the sequence satisfy the formula

$$a_n = 2 \cdot 5^{n-1} \quad \text{for all } n \geq 1.$$

SOLUTION : We have

$$
\begin{aligned}
a_1 &= 2 \\
a_2 &= 5a_1 = 5 \cdot 2 = 10 \\
a_3 &= 5a_2 = 5 \cdot 10 = 50 \\
a_4 &= 5a_3 = 5 \cdot 50 = 250.
\end{aligned}
$$

Let $P(n)$ denote the predicate " $a_n = 2 \cdot 5^{n-1}$ ", where the universe of discourse is the set of positive integers. We shall prove by induction that the proposition $\forall n\ P(n)$ is true.

BASIS STEP : $P(1)$ is true, since $a_1 = 2 \cdot 5^0 = 2$.

INDUCTIVE STEP : We assume that

$$
a_n = 2 \cdot 5^{n-1}.
$$

Under this assumption, we must show that

$$
a_{n+1} = 2 \cdot 5^n.
$$

We write

$$
\begin{aligned}
a_{n+1} &= 5a_n \\
&= 5 \cdot (2 \cdot 5^{n-1}) \\
&= 2 \cdot (5 \cdot 5^{n-1}) \\
&= 2 \cdot 5^n.
\end{aligned}
$$

This is what was to be shown. Since we have proved the basis and inductive steps, we conclude the formula holds for all terms of the sequence.

4.3.5 EXAMPLE.   Observe that

$$
\begin{aligned}
1 &= 1, \\
1 - 4 &= -(1 + 2), \\
1 - 4 + 9 &= 1 + 2 + 3, \\
1 - 4 + 9 - 16 &= -(1 + 2 + 3 + 4), \\
1 - 4 + 9 - 16 + 25 &= 1 + 2 + 3 + 4 + 5.
\end{aligned}
$$

Guess a general formula and prove it by induction.

SOLUTION :   General formula is

$$
1 - 4 + 9 - 16 + \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}(1 + 2 + \cdots + n)
$$

(in expanded form) or

$$
\sum_{i=1}^{n} (-1)^{i-1} i^2 = (-1)^{n-1} \left(\sum_{i=1}^{n} i \right)
$$

(in closed form). We shall prove (by mathematical induction) that this formula is true for all positive integers n.

BASIS STEP :   The formula is true for $n = 1$: $1 = (-1)^0 \cdot 1$.

INDUCTIVE STEP :   Assume that the formula is true for some n; that is, assume that

$$
1 - 4 + 9 - 16 + \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}(1 + 2 + \cdots + n).
$$

We write

$$
\begin{aligned}
1 - 4 + \cdots + (-1)^n (n+1)^2 &= \left(1 - 4 + \cdots + (-1)^{n-1} n^2 \right) + (-1)^n (n+1)^2 \\
&= (-1)^{n-1}(1 + 2 + \cdots + n) + (-1)^n (n+1)^2 \\
&= (-1)^{n-1} \frac{n(n+1)}{2} + (-1)^n (n+1)^2 \\
&= (-1)^n \frac{n+1}{2} \left[-n + 2(n+1) \right] \\
&= (-1)^n \frac{(n+1)(n+2)}{2} \\
&= (-1)^n \left(1 + 2 + \cdots + n + (n+1) \right).
\end{aligned}
$$

The last equality shows that the formula is true for $n+1$. This completes the proof and we are done.

Second principle of mathematical induction

There is another form of mathematical induction that is often used in proofs. It is based on what is called the **second principle of mathematical induction**.

Second Principle of Mathematical Induction : *Let S be a subset of $\mathbb{N}$ such that*

- $0 \in S$;

- $\forall n, \quad if \; \{0, 1, \ldots, n\} \subseteq S \; then \; n+1 \in S.$

Then $S = \mathbb{N}$.

The corresponding proof by mathematical induction (of the proposition $\forall n \, P(n)$) consists of

1. *Basis step.* The proposition $P(0)$ is shown to be true.

2. *Inductive step.* It is shown that the implication $P(0) \wedge P(1) \wedge \cdots \wedge P(n) \to P(n+1)$ is true for every natural number n.

NOTE : (1) To prove that the implication

$$P(0) \wedge P(1) \wedge \cdots \wedge P(n) \to P(n+1)$$

is true for every $n \in \mathbb{N}$, we need to show that $P(n+1)$ *cannot* be false when $P(0), P(1), \ldots, P(n)$ are all true; this can be accomplished by assuming that $P(0), P(1), \ldots, P(n)$ are true and showing that *under these premises* $P(n+1)$ must also be true.

(2) Just as with the principle of mathematical induction, the second principle of mathematical induction is equally valid if, instead of starting with 0, we (1) start with

a given a, (2) show that $a \in S$, and (3) show that, if $n \geq a$ and $\{a, a+1, \ldots, n\} \subseteq S$, then $n + 1 \in S$. Again, when we do this, we will know that every natural number greater than or equal to a belongs to the set S.

4.3.6 EXAMPLE.   Prove by induction that, if $n \in \mathbb{N}$ and $n \geq 4$, then n can be written as a sum of numbers each of which is a 2 or a 5.

SOLUTION :   Let $P(n)$ be the predicate " n can be written as a sum of 2s and 5s", where the universe of discourse is the set $\{n \in \mathbb{N} \mid n \geq 4\}$. We shall prove by induction that the proposition $\forall n \, P(n)$ is true.

BASIS STEP : $P(4)$ is true, since $4 = 2 + 2$.

INDUCTIVE STEP :   Assume that $n \geq 4$ and $4, 5, \ldots, n$ can all be written as a sum of 2s and 5s. Then $n - 1$ can be written as a sum of 2s and 5s; that is,

$$n - 1 = a_1 + a_2 + \cdots + a_p, \quad a_i \in \{2, 5\}.$$

So,

$$n + 1 = a_1 + a_2 + \cdots + a_p + 2$$

and, therefore, $n + 1$ can be written as a sum of 2s and 5s. This completes the proof by induction.

4.3.7 EXAMPLE.   Define a sequence $(b_n)_{n \geq 1}$ as follows :

$$b_1 = 0, \ b_2 = 2 \quad \text{and} \quad b_n = 3 \cdot b_{\lfloor k/2 \rfloor} + 2 \ \text{ for all } n \geq 3.$$

1. Write the first seven terms of the sequence.

2. Use mathematical induction to show that b_n is even for all $n \geq 1$.

SOLUTION : We have

$$
\begin{aligned}
b_1 &= 0 \\
b_2 &= 2 \\
b_3 &= 3 \cdot b_{\lfloor 3/2 \rfloor} + 2 = 3 \cdot b_1 + 2 = 3 \cdot 0 + 2 = 2 \\
b_4 &= 3 \cdot b_{\lfloor 4/2 \rfloor} + 2 = 3 \cdot b_2 + 2 = 3 \cdot 2 + 2 = 8 \\
b_5 &= 3 \cdot b_{\lfloor 5/2 \rfloor} + 2 = 3 \cdot b_2 + 2 = 3 \cdot 2 + 2 = 8 \\
b_6 &= 3 \cdot b_{\lfloor 6/2 \rfloor} + 2 = 3 \cdot b_3 + 2 = 3 \cdot 2 + 2 = 8 \\
b_6 &= 3 \cdot b_{\lfloor 7/2 \rfloor} + 2 = 3 \cdot b_3 + 2 = 3 \cdot 2 + 2 = 8.
\end{aligned}
$$

Let $P(n)$ be the property (predicate) "b_n is even". We shall use mathematical induction (based on the second principle) to show that this property holds for all positive integers (i.e. the proposition $\forall n\, P(n)$ is true).

BASIS STEP : The property holds for $n = 1$: $b_1 = 0$ is even.

INDUCTIVE STEP : Assume that the property holds for all $1 \leq k \leq n$. We need to show that the property then holds for $n + 1$.

The number $b_{\lfloor (n+1)/2 \rfloor}$ is even by assumption (inductive hypothesis), since

$$
1 \leq \left\lfloor \frac{n+1}{2} \right\rfloor \leq n.
$$

Thus $3 \cdot b_{\lfloor (n+1)/2 \rfloor}$ is even (because $odd \cdot even = even$), and hence $3 \cdot b_{\lfloor (n+1)/2 \rfloor} + 2$ is even (because $even + even = even$). Consequently, b_{n+1} — which equals $b_{\lfloor (n+1)/2 \rfloor} + 2$ — is even, as was to be shown.

We conclude that the statement is true.

We now ask a natural question : *"What is the relationship between the second principle of mathematical induction and the principle of mathematical induction ?"* It is clear that the second principle of mathematical induction logically implies the principle of mathematical induction. Indeed, if we are allowed to assume that $\{0, 1, \ldots, n\} \subseteq S$, then we are surely allowed to assume that $n \in S$.

In fact, it is also true that the principle of mathematical induction logically implies the second principle. So, *the two principles of mathematical induction are logically equivalent.*

NOTE :   There is nothing wrong with guessing in mathematics, and presumably most mathematical results are first arrived at intuitively and only later established by proofs as theorems. There is a natural temptation, however, to make a plausible guess and then allow that guess to stand unproved.

4.4   Exercises

Exercise 46 Find the value of each of the following sums :

(a) $\displaystyle\sum_{i=0}^{10} 3 \cdot 2^i$.

(b) $\displaystyle\sum_{i=0}^{10} 2 \cdot (-3)^i$.

(c) $\displaystyle\sum_{i=0}^{10} (3^i - 2^i)$.

(d) $\displaystyle\sum_{i=0}^{10} (2 \cdot 3^i + 3 \cdot 2^i)$.

(e) $\displaystyle\sum_{i=1}^{3} \sum_{j=1}^{4} (2i + 3j)$.

Exercise 47 Use the formula for the sum of the first n natural numbers and/or the formula for the sum of a geometric sequence to find the following sums :

(a) $3 + 4 + 5 + \cdots + 1\,000$.

(b) $5 + 10 + 15 + \cdots + 300$.

(c) $2 + 3 + \cdots + (k - 1)$.

(d) $1 + 2 + 2^2 + \cdots + 2^{25}$.

(e) $3 + 3^2 + 3^3 + \cdots + 3^n$.

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

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

Exercise 48

(a) Let $(a_n)_{n\geq 1}$ be a sequence (of numbers). Verify that

$$\sum_{k=1}^{n}(a_k - a_{k+1}) = a_1 - a_{n+1}.$$

(b) Use identity

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

and part (a) to compute the sum

$$\sum_{k=1}^{n}\frac{1}{k(k+1)}.$$

(c) Use identity

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

to compute the sum

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

(d) Evaluate the sum

$$\sum_{k=1}^{n}\frac{k}{(k+1)!}.$$

Exercise 49 Prove by induction that (for each positive integer n)

(a) $5 + 7 + 9 + \cdots + (2n+3) = n(n+4)$.

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

(c) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$.

(d) $1\cdot 2 + 2\cdot 3 + \cdots + n\cdot(n+1) = \dfrac{n(n+1)(n+2)}{3}$.

(e) $\dfrac{1}{1\cdot 3} + \dfrac{1}{3\cdot 5} + \cdots + \dfrac{1}{(2n-1)\cdot(2n+1)} = \dfrac{n}{2n+1}$.

Exercise 50 Prove by induction that

(a) $n^3 + 1 \geq n^2 + n$, $\quad n \in \mathbb{N}$.

(b) $n! > 2^n$, $\quad n \geq 4$.

(c) $1 + \dfrac{1}{4} + \dfrac{1}{9} + \cdots + \dfrac{1}{n^2} < 2 - \dfrac{1}{n}, \quad n \geq 2.$

(d) $\dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \cdots + \dfrac{1}{\sqrt{n}} > \sqrt{n}, \quad n \geq 2.$

Exercise 51 Prove by induction that (for $n \geq 1$)

(a) $n(n+5)$ is divisible by 2.

(b) $n^3 - n$ is divisible by 6.

(c) $4^n - 1$ is divisible by 3.

(d) $2^{2n-1} + 3^{2n-1}$ is divisible by 5.

(e) $n(n+1)(n+2)$ is divisible by 6.

Exercise 52 A sequence $(a_n)_{n \geq 0}$ is defined by

$$a_0 = 3 \quad \text{and} \quad a_n = a_{n-1}^2 \quad \text{for all} \ n \geq 1.$$

Show that $a_n = 3^{2^n}$ for all $n \geq 0$.

Exercise 53 A sequence $(b_n)_{n \geq 1}$ is defined by

$$b_1 = 1 \quad \text{and} \quad b_n = \sqrt{3b_{n-1} + 1} \quad \text{for all} \ n \geq 2.$$

Show that $b_n < \frac{7}{2}$ for all $n \geq 1$.

Exercise 54 A sequence $(c_n)_{n \geq 1}$ is defined by

$$c_1 = 1 \quad \text{and} \quad c_n = 2 \cdot c_{\lfloor n/2 \rfloor} \quad \text{for all} \ n \geq 2.$$

Show that $c_n \leq n$ for all $n \geq 1$.

Exercise 55 A sequence $(d_n)_{n \geq 0}$ is defined by

$$d_0 = 12, \ d_1 = 29 \quad \text{and} \quad d_n = 5d_{n-1} - 6d_{n-2} \quad \text{for all} \ n \geq 2.$$

Show that $d_n = 5 \cdot 3^n + 7 \cdot 2^n$ for all $n \geq 0$.

Exercise 56 Find the following sums :

(a) $3 + 6 + 9 + \cdots + 3n.$

(b) $1 + 3 + 5 + \cdots + (2n - 1).$

(c) $\frac{1}{1\cdot2} + \frac{1}{2\cdot3} + \frac{1}{3\cdot4} + \cdots + \frac{1}{n(n+1)}$.

(d) $1 + 5 + 9 + 13 + \cdots$ to n terms.

(e) $4 \cdot 7 + 7 \cdot 10 + 10 \cdot 13 + \cdots$ to n terms.

Use mathematical induction to verify your answers.

Exercise 57 Prove that :

(a) Every positive integer other than 1 is either a prime number or the product of prime numbers.

(b) Every natural number $n \geq 14$ can be written as a sum of numbers, each of which is a 3 or an 8.

Exercise 58 Prove that :

(a) For each *odd* natural number $n \geq 3$,

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

(b) For each *even* natural number,

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

Exercise 59 Let $a > -1$. Prove by induction that

$$(1 + a)^n \geq 1 + na$$

for every $n \in \mathbb{N}$.

Exercise 60 Let $a, b \geq 0$. Prove by induction that

$$\left(\frac{a+b}{2}\right)^n \leq \frac{a^n + b^n}{2}$$

for every $n \in \mathbb{N}$.

Chapter 5

Counting

Topics :

1. BASIC COUNTING PRINCIPLES

2. PERMUTATIONS AND COMBINATIONS

3. BINOMIAL FORMULA

Counting objects is necessary in order to solve many different types of problems. Furthermore, counting can provide mathematical insight. For example, counting can determine the proportion between the number of elements of a set that have a property and the number that do not; the study of *discrete probability* is founded on such proportions.

5.1   Basic counting principles

A **list** is a finite sequence of objects. The order in which elements appear in a list is significant. For example, the list $(1, 2, 3)$ is *not* the same as the list $(3, 2, 1)$. Elements in a list might be repeated, as in $(1, 1, 2)$. The number of elements (or terms) in a list is called its **length**. For example, the list $(1, 1, 2, 1)$ is a list of length four (or a 4-list). A list of length two has a special name; it is called an *ordered pair*. A list of length zero is called *the* **empty list**.

NOTE :   An n-list is also called an n-tuple or an n-string (see section **4.1**). The 0-string may be referred to as the **null string**.

Some counting problems are as simple as counting the elements of a list. For example, how many integers are there from 5 to 20 ? To answer this question, imagine going along the list of integers from 5 to 20, counting each in turn. So the answer is 16.

More generally, *if m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.*

5.1.1 EXAMPLE.   How many 3-digit integers (integers from 100 to 999 inclusive) are divisible by 5 ?

SOLUTION :   Imagine writing the 3-digit integers in a row, noting those that are multiple of 5 :

$$\boxed{100} \quad 101 \quad \cdots \quad \boxed{105} \quad 106 \quad \cdots \quad \boxed{110} \quad 111 \quad \cdots \quad \boxed{995} \quad 996 \quad \cdots \quad 999.$$

Since $100 = 5 \cdot \mathbf{20}$, $105 = 5 \cdot \mathbf{21}$, $\cdots$, $995 = 5 \cdot \mathbf{199}$, it follows that there are as many 3-digit integers that are multiples of 5 as there are integers from 20 to 199 inclusive. Hence, there are $199 - 20 + 1 = 180$ integers that are divisible by 5.

NOTE :   We have $180 = \left\lceil \frac{999 - 100}{5} \right\rceil$ (see **Exercise 29**). So $\left\lceil \frac{n-m}{k} \right\rceil$ *represents the number of integers from m to n inclusive which are divisible by k; $k \leq m \leq n$.*

We discuss now three basic counting principles, namely the *addition rule*, the *multiplication rule*, and the *inclusion-exclusion principle*.

Addition rule

Suppose that a *procedure* can be performed by two different tasks. If there are n_1 ways to do the first task and n_2 ways to do the second task, and these tasks cannot be done at the same time, then there are $n_1 + n_2$ ways to do the procedure. This basic principle is known as the **addition rule**.

5.1.2 EXAMPLE.   A representative to a university committee is to be chosen from the Mathematics Department or the Computer Science Department. How many different choices are there for this representative if there are 8 members of the Mathematics Department and 10 members of the Computer Science Department, and no faculty member belongs to both departments ?

SOLUTION :   The task of choosing a representative from the Mathematics Department has 8 possible outcomes, and the task of choosing a representative from the Computer Science Department has 10 possible outcomes. By the addition rule, there are $8 + 10 = 18$ possible choices for the representative.

The addition rule can be stated in terms of sets.

The Addition Rule (for two sets) :   *If A and B are disjoint finite sets, then the number of elements in $A \cup B$ is the sum of the number of elements in A and the number of elements in B ; that is,*

$$|A \cup B| = |A| + |B|.$$

To relate this to our statement of the addition rule, let T_1 be the task of choosing an element from A, and T_2 the task of choosing an element of B. There are $|A|$ ways to do T_1, and $|B|$ ways to do T_2. Since these tasks cannot be done at the same time, the number of ways to choose an element from one of the sets, which is the number of elements in the union, is $|A| + |B|$.

An important consequence of the addition rule is the fact that if the number of elements in a set A and in a subset B of A are both known, then the number of elements that are in A and not in B can be computed.

5.1.3 PROPOSITION. *If A is a finite set and $B \subseteq A$, then*

$$|A \setminus B| = |A| - |B|.$$

SOLUTION : If B is a subset of A, then $B \cup (A \setminus B) = A$ and the two sets B and $A \setminus B$ have no elements in common. Hence by the addition rule,

$$|B| + |A \setminus B| = |A|.$$

Substracting $|B|$ from both sides gives the relation

$$|A \setminus B| = |A| - |B|.$$

□

5.1.4 EXAMPLE. How many 3-digit integers are *not* divisible by 5 ?

SOLUTION : There are $999 - 100 + 1 = 900$ 3-digit numbers. Among these numbers, 180 are divisible by 5. Hence there are $900 - 180 = 720$ integers that are not divisible by 5.

The addition rule can be extended to more than two sets.

The Addition Rule (for n sets) : *If $A_1, A_2, \ldots, A_n$ are pairwise disjoint finite sets, then*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

5.1.5 EXAMPLE. Let $A = \{2, 4, 6\}$, $B = \{1, 3, 5, 7\}$ and $C = \{8, 9\}$. Find $A \cup B \cup C$ and verify the addition rule with A, B and C.

SOLUTION : We have $A \cup B \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and so

$$|A \cup B \cup C| = 9 = 3 + 4 + 2 = |A| + |B| + |C|.$$

Multiplication rule

Suppose that a procedure can be performed by two different tasks. If there are n_1 ways to do the first task and n_2 ways to do the second task after the first task has been done, then there are $n_1 \cdot n_2$ ways to do the procedure. This counting principle is known as the **multiplication rule**.

5.1.6 EXAMPLE. The riders in a bycicle race are identified by a single letter and a single-digit number. If all riders are to be labeled differently, how many riders are permitted in the race ?

SOLUTION : The procedure of labeling the riders consists of two tasks : placing a single letter on each rider and then placing a single-digit number on each rider. There are 26 ways of performing the first task and 10 ways of performing the second task, so the number of riders permitted in the race is $26 \cdot 10 = 260$.

The multiplication rule can also be stated in terms of sets.

The Multiplication Rule (for two sets) : *If A and B are finite sets, then the number of elements of the Cartesian product $A \times B$ is the product of the number of elements in A and the number of elements in B ; that is,*

$$|A \times B| = |A| \cdot |B|.$$

Again, one can relate this to our statement of the multiplication rule. Let T_1 be the task of choosing an element from A, and T_2 the task of choosing an element of B. There are $|A|$ ways to do T_1, and $|B|$ ways to do T_2. We note that the task of choosing an element in the Cartesian product $A \times B$ is done by choosing an element in A and an element in B. The number of ways to do this, which is the number of elements of the Cartesian product, is $|A| \cdot |B|$.

The multiplication rule can be extended to more than two sets.

The Multiplication Rule (for n sets) : *If $A_1, A_2, \ldots, A_n$ are finite sets, then*

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

5.1.7 EXAMPLE. Let $A = \{1, 2\}$ and $B = \{1, 2, \alpha\}$. Find $A \times B$ and verify the product rule with A and B.

SOLUTION : We have $A \times B = \{(1,1), (1,2), (1,\alpha), (2,1), (2,2), (2,\alpha)\}$ and so

$$|A \times B| = 6 = 2 \cdot 3 = |A| \cdot |B|.$$

5.1.8 EXAMPLE. Write *all* bit strings of length 4.

SOLUTION : There are 16 bit strings of length 4 :

$$0000, \; 0001, \; 0010, \; 0011, \; 0100, \; 0101, \; 0110, \; 0111,$$
$$1000, \; 1001, \; 1010, \; 1011, \; 1100, \; 1101, \; 1110, \; 1111.$$

5.1.9 EXAMPLE. How many different bit strings of length 8 are there ?

SOLUTION : Each of the eight bits can be chosen in two ways, and so the multiplication rule shows that there are $2^8 = 256$ different bit strings of length 8.

5.1.10 EXAMPLE. How many functions are there from a set with m elements to a set with n elements ?

SOLUTION : A function corresponds to a choice of one of the n elements in the codomain for each of the m elements in the domain. Hence, by the multiplication rule, there are $n \cdot n \cdots n = n^m$ functions from a set with m elements to a set with n elements.

NOTE : If A and B are finite sets such that $|A| = m$ and $|B| = n$, then

$$\left|B^A\right| = n^m = |B|^{|A|}.$$

5.1.11 EXAMPLE.   How many one-to-one functions are there from a set with m elements to a set with n elements ?

SOLUTION :   We note that for $m > n$ there are *no* one-to-one functions from a set with m elements to a set with n elements. Let $m \leq n$. Suppose the elements in the domain are $a_1, a_2, \ldots, a_m$. There are n ways to choose the value of the function at a_1. Since the function is one-to-one, the value of the function at a_2 can be chosen in $n-1$ ways (since the value used for a_1 cannot be used again). In general, the value of the function at a_k can be chosen in $n-k+1$ ways. By the multiplication rule, there are $n(n-1)(n-2)\cdots(n-m+1)$ one-to-one functions from a set with m elements to a set with n elements.

NOTE :   If A is a finite set such that $|A| = n$, then

$$|S_A| = |S_n| = n(n-1)\cdots 2 \cdot 1 = n!.$$

So the symmetric group S_n has $n!$ elements.

Inclusion-exclusion principle

Suppose that a procedure can be performed by two different tasks, which can be done at the same time. If there are n_1 ways to do the first task, n_2 ways to do the second task, and n_{12} ways to do both tasks, then there are $n_1 + n_2 - n_{12}$ ways to do the procedure. This principle is known as the **principle of inclusion-exclusion**.

5.1.12 EXAMPLE.   How many integers from 1 to $1\,000$ are multiples of 3 or multiples of 5 ?

SOLUTION :   The procedure of choosing such an integer can be performed by two different tasks : choosing a multiple of 3 and choosing a multiple of 5. The first task has 333 possible outcomes, the second task has 200 possible outcomes, and there are 66 ways to do both tasks (since there are 66 multiples of 15 from 1 to $1\,000$). By the principle of inclusion-exclusion,

there are $333 + 200 - 66 = 467$ integers from 1 through $1\,000$ that are multiples of 3 or multiples of 5.

Once again, we can state this counting principle in terms of sets.

The Inclusion-Exclusion Principle (for two sets) : *If A and B are finite sets, then*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Let T_1 be the task of choosing an element from A and T_2 the task of choosing an element from B. There are $|A|$ ways to do T_1 and $|B|$ ways to do T_2. The number of ways to do either T_1 or T_2 is the sum $|A| + |B|$ minus the number of ways to do both T_1 and T_2. Since there are $|A \cup B|$ ways to do either T_1 or T_2, and $|A \cap B|$ ways to do both T_1 and T_2, we have

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

5.1.13 PROPOSITION. *Let A, B, and C be finite sets. Then*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

PROOF : We have

$$
\begin{aligned}
|A \cup B \cup C| &= |(A \cup B) \cup C)| \\
&= |A \cup B| + |C| - |(A \cup B) \cap C| \\
&= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| \\
&= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.
\end{aligned}
$$

$\square$

5.1.14 EXAMPLE. A car manufacturer finds that the most common production defects are faulty brakes and broken headlights. In testing a sample of 80 cars, the manufacturer recorded the following data : 20 cars have faulty brakes, 15 cars have broken headlights, and 10 cars have both defects. How many cars in the sample have *at least* one of these defects ?

SOLUTION :   Let B be the set of cars in this sample with faulty brakes, and let H be the set of cars in this sample with broken headlights. Using the principle of inclusion-exclusion, we have :

$$|B \cup H| = |B| + |H| - |B \cap H| = 20 + 15 - 10 = 25.$$

There are 25 cars in this sample with at least one of theses two defects.

The principle of inclusion-exclusion can be extended to more than three sets.

The Inclusion-Exclusion Principle (for n sets) :   *If* A_1, $A_2, \ldots,$ A_n *are finite sets, then*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{\substack{i,j=1 \\ i<j}}^{n} |A_i \cap A_j| + \sum_{\substack{i,j,k=1 \\ i<j<k}}^{n} |A_i \cap A_j \cap A_k| - \cdots$$

$$+(-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n|.$$

5.1.15 EXAMPLE.   How many *onto* function are there from a set with m elements to a set with n elements ?

SOLUTION :   We note that for $m < n$ there are *no* onto functions from a set with m elements to a set with n elements. Let $m \geq n$. Recall that the number of *all* functions between these given sets is n^m. Let's call, for convenience, the functions which are not onto "bad". If we can count the number of bad functions, then we are done because

$$\# \text{ onto functions} = n^m - \# \text{ bad functions.}$$

Suppose that the elements of the codomain are b_1, b_2, $\ldots, b_n$. Now a function might be bad because its range fails to contain b_1; or it might be bad because its range fails to contain b_2, and so on. Let B_i denote the set of all functions that fail to contain the element b_i in their range. Then the set $|B_1 \cup B_2 \cup \cdots \cup B_n|$ contains precisely all the bad functions; what we want to do is to

calculate the size of this union. We have

$$
\begin{aligned}
|B_i| &= (n-1)^m, \quad 1 \le i \le n \\
|B_i \cap B_j| &= (n-2)^m, \quad 1 \le i < j \le n \\
|B_i \cap B_j \cap B_k| &= (n-3)^m, \quad 1 \le i < j < k \le n
\end{aligned}
$$

and so on. The question that remains is how many terms are on each row ? It turns out that *the number of all such l-fold intersections is*

$$
\binom{n}{l} := \frac{n\,!}{l\,! \cdot (n-l)!}, \quad 1 \le l \le n.
$$

(See section **5.2** for more explanation and a proof of this statement.) So we have

$$
|B_1 \cup \cdots \cup B_n| = \binom{n}{1}(n-1)^m - \binom{n}{2}(n-2)^m + \cdots + (-1)^{n+1}\binom{n}{n}(n-n)^m
$$

which can be rewritten in closed form as

$$
|B_1 \cup B_2 \cup \cdots \cup B_n| = \sum_{i=1}^{n}(-1)^{i+1}\binom{n}{i}(n-i)^m.
$$

Recall that the set $B_1 \cup B_2 \cup \cdots \cup B_n$ counts the number of bad functions; we want the number of "good" functions (i.e. the onto functions). We get $\#$ onto functions

$$
\begin{aligned}
&= n^m - \#\,\text{bad functions} \\
&= n^m - |B_1 \cup B_2 \cup \cdots \cup B_n| \\
&= n^m - \left[\binom{n}{1}(n-1)^m - \binom{n}{2}(n-2)^m + \cdots + (-1)^{n+1}\binom{n}{n}(n-n)^m \right] \\
&= n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \cdots - (-1)^{n+1}\binom{n}{n}(n-n)^m \\
&= \binom{n}{0}n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \cdots + (-1)^n\binom{n}{n}(n-n)^m \\
&= \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^m.
\end{aligned}
$$

Let us collect what we learned about *counting* functions.

5.1.16 PROPOSITION.   *Let A and B be finite sets with $|A| = m$ and $|B| = n$.*

(1) *The number of functions from A to B is n^m.*

(2) *If $m \leq n$, the number of one-to-one functions $f : A \to B$ is*

$$(n)_m := n(n-1)(n-2)\cdots(n-m+1).$$

If $m > n$, the number of such functions is zero.

(3) *If $m \geq n$, the number of onto functions $f : A \to B$ is*

$$(n)^m := \sum_{i=0}^{n-1}(-1)^i \binom{n}{i}(n-i)^m.$$

If $m < n$, the number of such functions is zero.

NOTE :   For $m = n$ we get

$$n! = (n)_n = (n)^n = \sum_{i=0}^{n-1}(-1)^i \binom{n}{i}(n-i)^n.$$

5.2   Permutations and combinations

We are interested in counting *selections* of objects of a finite set. We shall consider first the case when the objects are *distinct*; in other words, there is no repetition allowed.

There are two distinct ways of selecting r (distinct) objects from a set of n elements. In an *ordered selection*, it is not only what elements are chosen but also the *order* in which they are chosen that matter. Two ordered selections are said to be the same if the elements chosen are the same and also if the elements are chosen in the same order.

In an *unordered selection*, on the other hand, it is only the identity of the chosen elements that matters. Two unordered selections are said to be the same if they consists of the same elements, regardless of the order in which the elements are chosen.

Permutations

5.2.1 DEFINITION. Let A be a set with n elements and let $0 \leq r \leq n$. An ordered selection of r elements of A is called an **r-permutation**. An n-permutation of A is simply called a **permutation** of A.

NOTE : An r-permutation of a set A is simply an r-string (or r-list) of elements of A, when repetition is *not* allowed.

5.2.2 EXAMPLE. Consider the set $A = \{a, b, c, d\}$. How many ordered selections of two elements can be made from the set A ?

SOLUTION : There are twelve 2-permutations of the set A :

$$ab, ac, ad, ba, bc, bd, ca, cb, cd, da, db, dc.$$

.

The number of r-permutations of a set with n elements is denoted by $P(n, r)$. We can find $P(n, r)$ using the multiplication rule.

5.2.3 PROPOSITION. *The number of r-permutations of a set with n elements is*

$$P(n, r) = n(n-1)(n-2) \cdots (n-r+1), \quad 1 \leq r \leq n \,.$$

PROOF : The first element of the permutation can be chosen in n ways. There are $n-1$ ways to choose the second element of the permutation, $n-2$ ways to choose the third element of the permutation, and so on, until there

are exactly $n - r + 1$ ways to choose the rth element. Consequently, by the multiplication rule, there are

$$n(n-1)(n-2)\cdots(n-r+1)$$

r-permutations of the set. $\qquad\qquad\square$

NOTE : An alternative notation for $n(n-1)(n-2)\cdots(n-r+1)$ is $(n)_r$. This notation is called *falling factorial*.

Equivalently, the number of all r-permutations of a set with n elements is

$$P(n,r) = \frac{n!}{(n-r)!}, \quad 0 \le r \le n.$$

In particular,

$$P(n,0) = \frac{n!}{n!} = 1$$

(the 0-permutation corresponds to the **empty list** (or **null string**)) and

$$P(n,n) = (n)_n = n(n-1)(n-2)\cdots 2 \cdot 1 = n!.$$

NOTE : By convention,

$$0! := 1 \quad \text{and} \quad (n)_0 := 1.$$

5.2.4 EXAMPLE. How many ways can the letters in the word COMPUTER be arranged in a row ?

SOLUTION : All the eight letters in the word COMPUTER are distinct, so the number of ways to arrange the letters equals the number of permutations of a set with 8 elements, namely $8! = 40\,320$.

5.2.5 EXAMPLE. Suppose that there are 12 runners in a race. The winner receives a gold medal, the second-place finisher receives a silver medal, and the third-place finisher receives a bronze medal. How many different ways are there to award these medals, if all possible outcomes of the race can occur ?

SOLUTION : The number of different ways to award the medals is the number of 3-permutations of a set with 12 elements, namely $P(12,3) = 12 \cdot 11 \cdot 10 = 1320$.

5.2.6 EXAMPLE. How many different ways can three letters of the word MATHS be chosen and written in a row ? How many different ways can this be done if the first letter must be M ?

SOLUTION : The answer to the first question equals the number of 3-permutations of a set with 5 elements, namely $P(5,3) = 5 \cdot 4 \cdot 3 = 60$. Since the first letter must be M, there are effectively only two letters to be chosen and placed in the other two positions. Hence the answer to the second question is the number of 2-permutations of a set with 4 elements, which is $P(4,2) = 4 \cdot 3 = 12$.

5.2.7 EXAMPLE. Find the number of permutations of the letters in COMPUTER, such that the letters in MUTE are together in any order.

SOLUTION : COPRMUTE is one such permutation, as is COPRMTEU. In order to keep the letters in MUTE together, let Ω denote the set $\{M, U, T, E\}$. We consider Ω as a symbol in a permutation. The number of permutations of C, O, P, R, Ω is $5! = 120$. In each of these 120 permutations, the presence of Ω will keep the letters in MUTE together. Now, for each of these permutations, there are $4! = 24$ permutations of the letters in Ω. Hence, the number of permutations of COMPUTER that contain the letters of MUTE together in any order is $120 \cdot 24 = 2\,880$.

Combinations

5.2.8 DEFINITION. Let A be a set with n elements and let $0 \leq r \leq n$. An unordered selection of r elements of A is called an **r-combination**.

NOTE : An r-combination of a set with n elements is simply a subset with r elements of the given set.

5.2.9 EXAMPLE. Find all the 2-combinations of the set $A = \{1, 2, 3, 4\}$.

SOLUTION :   There are six 2-combinations of A, namely

$$\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}.$$

The number of r-combinations of a set with n elements is denoted by $C(n,r)$. We can determine the number of r-combinations of a set with n elements using the formula for the number of r-permutations of a set.

5.2.10 PROPOSITION.   *The number of r-combinations of a set with n elements is*

$$\boxed{C(n,r) = \frac{n\,!}{r\,!(n-r)\,!}, \quad 0 \le r \le n.}$$

PROOF :   The r-permutations of the set can be obtained by forming the $C(n,r)$ combinations of the set, and then *ordering* the elements in each r-combination, which can be done in $P(r,r)$ ways. Hence,

$$P(n,r) = C(n,r) \cdot P(r,r).$$

Thus

$$C(n,r) = \frac{P(n,r)}{P(r,r)} = \frac{\frac{n!}{(n-r)!}}{\frac{r!}{(r-r)!}} = \frac{n\,!}{r\,!(n-r)\,!}.$$

$\square$

In particular,

$$C(n,0) = \frac{n\,!}{0\,! \cdot n\,!} = 1$$

(the 0-combination corresponds to the empty set) and

$$C(n,n) = \frac{n\,!}{n\,! \cdot 0\,!} = 1.$$

5.2.11 EXAMPLE.   A group of twelve consists of five men and seven women. How many five-person teams can be chosen that consists of three men and two women ?

SOLUTION :   We can think of forming a team as a two-step process : step 1 is to choose the men, and step 2 is to choose the women. There are $C(5,3)$

ways to choose the three men out of the five, and $C(7,2)$ ways to choose the two women out of the seven. Hence, by the product rule, the number of teams of five that contain three men and two women is

$$C(5,3) \cdot C(7,2) = \frac{5!}{3! \cdot 2!} \cdot \frac{7!}{2! \cdot 5!} = 210.$$

NOTE : There is another common notation for the number of r-combinations of a set with n elements, namely

$$\binom{n}{r} \quad (\text{read} \quad \text{``}n \text{ choose } r\text{''}).$$

This number is also called a **binomial coefficient**, since it occurs as a coefficient in the expansion of powers of binomial expressions such as $(a+b)^n$.

5.2.12 EXAMPLE. Evaluate $\binom{5}{3}$.

SOLUTION : We can simply list all the 3-element subsets of the set $\{1,2,3,4,5\}$. Here they are

$$\{1,2,3\}, \quad \{1,2,4\}, \quad \{1,2,5\}, \quad \{1,3,4\}, \quad \{1,3,5\},$$
$$\{1,4,5\}, \quad \{2,3,4\}, \quad \{2,3,5\}, \quad \{2,4,5\}, \quad \{3,4,5\}.$$

Alternatively, we have

$$\binom{5}{3} = \frac{5!}{3! \cdot (5-3)!} = \frac{5!}{3! \cdot 2!} = \frac{3! \cdot 4 \cdot 5}{3! \cdot 2} = 10.$$

NOTE : More generally,

$$\binom{n}{3} = \frac{n(n-1)(n-2)}{6}, \quad n \geq 3.$$

Observe that

$$\binom{5}{2} = \binom{5}{3} = 10.$$

This equality is no coincidence. The following result holds.

5.2.13 PROPOSITION.   *Let $n, r \in \mathbb{N}$ with $0 \leq r \leq n$. Then*

$$\binom{n}{r} = \binom{n}{n-r}.$$

SOLUTION :   We have

$$\binom{n}{r} = \frac{n!}{r! \cdot (n-r)!} = \frac{n!}{(n-r)! \cdot [n-(n-r)]!} = \binom{n}{n-r}.$$

Here is another way to think about this result. Imagine a class with n children. The teacher has r identical chocolate bars to give to exactly r of the children. In how many ways can the chocolate bars be distributed ? The answer is $\binom{n}{r}$ because we are selecting a lucky set of r children to get chocolate. But the pessimistic view is also interesting. We can think about selecting the unfortunate children who will not be receiving chocolate. There are $n - r$ children who do not get chocolate, and we can select that subset of the class in $\binom{n}{n-r}$ ways. Since the two countings are clearly the same, we must have $\binom{n}{r} = \binom{n}{n-r}$.   □

5.2.14 EXAMPLE.   How many bit strings of length eight have exactly three 1's ?

SOLUTION :   To solve this problem, imagine eight empty positions into which the 0's and 1's of the bit string will be placed. Once a subset of three positions has been chosen from the eight to contain 1's, the remaining five positions must all contain 0's. It follows that the number of ways to construct a bit string of length eight with exactly three 1's is the same as the number of subsets of three positions that can be chosen from the eight into which to place the 1's. This number equals

$$\binom{8}{3} = \frac{8!}{3! \cdot 5!} = 56.$$

In many counting problems, objects may be used repeatedly. We are now interested in counting the ordered selections and unordered selections of objects of a finite set, when repetition is allowed.

Permutations with repetition

5.2.15 DEFINITION. Let A be a set with n elements and let $r \geq 0$. An **r-permutation with repetition** of A is an *ordered* selection of r elements of A, where each of the r elements can be repeated. An n-permutation with repetition of A is simply called a **permutation with repetition** of A.

5.2.16 EXAMPLE. How many bit strings of length seven can be constructed from the set $\Sigma = \{0, 1, 2, \ldots, 9\}$? How many seven-digit telephone numbers can be constructed from the set Σ if 0 or 1 is not allowed as a first digit in any telephone number ? Assume repeated digits can be used.

SOLUTION : The number of strings of length seven (over Σ) is

$$10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 10^7 = 10\,000\,000.$$

If 0 or 1 cannot be used as a first digit in a telephone number, then the number of such seven-digit telephone numbers is

$$8 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 8 \cdot 10^6 = 8\,000\,000.$$

The number of r-permutations with repetition of a set with n elements can be obtained by using the multiplication rule.

5.2.17 PROPOSITION. *The number of r-permutations with repetition of a set with n elements is n^r.*

PROOF : First assume $r > 0$. For each of the r elements in the r-permutation with repetition, there are n choices of elements, since repetition is allowed. By the multiplication rule, the number of r-permutations with repetition is $n \cdot n \cdots n = n^r$. For $r = 0$, there is one 0-permutation, the empty permutation. Hence, the number of 0-permutations is $n^0 = 1$. $\qquad \square$

Combinations with repetition

5.2.18 DEFINITION.   Let A be a set with n elements and let $r \geq 0$. An **r-combination with repetition** of A is an unordered selection of r elements of A, when repetition is allowed.

An r-combination with repetition is also called a **multiset** of size r.

5.2.19 EXAMPLE.   Write down all 3-combinations with repetition of the set $\{1, 2, 3, 4\}$. (Write such an unordered selection as $[a, b, c]$)

SOLUTION :   We observe that because the order in which the elements are chosen does not matter, the elements of each selection may be written in increasing order. There are 20 such 3-combinations with repetition :

$[1, 1, 1]$, $[1, 1, 2]$, $[1, 1, 3]$, $[1, 1, 4]$, $[1, 2, 2]$, $[1, 2, 3]$, $[1, 2, 4]$, $[1, 3, 3]$, $[1, 3, 4]$, $[1, 4, 4]$,

$[2, 2, 2]$, $[2, 2, 3]$, $[2, 2, 4]$, $[2, 3, 3]$, $[2, 3, 4]$, $[2, 4, 4]$, $[3, 3, 3]$, $[3, 3, 4]$, $[3, 4, 4]$, $[4, 4, 4]$.

Let $n, r \in \mathbb{N}$. The symbol $\left(\binom{n}{r}\right)$ denotes the number of mutisets of size r whose elements belong to a set with n elements.

NOTE :   The notation $\left(\binom{n}{r}\right)$ is pronounced "n multichoose r". The double parantheses remind us that we may include elements more than once.

5.2.20 EXAMPLE.   Let n and r positive integers. Evaluate

$$\left(\binom{n}{1}\right) \quad \text{and} \quad \left(\binom{1}{r}\right).$$

SOLUTION :   The multisets of size 1 whose elements are selected from the set $\{1, 2, \ldots, n\}$ are

$$[1], \ [2], \ \ldots, \ [n]$$

and so

$$\left(\binom{n}{1}\right) = n.$$

We need to count the multisets of size r whose elements are selected from $\{1\}$. The only possibility is

$$[1, 1, \ldots, 1]$$

and so

$$\left(\binom{1}{r}\right) = 1.$$

One can prove the following result.

5.2.21 PROPOSITION. *Let $n, r \in \mathbb{N}$. Then*

$$\left(\binom{n}{r}\right) = \binom{n+r-1}{r}.$$

This equals the number of ways r objects can be selected from n categories of objects with repetition allowed.

5.2.22 EXAMPLE. A person giving a party wants to set out 15 assorted cans of soft drinks for his guests. He shops at a store that sells five different types of soft drinks. How many different selections of 15 soft drinks can he make ?

SOLUTION : We think of the five different types of soft drinks as the n categories and the 15 cans of soft drinks to be chosen as the r objects. So $n = 5$ and $r = 15$. The total number of different selections of 15 cans of soft drinks of the five types is

$$\left(\binom{5}{15}\right) = \binom{5 + 15 - 1}{15} = \binom{19}{5} = \frac{19 \cdot 18 \cdot 17 \cdot 16 \cdot 15!}{15! \cdot 4 \cdot 3 \cdot 2} = 3\,876.$$

5.2.23 EXAMPLE. If n is a positive integer, how many triples of integers (i, j, k) are there with $1 \le i \le j \le k \le n$?

SOLUTION : We observe that there are exactly as many triples of integers (i, j, k) with $1 \le i \le j \le k \le n$ as there are 3-combinations of integers from 1 through n with repetition allowed, because the elements of any such

3-combination can be written in increasing order in only one way. Hence, the number of such triples is

$$\left(\!\!\binom{n}{3}\!\!\right) = \binom{n+3-1}{3} = \binom{n+2}{3} = \frac{(n+2)!}{3! \cdot (n-1)!} = \frac{n(n+1)(n+2)}{6} \,.$$

5.2.24 EXAMPLE.   How many solutions are there to the equation

$$x + y + z + t = 10$$

if x, y, z, t are natural numbers ?

SOLUTION :   We observe that a solution corresponds to a way of selecting 10 objects from a set with 4 elements, so that x objects of type 1, y objects of type 2, z objects of type 3, and t objects of type 4 are chosen. Hence, the number of solutions is equal to the number of 10-combinations with repetition from a set with 4 elements, namely

$$\left(\!\!\binom{4}{10}\!\!\right) = \binom{4+10-1}{10} = \binom{13}{10} = \frac{13!}{3! \cdot 10!} = \frac{13 \cdot 12 \cdot 11}{3 \cdot 2} = 286.$$

5.3   Binomial formula

In algebra a sum of two terms, such as $a + b$, is called a **binomial**. The *binomial formula* gives an expression for the powers of a binomial $(a + b)^n$, for each positive integer n and all real numbers a and b.

If we compute the coefficients in the expansion $(a+b)^n$ for $n = 1, 2, 3, \ldots$ we obtain :

$$
\begin{aligned}
(a + b)^1 &= 1a + 1b \\
(a + b)^2 &= 1a^2 + 2ab + 1b^2 \\
(a + b)^3 &= 1a^3 + 3a^2b + 3ab^2 + b^3 \\
(a + b)^4 &= 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4.
\end{aligned}
$$

If we arrange the coefficients, we obtain the following triangle, known as **Pascal's triangle.**

$$1 \quad 1$$
$$1 \quad 2 \quad 1$$
$$1 \quad 3 \quad 3 \quad 1$$
$$1 \quad 4 \quad 6 \quad 4 \quad 1.$$

We observe that this can be written as

$$\binom{1}{0} \qquad \binom{1}{1}$$

$$\binom{2}{0} \qquad \binom{2}{1} \qquad \binom{2}{2}$$

$$\binom{3}{0} \qquad \binom{3}{1} \qquad \binom{3}{2} \qquad \binom{3}{3}$$

$$\binom{4}{0} \qquad \binom{4}{1} \qquad \binom{4}{2} \qquad \binom{4}{3} \qquad \binom{4}{4}$$

NOTE : Pascal's triangle is a geometric version of a famous formula, called **Pascal's formula**. It relates the values of $\binom{n+1}{r}$ to the values of $\binom{n}{r-1}$ and $\binom{n}{r}$. Specifically, it says that

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

whenever n and r are positive integers with $r \leq n$. This formula makes it easy to compute higher combinations in terms of lower ones : if the values of $\binom{n}{r}$ are known for all r, then the values of $\binom{n+1}{r}$ can be computed for all r such that $1 \leq r \leq n$.

The pattern that seems to be emerging is that :

5.3.1 PROPOSITION. *In the expansion of $(a+b)^n$, the coefficient of $a^{n-k}b^k$ is*

$$\binom{n}{k} = \binom{n}{n-k}.$$

PROOF : We use a combinatorial argument.

$$(a + b)^n = (a + b) \cdot (a + b) \cdots (a + b) \qquad (n \text{ factors}).$$

To multiply this out we choose a term $t_i \in \{a, b\}$ for each $i \in [n] = \{1, 2, \ldots n\}$ and form the product

$$t_1 \cdot t_2 \cdot \cdots \cdot t_n,$$

and add up all such products. An example of such a product is

$$a \cdot a \cdot b \cdot a \cdot b \cdot b \cdot a \cdot \cdots \cdot a,$$

which we can rearrange to form

$$a^{n-k}b^k$$

for some k. If k is specified, the number of products which collapse to form $a^{n-k}b^k$ is the number of ways in which we can choose $n - k$ a's (and k b's) from the n factors. This is just $\binom{n}{n-k} = \binom{n}{k}$. So there are

$$\binom{n}{k} \quad \text{terms of the form} \quad a^{n-k}b^k$$

and this is the coefficient of $a^{n-k}b^k$.   □

We immediately obtain :

5.3.2 PROPOSITION.   (THE BINOMIAL FORMULA)

$$
\begin{aligned}
(a + b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k \\
&= a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \cdots + \binom{n}{n-1} ab^{n-1} + b^n.
\end{aligned}
$$

PROOF :

$$(a + b)^n = \text{the sum of all products of form } t_1 \cdot t_2 \cdot \cdots \cdot t_n$$

$$= \sum_{k=0}^{n} (\text{the number of products with } k \text{ } b\text{'s }) \cdot a^{n-k}b^k$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k.$$

□

Note :

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

5.3.3 Example.   Use the binomial formula to expand $(x + y)^5$.

Solution :   We have

$$(x + y)^5 = \sum_{k=0}^{5} \binom{5}{k} x^{5-k} y^k =$$

$$= \binom{5}{0} x^5 + \binom{5}{1} x^4 y + \binom{5}{2} x^3 y^2 + \binom{5}{3} x^2 y^3 + \binom{5}{4} x y^4 + \binom{5}{5} y^5 =$$

$$= x^5 + 5x^4 y + 10x^3 y^2 + 10x^2 y^3 + 5xy^4 + y^5.$$

5.3.4 Example.   What is the coefficient of $a^7 b^8$ in the expansion of $(a + b)^{15}$?

Solution :   From the binomial formula it follows that this coefficient is

$$\binom{15}{7} = \frac{15!}{7! \cdot 8!} = 6\,435.$$

5.3.5 Example.   Use the binomial formula to show that

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$$

for all natural numbers n.

Solution :   We have

$$2^n = (1 + 1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}.$$

Note : 2^n represents the number of all the subsets of a set with n elements.

5.3.6 Example.   The following identity holds

$$\binom{n}{3} = \binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{n-1}{2}.$$

SOLUTION :   We have (using Pascal's formula)

$$
\begin{aligned}
\binom{n}{3} &= \binom{n-1}{2} + \binom{n-1}{3} \\
&= \binom{n-1}{2} + \binom{n-2}{2} + \binom{n-2}{3} \\
&\vdots \\
&= \binom{n-1}{2} + \binom{n-2}{2} + \cdots + \binom{4}{2} + \binom{4}{3} \\
&= \binom{n-1}{2} + \binom{n-2}{2} + \cdots + \binom{4}{2} + \binom{3}{2} + \binom{3}{3}.
\end{aligned}
$$

5.4   Exercises

Exercise 61

(a) How many integers from 1 through 1 000 do not have any repeated digits?

(b) How many four-digit integers (integers from 1 000 through 9 999) are divisible by 5 ?

(c) How many integers from 1 through 100 000 contain the digit 6 exactly once?

Exercise 62

(a) A typical PIN (personal identification number) is a sequence of any four symbols chosen from 26 letters in the alphabet and ten digits, with repetition allowed. How many different PINs are possible ?

(b) Now suppose that repetition is not allowed. How many different PINs are there?

Exercise 63 How many permutations of the seven letters A, B, C, D, E, F, G

(a) are there ?

(b) have E in the first position ?

(c) have E in one of the first two positions ?

(d) do not have vowels on the ends ?

(e) have 2 vowels before the 5 consonants ?

(f) have A immediately to the left of E ?

(g) neither begin nor end with A ?

(h) do not have the vowels next to each other ?

Exercise 64 A survey of 100 university students revealed the following data : 18 like to eat chicken, 40 like to eat beef, 20 like to eat lamb, 12 like to eat chicken and beef, 5 like to eat chicken and lamb, 4 like to eat beef and lamb, and 3 like to eat all three. We will classify the student who does not like to eat any of the three kinds of meat as a *non-meat eater*.

(a) How many students in our sample like to eat at least one of the three kinds of meat ?

(b) How many non-meat eaters are in our sample ?

(c) How many students in our sample like to eat *only* lamb ?

Exercise 65 Suppose you have 30 books (15 novels, 10 history books, and 5 math books). Assume that all 30 books are different. In how many ways can you :

(a) put the 30 books in a row on the shelf ?

(b) get a bunch of 4 books to give to a friend ?

(c) get a bunch of 3 history books and 7 novels to give to a friend ?

(d) put the 30 books in a row on a shelf if the novels are on the left, the math books are in the middle, and the history books are on the right ?

Exercise 66

(a) Determine the number of functions from a five-element set to an eight-element set.

(b) Determine the number of functions from a five-element set to an eight-element set that are *not* one-to-one.

(c) Determine the number of functions from a five-element set to a three-element set that are onto.

(d) Determine the number of subsets of a set with 10 elements. (Hint : Count all the characteristic functions of the given set)

Exercise 67 Using *only* the digits $1, 2, 3, 4, 5, 6$, and 7, how many five-digit numbers can be formed that satisfy the following conditions ?

(a) no additional conditions.

(b) at least one 5.

(c) at least one 5 and at least one 6.

(d) no repeated digits.

(e) at least one 5 and no repeated digits.

(f) the first and the last digits the same.

Exercise 68 Consider the word ALGORITHM.

(a) How many ways can three of the letters of the word be selected an written in a row ?

(b) How many ways can five of the letters of the word be selected and written in a row if the first letter must be A ?

Exercise 69 How many different committees of five from a group of fourteen people can be selected if

(a) a certain pair of people insist on serving together or not at all ?

(b) a certain pair of people refuse to serve together ?

Exercise 70 Consider a group of twelve consisting of five men and seven women.

(a) How many five-person teams can be chosen that consists of three men and two women ?

(b) How many five-person teams contain at least one man ?

(c) How many five-person teams contain at most one man ?

Exercise 71

(a) How many bit strings of length 16 contain exactly nine 1's ?

(b) How many bit strings of length 16 contain at least one 1 ?

Exercise 72 Nine points $A, B, C, D, E, F, G, H, I$ are arranged in a plane in such a way that no three lie on the same straight line.

(a) How many straight lines are determined by the nine points ?

(b) How many of these straight lines do not pass through point A ?

(c) How many triangles have three of the nine points as vertices ?

(d) How many of these triangles do not have A as a vertex ?

Exercise 73 Use the binomial formula to expand :

(a) $(2 - x)^5$.

(b) $(2a - 3b)^6$.

(c) $(a + 2)^6$.

(d) $\left(x - \frac{3}{x}\right)^5$.

(e) $\left(x^2 + \frac{1}{x}\right)^7$.

Exercise 74 Find :

(a) the coefficient of x^5 in $(1 + x)^{12}$.

(b) the coefficient of $x^5 y^6$ in $(2x - y)^{11}$.

(c) the coefficient of x^5 in $(2 + x^2)^{12}$.

(d) the middle term of $(a - b)^{10}$.

(e) the number of terms in the expansion of $(5a + 8b)^{15}$.

(f) the largest coefficient in the expansion of $(x + 3)^5$.

(g) the last term of $(x - 2y)^6$.

Exercise 75 Use the binomial formula to prove that

(a) $\quad \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0 \, ; \quad n \geq 1.$

(b) $\quad \binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n \binom{n}{n} = 3^n, \quad n \geq 0.$

Chapter 6

Recursion

Topics :

1. RECURSIVELY DEFINED SEQUENCES

2. MODELLING WITH RECURENCE RELATIONS

3. LINEAR RECURRENCE RELATIONS

Sometimes an object is difficult to define explicitly; it may be easy to define it in terms of itself. This procedure is called *recursion*. Recursive definitions are at the hart of discrete mathematics. Furthermore, recursion is one of the central ideas of computer science.

6.1 Recursively defined sequences

Recall that a sequence (of numbers), denoted $(a_n)_{n \geq 0}$ (or simply (a_n)), is just a function from $\mathbb{N}$ to $\mathbb{R}$; that is, an element of $\mathbb{R}^{\mathbb{N}}$.

A common way to define a sequence is to give an *explicit formula* for its nth term. For example, a sequence (a_n) can be specified by writing

$$a_n = 2^n \quad \text{for} \ \ n = 0, 1, 2 \ldots.$$

The advantage of defining a sequence by such an explicit formula is that each term of the sequence is uniquely determined and any term can be computed in a fixed, finite number of steps.

Another way to define a sequence is to use *recursion*. This requires giving both an equation, called a *recurrence relation*, that relates later terms in the sequence to earlier terms and a specification, called *initial conditions*, of the values of the first few terms of the sequence. For example, the sequence of powers of 2 can also be defined recursively as follows :

$$a_n = 2a_{n-1} \quad \text{for} \ \ n \geq 1 \quad \text{and} \quad a_0 = 1.$$

Sometimes it is very difficult or impossible to find an explicit formula for a sequence, but it *is* possible to define the sequence using recursion.

NOTE : Defining a sequence recursively is similar to proving statements by mathematical induction. The recurence relation is like the inductive step and the initial conditions are like the basis step. Indeed, *the fact that sequences can be defined recursively is equivalent to the fact that mathematical induction works as a method of proof*.

6.1.1 DEFINITION. A **recurrence relation** for a sequence (a_n) is a formula that expresses a_n in terms of one or more of the previous terms of the sequence, namely $a_{n-1}, a_{n-2}, \ldots.$ One or more of these terms may be given specific values; the given values are called **initial conditions**.

6.1.2 EXAMPLE.   Consider the *factorial* sequence $(n!)$. We can see that

$$0! = 1, \quad 1! = 1, \quad 2! = 2 \cdot 1, \quad 3! = 3 \cdot 2 \cdot 1 = 3 \cdot 2!, \quad 4! = 4 \cdot 3!, \quad \ldots$$

In general, $n! = n \cdot (n-1)!$. If we let $\varphi_n := n!$, then we have $\varphi_n = n\varphi_{n-1}$. So

$$\varphi_n = n\varphi_{n-1} \quad \text{for} \quad n = 1, 2, 3, \ldots$$

is a recurrence relation defining $n!$. However, $a_n = na_{n-1}$ does *not* define a unique sequence; for example, the sequence $\pi, \pi, 2\pi, 6\pi, \ldots$ also satisfies this recurrence relation. If we require that

$$\varphi_n = n\varphi_{n-1} \quad \text{for} \quad n \geq 1 \quad \text{and} \quad \varphi_0 = 1$$

we obtain $n!$ *uniquely.* This illustrates the need for initial conditions if we want a recurrence relation to define a sequence uniquely. The initial condition $\varphi_0 = 1$ for the factorial sequence is $0! = 1$.

NOTE :   A sequence defined recursively need *not* start with a subscript of zero.

6.1.3 EXAMPLE.   Show that the sequence $(s_n)_{n \geq 1}$ with $s_n = \frac{(-1)^{n+1}}{n!}$ satisfies the recurrence relation

$$s_{n+1} = -\frac{1}{n+1}s_n \quad \text{for} \quad n \geq 1.$$

SOLUTION :   We have

$$
\begin{aligned}
-\frac{1}{n+1}s_n &= -\frac{1}{n+1}\frac{(-1)^{n+1}}{n!} \\
&= \frac{(-1)^{n+2}}{(n+1)!} \\
&= s_{n+1}.
\end{aligned}
$$

Given a sequence that satisfies a certain recurrence relation and initial conditions, it is often helpful to know an explicit formula for the sequence; such an explicit formula is called a **solution** to the recurrence relation.

The most basic method for finding an explicit fromula for a recursively defined sequence is **iteration**. Iteration works as follows : given a sequence (a_n) defined by a recurrence relation and initial conditions, we start from the initial conditions and calculate succesive terms of the sequence until we can see a *pattern* developing. At that point we guess an explicit formula.

6.1.4 EXAMPLE.   Let (a_n) be the sequence defined recursively as follows :

$$a_n = a_{n-1} + 2 \, ; \quad a_0 = 1.$$

Use iteration to guess an explicit formula for a_n.

SOLUTION :   We have

$$
\begin{aligned}
a_0 \quad &= 1 & &= 1 + 0 \cdot 2 \, ; \\
a_1 \quad &= a_0 + 2 = 1 + 2 & &= 1 + 1 \cdot 2 \, ; \\
a_2 \quad &= a_1 + 2 = (1 + 1 \cdot 2) + 2 & &= 1 + 2 \cdot 2 \, ; \\
a_3 \quad &= a_2 + 2 = (1 + 2 \cdot 2) + 2 & &= 1 + 3 \cdot 2 \, ; \\
a_4 \quad &= a_3 + 2 = (1 + 3 \cdot 2) + 2 & &= 1 + 4 \cdot 2.
\end{aligned}
$$

Guess : $a_n = 1 + 2n$.

NOTE :   A sequence $(a_n)_{n \geq 0}$ is called an **arithmetic sequence** (or **progression**) if and only if there is a constant r such that

$$a_n = a_{n-1} + r \quad \text{for all } n \geq 1.$$

Or, equivalently,

$$a_n = a_0 + r \cdot n.$$

6.1.5 EXAMPLE.   Consider the sequence (b_n) defined recursively as follows :

$$b_n = 3b_{n-1} \, ; \quad b_0 = 2.$$

Use iteration to guess an explicit formula for this sequence.

SOLUTION :   We have

$$
\begin{aligned}
b_0 &= 2 &&= 1 \cdot 2 \,; \\
b_1 &= 3 \cdot b_0 &&= 3 \cdot 2 \,; \\
b_2 &= 3 \cdot b_1 &&= 3^2 \cdot 2 \,; \\
b_3 &= 3 \cdot b_2 &&= 3^3 \cdot 2.
\end{aligned}
$$

Guess : $b_n = 2 \cdot 3^n$.

NOTE :   A sequence $(b_n)_{n \geq 0}$ is called an **geometric sequence** (or **progression**) if and only if there is a constant $q \neq 0$ such that

$$b_n = q \cdot b_{n-1} \quad \text{for all } n \geq 1.$$

Or, equivalently,

$$b_n = b_0 \cdot q^n.$$

6.1.6 EXAMPLE.   Find an explicit formula for the sequence $(H_n)_{n \geq 1}$ defined recursively by

$$H_n = 2H_{n-1} + 1 \quad \text{for } n \geq 2 \quad \text{and} \quad H_1 = 1.$$

(This sequence may be referred to as the **Tower of Hanoi sequence**; see the entertaining discussion of the *Tower of Hanoi puzzle* further in this section).

SOLUTION :   By iteration

$$
\begin{aligned}
H_1 &= 1 \\
H_2 &= 2H_1 + 1 = 2 \cdot 1 + 1 &&= 2^1 + 1 \,; \\
H_3 &= 2H_2 + 1 = 2(2 + 1) + 1 &&= 2^2 + 2 + 1 \,; \\
H_4 &= 2H_3 + 1 = 2(2^2 + 2 + 1) &&= 2^3 + 2^2 + 2 + 1.
\end{aligned}
$$

Guess : $H_n = 2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2 + 1$. By the formula for the sum of a geometric sequence,

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

Hence, the explicit formula seems to be

$$H_n = 2^n - 1 \quad \text{for all integers } n \geq 1.$$

The process of solving a recurrence relation by iteration can involve complicated calculations. It is all too easy to make a mistake and come up with the wrong formula. That is why it is important to confirm your calculations by checking the correctness of your formula. The most common way to do this is to use mathematical induction.

6.1.7 EXAMPLE. Use mathematical induction to show that the formula we have obtained for the Tower of Hanoi sequence is correct.

SOLUTION : Let $P(n)$ be the predicate

$$\text{``}H_n = 2^n - 1.\text{''}$$

We shall prove by induction that the proposition $\forall n\, P(n)$ is true.

BASIS STEP : $P(1)$ is true, since $H_1 = 2^1 - 1$.

INDUCTIVE STEP : Assume that $P(n)$ is true. That is, assume that

$$H_n = 2^n - 1.$$

Under this assumption, we must show that $P(n+1)$ is true, namely that

$$H_{n+1} = 2^{n+1} - 1.$$

We have

$$H_{n+1} = 2H_n + 1 = 2(2^n - 1) + 1 = 2^{n+2} - 2 + 1 = 2^{n+1} - 1.$$

This shows that $P(n+1)$ is true, and therefore we are done.

The following example shows how the process of trying to verify a formula by mathematical induction may reveal a mistake.

6.1.8 EXAMPLE. Consider the sequence (c_n) defined by

$$c_n = 2c_{n-1} + n \quad \text{for all integers } n \geq 1\,; \quad c_0 = 1.$$

Suppose that your calculations suggests that

$$c_n = 2^n + n \quad \text{for all integers } n \geq 0.$$

Is this formula correct ?

SOLUTION : Let us start to prove the proposition $\forall n \, (c_n = 2^n + n)$ and see what develops. The proposed formula passes the basis step with no trouble, since $2^0 + 0 = 1$. In the inductive step we suppose that

$$c_n = 2^n + n \quad \text{for some integer } n$$

and we must show that

$$c_{n+1} = 2^{n+1} + (n+1).$$

We have

$$c_{n+1} = 2c_n + (n+1) = 2(2^n + n) + (n+1) = 2^{n+1} + 3n + 1.$$

To finish the verification, we need to show that

$$2^{n+1} + 3n + 1 = 2^{n+1} + (n+1),$$

which is equivalent to $2n = 0$. But this is false, since n may be *any* natural number. Hence, the proposed formula is wrong. (The right formula is $c_n = 3 \cdot 2^n - (n+2)$.)

Once we have found a proposed formula to be false, we should look back at our calculations to see where we have made a mistake, correct it, and try again.

6.2   Modelling with recurrence relations

Recurrence relations can be used to model a variety of problems such as finding compound interest or counting various objects with certain properties (e.g. bacteria, sequences, bit strings, etc.).

6.2.1 EXAMPLE. **(Compound interest)** On your twenty-first birthday you get a letter informing you that on the day you were born an eccentric rich aunt deposited $R\,1\,000$ in a bank account earning $5.5\,\%$ interest compounded annually and she now intends to turn the account over to you provided you can figure out how much it is worth. What is the amount currently in the account ?

SOLUTION : We observe that the amount in the account at the end of any particular year equals the amount at the end of the previous year plus the interest earned on the account during the year. Now the interest earned during the year equals the interest rate, $5.5\,\% = 0.055$, times the amount in the account at the end of the previous year. For any positive integer n, let A_n denote the amount in the account at the end of year n and let $A_0 = 1\,000$ be the initial amount in the account. Then we get

$$A_n = A_{n-1} + (0.055) \cdot A_{n-1} = (1.055) \cdot A_{n-1}\,.$$

Thus a (complete) recurrence relation for the sequence (A_n) is as follows

$$A_n = (1.055) \cdot A_{n-1}\,; \quad A_0 = 1\,000\,.$$

The value on your twenty-first birthday can be computed by *repeated substitution* : $A_1 = 1\,055.00, A_2 = 1\,113.02, A_3 = 1\,174.24, \ldots, A_{20} = 2\,917.76, A_{21} = 3\,078.23$.

6.2.2 EXAMPLE. **(Number of bacteria in a colony)** Suppose that the number of bacteria in a colony triples every hour.

1. Set up a recurrence relation for the number of bacteria after n hours have elapsed.

2. If 100 bacteria are used to begin a new colony, how many bacteria will be in the colony in 10 hours ?

SOLUTION : (1) Since the number of bacteria triples every hour, the recurrence relation should say that *the number of bacteria after n hours is 3 times*

the number of bacteria after $n-1$ *hours.* Letting b_n denote the number of bacteria after n hours, this statement translates into the recurrence relation $b_n = 3b_{n-1}$.

(2)   The given statement is the initial condition $b_0 = 100$ (the number of bacteria at the beginning is the number of bacteria after no hours have elapsed). We can solve the recurrence relation easily by iteration :

$$b_n = 3b_{n-1} = 3^2 b_{n-2} = \cdots = 3^n b_{n-n} = 3^n b_0.$$

Letting $n = 10$ and knowing that $b_0 = 100$, we see that

$$b_{10} = 3^{10} \cdot 100 = 5,904,900.$$

6.2.3 EXAMPLE.   **(Number of sequences with a certain property)**

1. Find a recurrence relation for the number of strictly increasing sequences of positive integers that have 1 as their first term and n as their last term, where n is a positive integer. (That is, finite sequences $a_1, a_2, \ldots, a_k$ where $a_1 = 1$, $a_k = n$, and $a_i < a_{i+1}$ for $i = 1, 2, \ldots, k-1$.)

2. What are the initial conditions ?

3. How many sequences of the type described in (a) are there, when n is a positive integer with $n \geq 2$?

SOLUTION :   (1)   Let s_n be the number of such sequences. A string ending in n must consist of a string ending in something less than n, followed by an n as the last term. Therefore the recurrence relation is

$$s_n = s_{n-1} + s_{n-2} + \cdots + s_2 + s_1 .$$

Here is another approach, with a more compact form of the answer. A sequence ending in n is either a sequence ending in $n-1$ followed by n (and there are

clearly s_{n-1} of these), or else it does not contain $n-1$ as a term at all, in which case it is *identical* to a sequence ending in $n-1$ in which the $n-1$ has been replaced by n (and there are clearly s_{n-1} of these as well). Therefore,

$$s_n = 2s_{n-1}.$$

(2)   We need *two* initial conditions if we use the second formulation above, $s_1 = 1$ and $s_2 = 1$ (otherwise, our argument is invalid, because the first and the last terms are the same). There is one sequence ending in 1, namely the sequence with just this 1 in it, and there is only the sequence (string) $(1, 2)$ ending in 2. If we use the first formulation above, then we can get by with just the initial condition $s_1 = 1$.

(3)   Clearly, the solution to this recurrence relation and initial condition is $s_n = 2^{n-2}$ for al $n \geq 2$.

6.2.4 EXAMPLE.   (**Number of bit strings with a certain property**) Find the number of bit strings of length 10 that do *not* contain the pattern 11.

SOLUTION :   To find the required number you could list all $2^{10} = 1024$ strings of length 10 and cross off those that contain the pattern 11. However, this approach would be very time-consuming. A more efficient solution uses recursion. Suppose the number of bit strings of length n that do not contain the pattern 11 is known. Any such bit string begins with either a 0 or a 1. If the string begins with a 0, the remaining $n-1$ characters can be any sequence of 0's and 1's except that the pattern 11 cannot appear. If the string begins with a 1, then the second character must be a 0, for otherwise the string would contain the pattern 11; the remaining $n-2$ characters can be any sequence of 0's and 1's that does not contain the pattern 11. Let s_n denote the number of bit strings of length n that do not contain the pattern 11. Then we can write

$$s_n = s_{n-1} + s_{n-2}.$$

So, a (complete) recurrence relation for the sequence (s_n) is

$$s_n = s_{n-1} + s_{n-2}; \quad s_0 = 1, \ s_1 = 2 \ \text{(or } \ s_1 = 2, \ s - 2 = 3).$$

It follows that $s_2 = 3, s_3 = 5, s_4 = 8, \ldots, s_{10} = 144$. Hence, there are 144 bit strings of length 10 that do not contain the pattern 11.

We give some more interesting examples.

6.2.5 EXAMPLE.   **(Fibonacci numbers)**   One of the earliest examples of recursively defined sequences arises in the writings of LEONARDO OF PISA, commonly known as FIBONACCI. In 1202 FIBONACCI posed the following problem.

A single pair of rabbits (male and female) is born at the beginning of a year. Assume the following conditions :

1. *Rabbit pairs are not fertile during their first month of life, but thereafter give birth to one new male/female pair at the end of every month;*

2. *No rabbits die.*

How many rabbits will there be at the end of the year ?

SOLUTION :   One way to solve this problem is to plunge right into the middle of it using recursion. Suppose we know how many rabbit pairs there were at the ends of previous months. How many will there be at the end of the current month ? The crucial observation is that *the number of rabbit pairs born at the end of month k is the same as the number of pairs alive at the end of month $k - 2$.* (Why ? Because it is exactly the rabbit pairs that were alive at the end of the month $k - 2$ that were fertile during month k. The rabbits born at the end of month $k - 1$ were not.) Now the number of rabbit pairs alive at the end of month k equals the ones alive at the end of the month $k - 1$ plus the pairs newly born at the end of the month. For any positive integer n, let F_n denote the number of rabbit pairs alive at the end of month n and

let $F_0 = 1$ be the initial number of rabbit pairs. Then we get the following recurrence relation

$$F_n = F_{n-1} + F_{n-2}; \quad F_0 = 1, \ F_1 = 1.$$

NOTE :   The terms of the sequence $(F_n)_{n \geq 0}$ are called **Fibonacci numbers**.

To answer FIBONACCI's question, compute F_2, F_3, and so forth through F_{12}. We get $F_2 = 2$, $F_3 = 3$, $F_4 = 5$, $\ldots, F_{12} = 233$. At the end of the twelfth month there are 233 rabbit pairs in all.

6.2.6 EXAMPLE.

1. Find a recurrence relation for the number of bit strings of length n that contain a pair of consecutive 0s.

2. What are the initial conditions ?

3. How many bit strings of length seven contain two consecutive 0s ?

SOLUTION :   (1)   Let a_n be the number of bit strings of length n containing a pair of consecutive 0s. In order to construct a bit string of length n containing a pair of consecutive 0s we could start with 1 and follow with a string of length $n - 1$ containing a pair of consecutive 0s, or we could start with a 01 and follow with a string of length $n - 2$ containing a pair of consecutive 0s, or we could start with 00 and follow with any string of length $n - 2$. These three cases are mutually exclusive and exhaust the possibilities for how the string might start. From this analysis we can immediately write down the recurrence relation, valid for all $n \geq 2$:

$$a_n = a_{n-1} + a_{n-2} + 2^{n-2}.$$

(2)   There are no bit strings of length 0 or 1 containing a pair of consecutive 0s, so the initial conditions are $a_0 = a_1 = 0$ (or $a_1 = 0, \ a_2 = 1$).

(3)   We will compute a_2 through a_7 using the recurrence relation :

$$
\begin{aligned}
a_2 &= a_1 + a_0 + 2^0 = 0 + 0 + 1 = 1\,; \\
a_3 &= a_2 + a_1 + 2^1 = 1 + 0 + 2 = 3\,; \\
a_4 &= a_3 + a_2 + 2^2 = 3 + 1 + 4 = 8\,; \\
a_5 &= a_4 + a_3 + 2^3 = 8 + 3 + 8 = 19\,; \\
a_6 &= a_5 + a_4 + 2^4 = 19 + 8 + 16 = 43\,; \\
a_7 &= a_6 + a_5 + 2^5 = 43 + 19 + 32 = 94.
\end{aligned}
$$

Thus, there are 94 bit strings of length 7 containing two consecutive 0s.

6.2.7 EXAMPLE.

1. Find a recurrence relation for the number of ways to climb n stairs if the person climbing the stairs can take one stair or two stairs at the time.

2. What are the initial conditions ?

3. How many ways can this person climb a flight of eigth stairs ?

SOLUTION :   (1)   Let S_n be the number of ways to climb n stairs. In order to climb n stairs, a person must either start with a step of one stair and then climb $n - 1$ stairs (and this can be done in S_{n-1} ways), or else start with a step of two stairs and then climb $n - 2$ stairs (and this can be done in S_{n-2} ways). From this analysis we can immediately write down the recurrence relation, valid for all $n \geq 2$:

$$
S_n = S_{n-1} + S_{n-2}.
$$

We note that the recurrence relation is the same as that for the Fibonacci sequence.

(2)   The initial conditions are $S_0 = 1$ and $S_1 = 1$, since there is one way to

climb no stairs (do nothing) and clearly one way to climb one stair.

(3)   We have

$$S_2 = 2, \ S_3 = 3, \ S_4 = 5, \ S_5 = 8, \ S_6 = 13, \ S_7 = 21, \ S_8 = 34.$$

Thus, a person can climb a flight of 8 stairs in 34 ways under the restrictions in this problem.

6.2.8 EXAMPLE.   **(The Tower of Hanoi puzzle)**   This puzzle was invented in 1883 by the French mathematician EDOUARD LUCAS, who made up the legend to accompany it. *According to "legend", a certain Hindu temple contains three thin diamond poles on one of which, at the time of creation, God placed* 64 *golden disks that decrease in size as they rise from the base. The priests of the temple work unceasingly to transfer all the disks one by one from the first pole to one of the others, but they must never place a larger disk on top of a smaller one. As soon as they have completed their task, "tower, temple, and Brahmins alike will crumble into dust, and with a thunderclap the world will vanish."*

The question is : Assuming the priests work as efficiently as possible, how long will it be from the time of creation until the end of the world ?

SOLUTION :   Suppose that we have found the most efficient way possible to transfer a tower of $k-1$ disks one by one from one pole to another, obeying the restriction that we never place a larger disk on top of a smaller one. What is the most efficient way to move a tower of k disks from one pole to another ? Let A be the initial pole, B the intermediate one, and C the target pole. The minimum sequence of moves includes three steps : step 1 - is to move the top $k-1$ disks from pole A to pole B; step 2 - is to move the bottom disk from pole A to pole C; step 3 - is to move the top $k-1$ disks from pole B to pole C. For any positive integer n, let H_n denote the minimum number of moves needed to move a tower of n disks from one pole to another. One can show that

$$H_n = H_{n-1} + 1 + H_{n-1} = 2H_{n-1} + 1.$$

Hence, a (complete) recursive description of the sequence (H_n) is as follows :

$$H_n = 2H_{n-1} + 1 \, ; \quad H_1 = 1.$$

Going back to the legend, suppose the priests work rapidly and move one disk every second. Then the time from the beginning of creation to the end of the world would be H_{64} seconds. We can compute this number on a calculator or a computer ; the approximate result is

$$1.844674 \times 10^{19} \text{ seconds } \approx 5.84542 \times 10^{11} \text{ years } \approx 584.5 \text{ billion years.}$$

6.3   Linear recurrence relations

We shall restrict our investigation to a special class of recurrence relations that can be explicitly solved in a systematic way. These are recurrence relations that express the terms of a sequence as a *linear combination* of previous terms.

6.3.1 DEFINITION.   A recurrence relation of the form

$$a_n = \beta_1 a_{n-1} + \beta_2 a_{n-2} + \cdots + \beta_k a_{n-k} + \varphi(n) \, ;$$

$$a_0 = \gamma_0, \ a_1 = \gamma_1, \ldots, a_{k-1} = \gamma_{k-1},$$

where β_1, β_2, ..., β_k are real numbers, and $\beta_k \neq 0$, is called a **linear (non-homogeneous) recurrence relation (of degree k) with constant coefficients**. If $\varphi(n) \equiv 0$, the recurrence relation is called **homogeneous**.

NOTE :   (1)   The recurrence relation in the definition is *linear* since the RHS is a sum of multiples of the previous terms of the sequence.

(2)   The recurrence relation is *homogeneous* if no terms occur (in the RHS) that are not multiples of the a_i's.

(3)   The *coefficients* $\beta_1, \beta_2, \ldots, \beta_k$ of the terms of the sequence are all constants.

(4)   The *degree* is k because a_n is expressed in terms of the previous k terms of the sequence.

6.3.2 EXAMPLES.

1. The recurrence relation $t_n = t_{n-1} \cdot t_{n-2}$ is not linear.

2. The recurrence relation $\varphi_n = n\varphi_{n-1}$ does not have constant coefficients.

3. The recurrence relation $F_n = F_{n-1} + F_{n-2}$ is a linear homogeneous recurrence relation of degree two.

4. The recurrence relation $H_n = 2H_{n-1} + 1$ is a linear (non-homogeneous) recurrence relation of degree one.

5. The recurrence relation $A_n = (1.055)A_{n-1}$ is a linear homogeneous recurrence relation of degree one.

The homogeneous case

We first tackle the homogeneous case, so we have :

$$a_n = \beta_1 a_{n-1} + \beta_2 a_{n-2} + \cdots + \beta_k a_{n-k} \,;$$

$$a_0 = \gamma_0, \ a_1 = \gamma_1, \ldots, a_{k-1} = \gamma_{k-1}.$$

The idea is to look for solutions of the form

$$a_n = r^n, \quad \text{where } r \text{ is a constant.}$$

6.3.3 EXAMPLE. Consider the FIBONACCI recurrence relation

$$F_n = F_{n-1} + F_{n-2} \,; \quad F_0 = 1, \ F_1 = 1.$$

We seek r such that

$$r^n = r^{n-1} + r^{n-2} \,;$$

that is,

$$r^{n-2} \left(r^2 - r - 1 \right) = 0.$$

Since the solution $r = 0$ is not acceptable, we solve

$$r^2 - r - 1 = 0.$$

This equation is called the **characteristic equation** and we see that it has two solutions :

$$r_{1,2} = \frac{1 \pm \sqrt{5}}{2}\,.$$

Thus

$$f_1(n) = \left(\frac{1 + \sqrt{5}}{2}\right)^n \quad \text{and} \quad f_2(n) = \left(\frac{1 - \sqrt{5}}{2}\right)^n$$

are solutions of the given recurrence relation and so is

$$F_n = C_1 f_1(n) + C_2 f_2(n) = C_1 \left(\frac{1 + \sqrt{5}}{2}\right)^n + C_2 \left(\frac{1 - \sqrt{5}}{2}\right)^n$$

for any constants C_1, C_2. We therefore choose the constants C_1 and C_2 such that

$$f(0) = 1\,, \quad f(1) = 1.$$

We need

$$\begin{cases} C_1 + C_2 = 1 \\[2mm] \left(\dfrac{1 + \sqrt{5}}{2}\right) C_1 + \left(\dfrac{1 - \sqrt{5}}{2}\right) C_2 = 1\,. \end{cases}$$

Solving this system we obtain

$$C_1 = \frac{\sqrt{5} + 1}{2\sqrt{5}} \quad \text{and} \quad C_2 = \frac{\sqrt{5} - 1}{2\sqrt{5}}$$

and hence the desired solution is

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

NOTE :   In general, the associated characteristic equation has the form

$$r^k - \beta_1 r^{k-1} - \beta_2 r^{k-2} - \cdots - \beta_{k-1} r - \beta_k = 0\,,$$

and its roots can be :

- real and distinct ;

- real and repeated ;

- complex.

Here, we shall deal only with the first two cases.

Distinct real roots :   *If $r_1, r_2, \ldots, r_k$ are distinct real roots of the characteristic equation, then for each $i \in [k]$ and each constant C_i, we have $C_i r_i^n$ as a solution (of the given recurrence relation) and it is easy to verify that*

$$a_n = C_1 r_1^n + C_2 r_2^n + \cdots + C_k r_k^n$$

is also a solution. The presence of k arbitrary constants $C_1, C_2, \ldots, C_k$ allows to find values for the C_i such that the initial conditions are satisfied.

Repeated real roots :   *If a root r is repeated m times, then it is easy to verify that*

$$r^n, \, nr^n, \, n^2 r^n, \ldots, n^{m-1} r^n$$

are solutions and so also is

$$a_n = C_1 r^n + C_2 n r^n + \cdots + C_m n^{m-1} r^n.$$

6.3.4 EXAMPLE.   Consider the linear recurrence relation

$$a_{n+2} = 4a_{n+1} - 4a_n ; \qquad a_1 = 1, \; a_2 = 3.$$

Its characteristic equation is

$$r^2 - 4r + 4 = 0$$

and the roots of this equation are $r_1 = r_2 = 2$. Thus, for any constants C_1, C_2

$$a_n = C_1 2^n + C_2 n 2^n$$

is a solution of our recurrence relation. We set

$$\begin{cases} 2C_1 + 2C_2 & = 1 \\[2mm] 4C_1 + 8C_2 & = 3 \end{cases}$$

and solve to obtain

$$C_1 = \frac{1}{4} \quad \text{and} \quad C_2 = \frac{1}{4}.$$

The solution is therefore

$$a_n = \frac{1}{4}2^n + \frac{1}{4}n2^n = \frac{(n+1)2^n}{4}.$$

The non-homogeneous case

We now investigate recurrence relations of the form

$$a_n = \beta_1 a_{n-1} + \beta_2 a_{n-2} + \varphi(n).$$

In other words, we are restricting ourselves to *(non-homogeneous) linear recurrence relations of degree two.* For such a recurrence relation, let us call

$$a_n = \beta_1 a_{n-1} + \beta_2 a_{n-2}$$

the **associated homogeneous equation.**

The following facts are easy to prove.

(1) If $f_1(n)$ and $f_2(n)$ are solutions, then

$$f(n) = C_1 f_1(n) + C_2 f_2(n)$$

is also a solution, for any constants C_1 and C_2.

(2) Suppose that $p(n)$ is a *particular solution.* Then $f(n) + p(n)$ is also a solution.

Based on these two simple facts one obtains an important result (given bellow without proof).

6.3.5 THEOREM.   *Consider the recurrence relation*

$$a_n = \beta_1 a_{n-1} + \beta_2 a_{n-2} + \varphi(n); \quad a_0 = \gamma_0, \, a_1 = \gamma_1.$$

Let $f_1(n)$ and $f_2(n)$ be solutions of the associated homogeneous equation such that $f_2(n)$ is not just a multiple of $f_1(n)$. Let $p(n)$ be a particular

solution. Then a sequence (a_n) *is a solution of the given recurrence relation if and only if*

$$a_n = C_1 f_1(n) + C_2 f_2(n) + p(n)$$

where C_1 *and* C_2 *are constants.*

NOTE :   (1)   We call

$$a_n = C_1 f_1(n) + C_2 f_2(n) + p(n)$$

the **general solution** of the recurrence relation.

(2)   Finding the particular solution $p(n)$ has to be done by inspection, since there is no general method available. If $\varphi(n)$ is a polynomial, we try for a polynomial $p(n)$ (of the same degree or higher). If $\varphi(n)$ is an exponential function, we try to find a similar function for $p(n)$. For example, if $\varphi(n) = 3 \cdot 2^n$, we try for a function of the form $A \cdot 2^n$ or $(An + B) \cdot 2^n$.

6.3.6 EXAMPLE.   The recurrence relation

$$s_n = 2s_{n-1} + 1 ; \quad s_1 = 1$$

has $f(n) = C2^n$ as a solution of the associated homogeneous equation, for any constant C. Since $\varphi(n) = 1$ is a polynomial of degree 0, we seek a constant A such that $p(n) = A$ is a particular solution. We obtain $A - 2A = 1$ and so $A = -1$. Thus $p(n) = -1$ is a particular solution and so

$$s_n = C2^n - 1$$

is a solution of the given recurrence relation, for any constant C. If we set $1 = C2^1 - 1$ then $C = 1$ and so

$$s_n = 2^n - 1$$

is the solution which satisfies the initial condition.

6.3.7 EXAMPLE.   The recurrence relation

$$a_n = -2a_{n-1} - a_{n-2} + 2^n\,;\qquad a_1 = 0,\ a_2 = 0$$

has, as a solution to the associated homogeneous equation,

$$f(n) = C_1(-1)^n + C_2 n\ (-1)^n.$$

To find a particular solution, we seek k such that $p(n) = k2^n$ is a solution. We therefore require of k that

$$k2^n + 2k2^{n-1} + k2^{n-2} = 2^n$$

and this means that

$$k2^{n-2}(4 + 4 + 1) = 2^n.$$

Thus

$$k = \frac{2^n}{9 \cdot 2^{n-2}} = \frac{4}{9}.$$

Thus

$$a_n = C_1(-1)^n + C_2 n(-1)^n + \frac{4}{9} \cdot 2^n$$

is the general solution. We set

$$\begin{cases} -C_1 - C_2 + \frac{8}{9} = 0 \\[2mm] C_1 + 2\,C_2 + \frac{16}{9} = 0 \end{cases}$$

and solve, to obtain $C_1 = \frac{32}{9}$ and $C_2 = -\frac{8}{3}\cdot$ Thus

$$a_n = \frac{32}{9} \cdot (-1)^n - \frac{8}{3} \cdot n(-1)^n + \frac{4}{9} \cdot 2^n = \frac{(-1)^n 4}{9}\left(8 - 6n + (-2)^n\right)$$

is the solution of the given (complete) recurrence relation.

6.3.8 EXAMPLE.   The recurrence relation

$$a_n = -2a_{n-1} + n + 3\,;\quad a_1 = \frac{5}{9}$$

has $f(n) = C(-2)^n$ as solution to the associated homogeneous equation and, to find a particular solution, we try

$$p(n) = An + B.$$

We set

$$(An + B) + 2(A(n-1) + B) = n + 3.$$

Thus

$$(3A)n + (3B - 2A) = 1n + 3$$

and, by comparing coefficients, we obtain

$$3A = 1, \quad 3B - 2A = 3.$$

Thus $A = \frac{1}{3}$ and $B = \frac{11}{9} \cdot$ Therefore

$$a_n = C(-2)^n + \frac{1}{3} \cdot n + \frac{11}{9}$$

is the general solution. Setting

$$-2C + \frac{1}{3} + \frac{11}{9} = \frac{5}{9}$$

yields $C = \dfrac{1}{2}$ and so

$$a_n = \frac{1}{2} \cdot (-2)^n + \frac{1}{3} \cdot n + \frac{11}{9}$$

is the solution which satisfies the given initial condition.

6.4   Exercises

Exercise 76 Show that each of the following sequences satisfies the given recurrence relation.

    (a) $(a_n)_{n \geq 0}$,   where $a_n = 3n + 1$; $a_n = a_{n-1} + 3$ for $n \geq 1$.

    (b) $(b_n)_{n \geq 0}$,   where $b_n = 5^n$; $b_n = 5b_{n-1}$ for $n \geq 1$.

    (c) $(c_n)_{n \geq 0}$,   where $c_n = 2^n - 1$; $c_n = 2c_{n-1} + 1$ for $n \geq 1$.

(d) $(d_n)_{n \geq 0}$, where $d_n = \dfrac{(-1)^n}{n!}$; $d_n = -\dfrac{d_{n-1}}{n}$ for $n \geq 1$.

Exercise 77 Describe each of the following sequences recursively. Include initial conditions.

(a) $a_n = 5^n$.

(b) $b_n = 1 + 2 + 3 + \cdots + n$.

(c) $c_n = (-1)^n$.

(d) $\delta_n = \sqrt{2}$.

(e) $0, 1, 0, 1, 0, 1, \ldots$.

(f) $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots$.

(g) $0.1, 0.11, 0.111, 0.1111, \ldots$.

Exercise 78 Each of the following sequences is defined recursively. Use iteration to guess an explicit formula for the sequence.

(a) $a_n = \dfrac{a_{n-1}}{1 + a_{n-1}}$ for $n \geq 1$; $a_0 = 1$.

(b) $b_n = 2b_{n-1} + 3$ for $n \geq 2$; $b_1 = 2$.

(c) $c_n = c_{n-1} + 2n + 1$ for $n \geq 1$; $c_0 = 0$.

(d) $d_n = 2^n - d_{n-1}$ for $n \geq 1$; $d_0 = 1$.

(e) $e_n = 3e_{n-1} + n$ for $n \geq 2$; $e_1 = 1$.

(f) $f_n = f_{n-1} + n^2$ for $n \geq 2$; $f_1 = 1$.

(g) $g_n = ng_{n-1}$ for $n \geq 1$; $g_0 = 5$.

Exercise 79

(a) A sequence is defined recursively as follows :

$$s_n = n - s_{n-1} \quad \text{for } n \geq 1; \quad s_0 = 0.$$

Use iteration to guess an explicit formula for the sequence, and then check by mathematical induction that the obtained formula is correct.

(b) A sequence is defined recursively as follows :

$$t_n = t_{n-1} \cdot t_{n-2} \quad \text{for } n \geq 2; \quad t_0 = t_1 = 2.$$

Use iteration to guess an explicit formula for the sequence, and then check by mathematical induction that the obtained formula is correct.

Exercise 80 Assume that the population of the world in 1995 is 7 billion and is growing 3% a year.

    (a) Set up a recurrence relation for the population of the world n years after 1995.

    (b) Find an explicit formula for the population of the world n years after 1995.

    (c) What will the population of the world be in 2010 ?

Exercise 81

    (a) Find a recurrence relation for the number of bit strings of length n that contain three consecutive 0s.

    (b) What are the initial conditions ?

    (c) How many bit strings of length seven contain three consecutive 0s ?

Exercise 82 Messages are transmitted over a communications channel using two signals. The transmittal of one signal requires 1 microsecond, and the transmittal of the other signal requires 2 microseconds.

    (a) Find a recurrence relation for the number of different messages consisting of sequences of these two signals, where each signal in the message is immediately followed by the next signal, that can be sent in n microseconds.

    (b) What are the initial conditions ?

    (c) How many different messages can be sent in 10 microseconds using these two signals ?

Exercise 83 Suppose that inflation continues at 8% annually. (That is, an item that costs R 1.00 now will cost R 1.08 next year.) Let $R_n =$ the value (that is, the purchasing power) of one Rand after n years.

    (a) Find a recurrence relation for R_n.

    (b) What is the value of R 1.00 after 20 years ?

    (c) What is the value of R 1.00 after 80 years ?

    (d) If inflation were to continue at 10% annually, find the value of R 1.00 after 20 years.

   (e) If inflation were to continue at 10% annually, find the value of R 1.00 after 80 years.

Exercise 84 Solve the following recurrence relations.

   (a) $a_n = 5a_{n-1} - 6a_{n-2} + 2n + 1$; $a_1 = 0, a_2 = 0$.

   (b) $b_n = 4b_{n-1} - 4b_{n-2} + n^2$; $b_1 = 1, b_2 = 40$.

   (c) $c_n = \frac{1}{4}c_{n-2}$; $c_0 = 1, c_1 = 0$.

   (d) $d_n = d_{n-2} + 10^n$; $d_1 = \frac{1000}{99}, d_2 = \frac{10198}{99}$.

   (e) $e_n = e_{n-1} + n$; $e_0 = 1$.

   (f) $L_n = L_{n-1} + L_{n-2}$; $L_0 = 2, L_1 = 1$

   (g) $f_n = 4f_{n-1} - 4f_{n-2} + 2^n$; $f_1 = 2, f_2 = 8$.

   (h) $a_n + 3a_{n-1} = 4n^2 - 2n + 2^n$

Exercise 85 (*Compound Interest*)

   (a) The fractional increase in a quantity y, per unit of time, is r. Let $y = y(n)$ denote the value of y after n units of time. Find an expression for $y = y(n)$.

   (b) Money earns $i\%$ interest per year for n years. Let $y = y(n)$ denote the value after n years. Find an expression for $y = y(n)$.

   (c) An initial deposit of $R\,1000$ earns 10% interest per year for fifty years. Find the final value.

   (d) An initial deposit of $R\,1000$ earns 11% interest per year for fifty years. Find the final value. (Note the difference !)

Exercise 86 (*Annuities : Periodic Fixed Deposits*)

   (a) The fractional increase in a quantity y, per unit time is r and y also increases by an increment d per unit of time. Let $y = y(n)$ denote the value of y after n units of time. Find an expression for $y = y(n)$.

   (b) A student, aged twenty, decides to quit smoking and estimates that this saves $R\,1000$ per year. He makes an initial deposit of $R\,1000$ and deposits $R\,1000$ per year thereafter. Suppose that he earns 10% interest per year. Find the value of the annuity after fifty years.

(c) Compare the final amounts when the initial deposit is $R\,1\,000$, $d = 1\,000$, $n = 50$ and r is, in the one case 10% and in the other case 11%. (There is a 69% difference in the final amount for a 1% difference in interest rate !)

Exercise 87 (*Annuities : Periodic Increasing Deposits*)

(a) The fractional increase in a quantity y, per unit time is r. After each unit of time, there is an increment d to y and the fractional increase in d, per unit of time is i. Let $y = y(n)$ denote the value of y after n units of time. Find an expression for $y = y(n)$.

(b) A student, aged twenty, decides to quit smoking and estimates that this saves $R\,1\,000$ per year initially. He estimates that the price of cigarettes will increase at 15% per year so he makes an initial deposit of $R\,1\,000$ and makes deposits which increase at 15% per year thereafter. Suppose that he earns 10% interest per year. Find the value of the annuity after fifty years.

Exercise 88 (*Amortisation*)

(a) Let $y = y(n)$ denote the amount outstanding on a loan. So $y(0)$ is the initial loan. The loan is *amortised* by means of a sequence of equal payments. Let each payment be d. Find an expression for $y = y(n)$ if the interest rate is $r = i/100$.

(b) Find the payment d which is required to amortise a loan of $R\,100\,000$ over 360 monthly payments if the interest rate is 1% per month.

Exercise 89 (*Population Problems*)

(a) A population grows in such a way that *the fractional change in population per period is constant*. Let p_n be the population after time period n. Show that there exists $r \in [0, 1]$ such that

$$p_{n+1} = (1 + r)p_n.$$

If the initial population is p_0, show that

$$p_n = p_0(1 + r)^n.$$

(b) Suppose now that the population is *culled*, by an amount d, at the end of each time period. Show that :

$$p_n = \left(p_0 - \frac{d}{r}\right)(1+r)^n + \frac{d}{r}.$$

Find the value of d for which

    i. the population vanishes ;

    ii. the population remains stable ;

    iii. the population still grows.

Exercise 90 (*Drug Therapy*)

Equal doses, d, of a substance are administered at equal time intervals. Let s_n denote the amount of the substance in the blood at the beginning of period n. Suppose that $s_1 = d$ and that the fractional decrease, per period, in the amount of the substance in the blood is r.

(a) Obtain an expression for s_n ;

(b) Show that $s_n \to \frac{d}{r}$;

(c) If the dose $d = 100$ mg and the substance decreases by 25% per day, show that $s_n \to 400$.

Chapter 7

Linear Equations and Matrices

Topics :

1. SYSTEMS OF LINEAR EQUATIONS

2. MATRICES AND GAUSSIAN ELIMINATION

3. MATRIX OPERATIONS

Matrices are used to represent a variety of mathematical concepts. Matrices can be added and multiplied in ways similar to the ways in which numbers are added and multiplied, and these operations with matrices have far-reaching applications. For instance, matrices enable us to solve systems of linear equations and to do other computational problems in a *fast* and *efficient* manner.

7.1   Systems of linear equations

One of the most frequently recurring practical problems in many fields of study is that of solving a system of linear equations.

7.1.1 DEFINITION.   An equation of the form

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b$$

where $a_1, a_2, \ldots, a_n$ are (usually) real numbers, is called a **linear equation** in the **variables** (or **unknowns**) $x_1, x_2, \ldots, x_n$.

A **solution** to such a linear equation is an n-tuple of numbers $(s_1, s_2, \ldots, s_n)$ which *satisfy* the given equation.

7.1.2 EXAMPLE.   The triplet $(2, 3, -4)$ is a solution to the linear equation

$$6x_1 - 3x_2 + 4x_3 = -13$$

because

$$6 \cdot 2 - 3 \cdot 3 + 4 \cdot (-4) = -13.$$

7.1.3 DEFINITION.   A **system of m linear equations in n unknowns** (or, simply, a **linear system**) is a set of m linear equations in n unknowns.

A linear system can conveniently be written as

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m . \end{cases}$$

Thus the ith equation is

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i.$$

A **solution** to such a linear system is an n-tuple of numbers $(s_1, s_2, \ldots, s_n)$ which *satisfy* each equation of the system.

7.1.4 DEFINITION. If a linear system has no solution, it is said to be **inconsistent**. If it has a solution, it is called **consistent**.

If $b_1 = b_2 = \cdots = b_m = 0$, then the linear system is called **homogeneous**. The solution $x_1 = x_2 = \cdots = x_n = 0$ (that is, the n-tuple $(0, 0, \ldots, 0)$) to a homogeneous linear system is called the **trivial solution**. A solution to a homogeneous linear system in which not all of $x_1, x_2, \ldots, x_n$ are zero is called a **nontrivial solution**.

7.1.5 DEFINITION. Two linear systems are **equivalent** provided they have *exactly* the same solutions.

7.1.6 EXAMPLE. The linear system

$$\begin{cases} x_1 & - & 3x_2 = -7 \\ 2x_1 & + & x_2 = 7 \end{cases}$$

has only the solution $(2, 3)$. The linear system

$$\begin{cases} 8x_1 & - & 3x_2 = 7 \\ 3x_1 & - & 2x_2 = 0 \\ 10x_1 & - & 2x_2 = 14 \end{cases}$$

also has only the solution $(2, 3)$. Thus these linear systems are equivalent.

To find solutions to a linear system, we shall use a technique called the **method of elimination** ; that is, *we eliminate some variables by adding a multiple of one equation to another equation.* Elimination merely amounts to the development of a new linear system that is equivalent to the original system, but is much simpler to solve.

7.1.7 EXAMPLE. Consider the linear system

$$\begin{cases} x_1 & - & 3x_2 = -3 \\ 2x_1 & + & x_2 = 8. \end{cases}$$

To eliminate x_1, we add (-2) times the first equation to the second one, obtaining

$$7x_2 = 14.$$

Thus we have eliminated the unknown x_1. Then solving for x_2, we have

$$x_2 = 2$$

and substituting into the first equation, we obtain

$$x_1 = 3.$$

Then $(3, 2)$ is the *only* solution to the given linear system.

7.1.8 EXAMPLE.   Consider the linear system

$$\begin{cases} x_1 & - & 3x_2 = -7 \\ 2x_1 & - & 6x_2 = 7. \end{cases}$$

Again, we decide to eliminate x_1. We add (-2) times the first equation to the second one, obtaining

$$0 = 21$$

which makes no sense. This means that the given linear system has *no* solution : it is inconsistent.

7.1.9 EXAMPLE.   Consider the linear system

$$\begin{cases} x_1 & + & 2x_2 & - & 3x_3 = -4 \\ 2x_1 & + & x_2 & - & 3x_3 = 4. \end{cases}$$

Eliminating x_1, we add (-2) times the first equation to the second equation, to obtain

$$-3x_2 + 3x_3 = 12.$$

We must now solve this equation. A solution is

$$x_2 = x_3 - 4$$

where x_3 can be any real number. Then from the first equation of the system,

$$x_1 = -4 - 2x_2 + 3x_3 = -4 - 2(x_3 - 4) + 3x_3 = x_3 + 4.$$

Thus a solution to the given linear system is

$$x_1 = x_3 + 4, \quad x_2 = x_3 - 4, \quad x_3 = \text{ any real number.}$$

We may write such a solution as follows

$$(\alpha + 4, \alpha - 4, \alpha), \quad \alpha \in \mathbb{R}.$$

This means that the linear system has *infinitely many* solutions. Every time we assign a value α we obtain another solution.

NOTE : These examples suggest that *a linear system may have a unique solution, no solution, or infinitely many solutions.*

GEOMETRIC INTERPRETATION. Consider next a linear system of two equations in the unknowns x_1 and x_2 :

$$\begin{cases} a_1 x_1 & + & a_2 x_2 = c_1 \\ a_2 x_2 & + & a_2 x_2 = c_2 \,. \end{cases}$$

The graph of each of these equations is a straight line, which we denote by $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively. Then exactly one of the following situations must occur :

- the lines $\mathcal{L}_1$ and $\mathcal{L}_2$ intersect at a single point ;

- the lines $\mathcal{L}_1$ and $\mathcal{L}_2$ are parallel lines ;

- the lines $\mathcal{L}_1$ and $\mathcal{L}_2$ coincide - they actually are the same line.

If the pair (s_1, s_2) is a solution to the linear system, then the point (s_1, s_2) lies on both lines $\mathcal{L}_1$ and $\mathcal{L}_2$. Conversely, if the point (s_1, s_2) lies on both lines $\mathcal{L}_1$ and $\mathcal{L}_2$, then the pair (s_1, s_2) is a solution to the linear system. Thus we are led geometrically to the same three possibilities mentioned above.

If we examine the method of elimination more closely, we find that it involves three manipulations that can be performed on a linear system to convert it into an equivalent system. These manipulations, called **elementary operations**, are as follows :

- interchange the ith and j^{th} equations ;

- multiply an equation by a nonzero constant ;

- replace the ith equation by c times the jth equation plus the ith equation, $i \neq j$.

It is not difficult to prove that *performing these manipulations on a linear system leads to an equivalent system.*

7.2   Matrices and Gaussian elimination

If we examine the method of elimination described in the previous section, we make the following observation : only the numbers in front of the unknowns $x_1, x_2, \ldots, x_n$ and the numbers $b_1, b_2, \ldots, b_m$ on the right-hand side are being changed as we perform the steps in the method of elimination. Thus we might think of looking for a way of writing a linear system without having to carry along the unknowns. *Matrices* enable us to do this.

NOTE :   Their use is not, however, merely that of a convenient notation. As any good definition should do, the notion of a matrix provides not only a new way of looking at old problems but also gives rise to a great many new questions.

7.2.1 DEFINITION.   A **matrix** is a rectangular array of numbers denoted by

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}.$$

The ith **row** of A is

$$\begin{bmatrix} a_{i1} & a_{i2} & \ldots & a_{in} \end{bmatrix}, \quad 1 \leq i \leq m$$

while the jth **column** of A is

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}, \quad 1 \leq j \leq n.$$

If a matrix A has m rows and n columns, we say that A is an $m \times n$ **matrix** (read "m by n"). If $m = n$, we say that A is a **square matrix** of order n. We refer to a_{ij} as the (i,j) **entry** or the (i,j) **element** and we often write

$$A = [a_{ij}].$$

7.2.2 EXAMPLE.   Consider the matrices :

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & -1 & 0 \\ 0 & -3 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & -2 & 7 \end{bmatrix}, \quad C = \begin{bmatrix} 2 \\ -1 \\ 0 \\ 3 \end{bmatrix},$$

$$D = \begin{bmatrix} 2 & -1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad E = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}.$$

Here, A is 3×3, B is 1×3, C is 4×1, D is 3×2, and E is 2×2. In A, $a_{23} = 0$; in B, $b_{12} = -1$; in C, $c_{41} = 3$; in D, $d_{11} = 2$, and in E, $e_{12} = e_{21} = -1$.

Consider again a general system of m linear equations in the variables

$x_1, x_2, \ldots, x_n$:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \,. \end{cases}$$

NOTE :   Such a linear system may be written, in compact form, as follows :

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \,, \quad i = 1, 2, \ldots, m.$$

The **coefficient matrix** of such a linear system is the $m \times n$ matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}.$$

Let us write

$$b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

for the column of constants in the general system; this $m \times 1$ matrix is often called a **column vector**. When we adjoin the column vector b to the coefficient matrix A (as a final column), we get the matrix

$$[A \ b] = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{bmatrix}.$$

This $m \times (n+1)$ matrix is called the **augmented coefficient matrix** (or, simply, the **augmented matrix**) of the given linear system.

7.2.3 EXAMPLE.   The augmented matrix of the linear system

$$\begin{cases} 2x_1 & + & 3x_2 & - & 7x_3 & + & 4x_4 & = & 6 \\ & & x_2 & + & 3x_3 & - & 5x_4 & = & 0 \\ -x_1 & + & 2x_2 & & & - & 9x_4 & = & 17 \end{cases}$$

is the 3×5 matrix

$$\begin{bmatrix} 2 & 3 & -7 & 4 & 6 \\ 0 & 1 & 3 & -5 & 0 \\ -1 & 2 & 0 & -9 & 17 \end{bmatrix}.$$

In previous section we described the three elementary operations that are used in the method of elimination. To each of these corresponds an *elementary row operation* on the augmented matrix of the system.

7.2.4 DEFINITION.   The following are the three types of **elementary row operations** on the matrix A :

- interchange two rows of A ;

- multiply any (single) row of A by a nonzero constant ;

- add a constant multiple of one row of A to another row.

7.2.5 EXAMPLE.   Let

$$A = \begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ 3 & 3 & 6 & -9 \end{bmatrix}.$$

Interchanging rows 1 and 3 of A, we obtain

$$\begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ 3 & 3 & 6 & -9 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_3} \begin{bmatrix} 3 & 3 & 6 & -9 \\ 2 & 3 & 0 & -2 \\ 0 & 0 & 1 & 2 \end{bmatrix}.$$

Multiplying the third row of A by $\frac{1}{3}$, we obtain

$$\begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ 3 & 3 & 6 & -9 \end{bmatrix} \xrightarrow{(\frac{1}{3})R_3} \begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ 1 & 1 & 2 & -3 \end{bmatrix}.$$

Adding (-2) times row 2 to row 3 of A, we obtain

$$\begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ 3 & 3 & 6 & -9 \end{bmatrix} \xrightarrow{(-2)R_2+R_3} \begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ -1 & -3 & 6 & -5 \end{bmatrix}.$$

It is not self-evident that a sequence of elementary row operations produces a linear system which is equivalent to the original system. To state the pertinent result concisely, we need the following definition.

7.2.6 DEFINITION.   Two matrices are called **row-equivalent** provided one can be obtained from the other by a (finite) sequence of elementary operations.

7.2.7 EXAMPLE.   The matrix

$$A = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 2 \\ 1 & -1 & 2 & 3 \end{bmatrix}$$

is row equivalent to

$$B = \begin{bmatrix} 2 & 4 & 8 & 6 \\ 1 & -1 & 2 & 3 \\ 4 & -1 & 7 & 8 \end{bmatrix}$$

because

$$\begin{bmatrix} 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 2 \\ 1 & -1 & 2 & 3 \end{bmatrix} \xrightarrow{(2)R_3+R_2} \begin{bmatrix} 1 & 2 & 4 & 3 \\ 4 & -1 & 7 & 8 \\ 1 & -1 & 2 & 3 \end{bmatrix} \xrightarrow{R_2 \leftrightarrow R_3} \begin{bmatrix} 1 & 2 & 4 & 3 \\ 1 & -1 & 2 & 3 \\ 4 & -1 & 7 & 8 \end{bmatrix}$$

$$\xrightarrow{(2)R_1} \begin{bmatrix} 2 & 4 & 8 & 6 \\ 1 & -1 & 2 & 3 \\ 4 & -1 & 7 & 8 \end{bmatrix}.$$

The following result holds.

7.2.8 PROPOSITION.   *If the augmented coefficient matrices of two linear systems are row-equivalent, then the two systems are equivalent.*

Up to this point we have been somewhat informal in our description of the method of elimination : its objective is *to transform, by elementary row operations, a given linear system into one for which back substitution leads easily to a solution.* The following definition tells what should be the appearance of the augmented matrix of the transformed system.

7.2.9 DEFINITION.   A matrix E is in **(row) echelon form** provided it satisfies the following conditions :

(1)   every row of E that consists entirely of zeros (if any) lies *below* every row that contains a nonzero element ;

(2)   in each row of E that contains a nonzero element, the *first* nonzero element lies strictly to the *right* of the first nonzero element in the preceding row (if there is a preceding row).

Property 1 says that if E has any all-zero rows, then they are grouped together at the bottom of the matrix. The first (from left) *nonzero* element in each of the other rows is called its **leading entry** (or **pivot**).

NOTE :   One can always make the leading entries to be 1.

Property 2 says that the leading entries form a "descending staircase" pattern from upper left to lower right, as in the following echelon form matrix :

$$E = \begin{bmatrix} \mathbf{2} & -1 & 0 & 4 & 7 \\ 0 & \mathbf{1} & 2 & 0 & -3 \\ 0 & 0 & 0 & \mathbf{3} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Suppose that a linear system is in **echelon form** - its augmented matrix is in echelon form. Then those variables that correspond to *columns* containing

leading entries are called **leading** (or **basic**) **variables**; all the other (non-leading) variables are called **free variables**. The following algorithm describes the process of **back substitution** to solve such a system.

<div align="center">

Algorithm : Back substitution

</div>

To solve a consistent linear system in echelon form by back substitution, carry out the following steps :

1.   Set each free variable equal to an arbitrary parameter (a different parameter for each free variable).

2.   Solve the final (nonzero) equation for its leading variables.

3.   Substitute the result in the next-to-last equation and then solve for its leading variables.

4.   Continuing in this fashion, work upward through the system of equations until all variables have been determined.

7.2.10 EXAMPLE.   The augmented matrix of the linear system

$$\begin{cases} x_1 & - & 2x_2 & + & 3x_3 & + & 2x_4 & + & x_5 = 10 \\ & & & & x_3 & + & & & 2x_5 = -3 \\ & & & & & & x_4 & - & 4x_5 = 7 \end{cases}$$

is the echelon matrix

$$\begin{bmatrix} \mathbf{1} & -2 & 3 & 2 & 1 & 10 \\ 0 & 0 & \mathbf{1} & 0 & 2 & -3 \\ 0 & 0 & 0 & \mathbf{1} & -4 & 7 \end{bmatrix}.$$

The leading entries are in the first, third, and fourth columns. Hence, x_1, x_3 and x_4 are the leading variables, and x_2 and x_5 are the free variables. To solve the system by back substitution, we first write

$$x_2 = s \quad \text{and} \quad x_5 = t$$

where s and t are arbitrary parameters. Then the third equation gives

$$x_4 = 7 + 4x_5 = 7 + 4t \,;$$

the second equation gives

$$x_3 = -3 - 2x_5 = -3 - 2t \,;$$

finally, the first equation yields

$$x_1 = 10 + 2x_2 - 3x_3 - 2x_4 - x_5 = 5 + 2s - 3t.$$

Thus the linear system has infinitely many solutions $(x_1, x_2, x_3, x_4, x_5)$, given in terms of the two parameters s and t, as follows :

$$x_1 = 5 + 2s - 3t \,, \quad x_2 = s \,, \quad x_3 = -3 - 2t \,, \quad x_4 = 7 + 4t \,, \quad x_5 = t.$$

Alternatively, the *solution set* of the given linear system is

$$S = \{(5 + 2s - 3t, s, -3 - 2t, 7 + 4t, t) \,|\, s,\, t \in \mathbb{R}\}.$$

Because we can use back substitution to solve any linear system already in echelon form, it remains only to establish that we can transform any matrix (using elementary row operations) into an echelon form. This procedure is known as **Gaussian elimination** (named after the great German mathematician Carl F. Gauss (1777-1855)).

<p align="center">**Algorithm : Gaussian elimination**</p>

To transforme a matrix A into an echelon form, carry out the following steps :

1.   Locate the first column of A that contains a nonzero element.

2.   If the first (top) entry in this column is zero, interchange the first row of A with a row in which the corresponding entry is nonzero.

3.   Now the first entry in our column is nonzero. Replace the entries below it in the same column with zeroes by adding appropriate multiples of the first row of A to lower rows.

4.   Perform steps 1-3 on the lower right matrix A_1.

5.   Repeat the cycle of steps until an echelon form matrix is obtained.

7.2.11 EXAMPLE.   To solve the linear system

$$\begin{cases} x_1 & - & 2x_2 & + & 3x_3 & + & 2x_4 & + & x_5 = 10 \\ 2x_1 & - & 4x_2 & + & 8x_3 & + & 3x_4 & + & 10x_5 = 7 \\ 3x_1 & - & 6x_2 & + & 10x_3 & + & 6x_4 & + & 5x_5 = 27 \end{cases}$$

we reduce its augmented coefficient matrix to echelon form as follows :

$$\begin{bmatrix} 1 & -2 & 3 & 2 & 1 & 10 \\ 2 & -4 & 8 & 3 & 10 & 7 \\ 3 & -6 & 10 & 6 & 5 & 27 \end{bmatrix} \xrightarrow{(-2)R_1+R_2} \begin{bmatrix} 1 & -2 & 3 & 2 & 1 & 10 \\ 0 & 0 & 2 & -1 & 8 & -13 \\ 3 & -6 & 10 & 6 & 5 & 27 \end{bmatrix} \xrightarrow{(-3)R_1+R_3}$$

$$\begin{bmatrix} 1 & -2 & 3 & 2 & 1 & 10 \\ 0 & 0 & 2 & -1 & 8 & -13 \\ 0 & 0 & 1 & 0 & 2 & -3 \end{bmatrix} \xrightarrow{R_2\leftrightarrow R_3} \begin{bmatrix} 1 & -2 & 3 & 2 & 1 & 10 \\ 0 & 0 & 1 & 0 & 2 & -3 \\ 0 & 0 & 2 & -1 & 8 & -13 \end{bmatrix} \xrightarrow{(-2)R_2+R_3}$$

$$\begin{bmatrix} 1 & -2 & 3 & 2 & 1 & 10 \\ 0 & 0 & 1 & 0 & 2 & -3 \\ 0 & 0 & 0 & -1 & 4 & -7 \end{bmatrix} \xrightarrow{(-1)R_3} \begin{bmatrix} 1 & -2 & 3 & 2 & 1 & 10 \\ 0 & 0 & 1 & 0 & 2 & -3 \\ 0 & 0 & 0 & 1 & -4 & 7 \end{bmatrix} .$$

Our result is the echelon matrix in EXAMPLE 7.2.10, so the infinite solution set of the given linear system is

$$S = \{(5 + 2s - 3t, s, -3 - 2t, 7 + 4t, t) \,|\, s,\, t \in \mathbb{R}\}.$$

7.2.12 EXAMPLE.   To solve the linear system

$$\begin{cases} x_1 & + & 2x_2 & + & x_3 = 4 \\ 3x_1 & + & 8x_2 & + & 7x_3 = 20 \\ 2x_1 & + & 7x_2 & + & 9x_3 = 23 \end{cases}$$

whose augmented matrix is

$$\begin{bmatrix} 1 & 2 & 1 & 4 \\ 3 & 8 & 7 & 20 \\ 2 & 7 & 9 & 23 \end{bmatrix},$$

we carry the following sequence of elementary row operations :

$$\begin{bmatrix} 1 & 2 & 1 & 4 \\ 3 & 8 & 7 & 20 \\ 2 & 7 & 9 & 23 \end{bmatrix} \xrightarrow{(-3)R_1+R_2} \begin{bmatrix} 1 & 2 & 1 & 4 \\ 0 & 2 & 4 & 8 \\ 2 & 7 & 9 & 23 \end{bmatrix} \xrightarrow{(-2)R_1+R_3} \begin{bmatrix} 1 & 2 & 1 & 4 \\ 0 & 2 & 4 & 8 \\ 0 & 3 & 7 & 15 \end{bmatrix}$$

$$\xrightarrow{(\frac{1}{2})R_2} \begin{bmatrix} 1 & 2 & 1 & 4 \\ 0 & 1 & 2 & 4 \\ 0 & 3 & 7 & 15 \end{bmatrix} \xrightarrow{(-3)R_2+R_3} \begin{bmatrix} 1 & 2 & 1 & 4 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 3 \end{bmatrix}.$$

The final matrix here is the augmented matrix of the linear system

$$\begin{cases} x_1 & + & 2x_2 & + & x_3 = 4 \\ & & x_2 & + & 2x_3 = 4 \\ & & & & x_3 = 3, \end{cases}$$

whose *unique* solution (found by back substitution) is

$$x_1 = 5, \ x_2 = -2, \ x_3 = 3.$$

NOTE :   EXAMPLES 7.2.11 and 7.2.12 illustrate the ways in which Gaussian elimination can result in either a unique solution or infinitely many solutions. If the reduction of the augmented matrix to echelon form leads to a row of the form

$$\begin{bmatrix} 0 & 0 & \dots & 0 & * \end{bmatrix}$$

where the asterisc denotes a nonzero entry in the last column, then we have an inconsistent equation,

$$0x_1 + 0x_2 + \cdots + 0x_n = *$$

and therefore the linear system has no solution.

The structure of linear systems

The result of the process of Gaussian elimination is not uniquely determined. That is, two different sequences of elementary row operations, both starting with the same matrix A, may yield two different echelon matrices (each of course still row-equivalent to A). A full understanding of the structure of systems of linear equations depends upon the definition of a special class of echelon matrices - the *reduced echelon matrices.*

7.2.13 DEFINITION.   A matrix E is in **reduced (row) echelon form** provided

- E is in row echelon form.

- Each pivot (leading entry) is 1.

- All entries above each pivot are 0.

One can prove that

7.2.14 PROPOSITION.   *Every matrix is row-equivalent to precisely one reduced echelon form matrix.*

The following result(s) then follow :

7.2.15 PROPOSITION.   *A linear system has either*

- *no solution (it is inconsistent),*

- *exactly one solution (if the system is consistent and all variables are basic), or*

- *infinitely many solutions (if the system is consistent and there are free variables).*

In particular, a homogeneous linear system either has only the trivial solution or has infinitely many solutions.

7.2.16 COROLLARY. *A linear system with more variables than equations has either no solution or infinitely many solutions. In particular, a homogeneous linear system with more variables than equations has infinitely many solutions.*

7.2.17 EXAMPLE. The reduced row echelon forms of the augmented matrices of three systems are given below. How many solutions are there in each case ?

$$(1) \quad \begin{bmatrix} 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix} ; \quad (2) \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{bmatrix} ; \quad (3) \quad \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} .$$

SOLUTION : (1) Infinitely many solutions (the second variable is free).

(2) Exactly one solution (all variables are basic).

(3) No solutions (the third row represents the equation $0 = 1$).

NOTE : Let A be an $n \times n$ matrix. Then the homogeneous linear system with coefficient matrix A has only the trivial solution if and only if A is row-equivalent to the $n \times n$ identity matrix.

7.2.18 EXAMPLE. The 3×3 matrix

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 3 & 8 & 7 \\ 2 & 7 & 9 \end{bmatrix}$$

is row-equivalent to the 3×3 identity matrix (check !). Hence, the homogeneous linear system

$$\begin{cases} x_1 & + & 2x_2 & + & x_3 = 0 \\ 3x_1 & + & 8x_2 & + & 7x_3 = 0 \\ 2x_1 & + & 7x_2 & + & 9x_3 = 0 \end{cases}$$

with coefficient matrix A, has *only* the trivial solution.

7.3   Matrix operations

Matrices can be added and multiplied in ways similar to the ways in which numbers are added and multiplied.

7.3.1 DEFINITION.   Two matrices A and B of the *same size* are called **equal**, and we write $A = B$, provided that each element of A is equal to the corresponding element of B.

Thus, two matrices of the same size (the same number of rows and the same number of columns) are equal if they are *elementwise equal*.

7.3.2 EXAMPLE.   If

$$A = \begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 4 \\ 5 & 7 \end{bmatrix}, \quad \text{and} \quad C = \begin{bmatrix} 3 & 4 & 7 \\ 5 & 6 & 8 \end{bmatrix}$$

then $A \neq B$ because $a_{22} = 6$, whereas $b_{22} = 7$, and $A \neq C$ because the matrices A and C are not of the same size.

7.3.3 DEFINITION.   If $A = [a_{ij}]$ and $B = [b_{ij}]$ are matrices of the same size, their **sum** $A+B$ is the matrix obtained by adding corresponding elements of the matrices A and B. That is,

$$A + B := [a_{ij} + b_{ij}].$$

7.3.4 EXAMPLE.   If

$$A = \begin{bmatrix} 3 & 0 & -1 \\ 2 & -7 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} 4 & -3 & 6 \\ 9 & 0 & -2 \end{bmatrix}, \quad \text{and} \quad C = \begin{bmatrix} 3 & -2 \\ -1 & 6 \end{bmatrix}$$

then

$$A + B = \begin{bmatrix} 7 & -3 & 5 \\ 11 & -7 & 3 \end{bmatrix}.$$

But the sum $A + C$ is not defined because the matrices A and C are not of the same size.

7.3.5 DEFINITION.   If $A = [a_{ij}]$ is a matrix and r is a number, than rA is the matrix obtained by multiplying each element of A by r. That is,

$$rA := [ra_{ij}].$$

NOTE :   We also write

$$-A = (-1)A \quad \text{and} \quad A - B = A + (-B).$$

7.3.6 EXAMPLE.   If

$$A = \begin{bmatrix} 3 & 0 & -1 \\ 2 & -7 & 5 \end{bmatrix}, \quad \text{and} \quad B = \begin{bmatrix} 4 & -3 & 6 \\ 9 & 0 & -2 \end{bmatrix}$$

then

$$3A = \begin{bmatrix} 9 & 0 & -3 \\ 6 & -21 & 15 \end{bmatrix}, \quad -B = \begin{bmatrix} -4 & 3 & -6 \\ -9 & 0 & 2 \end{bmatrix}, \quad \text{and } 3A - B = \begin{bmatrix} 5 & 3 & -9 \\ -3 & -21 & 17 \end{bmatrix}.$$

We recall that a **column vector** (or simply **vector**) is merely an $n \times 1$ matrix. If

$$a = \begin{bmatrix} 6 \\ -2 \\ 1 \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} -2 \\ 0 \\ 3 \end{bmatrix}$$

we can form such (linear) combinations as

$$3a + 2b = 3\begin{bmatrix} 6 \\ -2 \\ 1 \end{bmatrix} + 2\begin{bmatrix} -2 \\ 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 14 \\ -6 \\ 9 \end{bmatrix}.$$

NOTE :   A column vector should not be confused with a row vector. A **row vector** is a $1 \times n$ (rather than $n \times 1$) matrix. For instance,

$$\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 3 & 2 & 1 \end{bmatrix}.$$

Given a linear system

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \quad i = 1, 2, \ldots, n$$

we may regard a solution of this system as a *vector*

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

whose elements satisfy each of the equations of the system.

7.3.7 EXAMPLE.   Consider the homogeneous linear system

$$\begin{cases} x_1 & + & 3x_2 & - & 15x_3 & + & 7x_4 = 0 \\ x_1 & + & 4x_2 & - & 19x_3 & + & 10x_4 = 0 \\ 2x_1 & + & 5x_2 & - & 26x_3 & + & 11x_4 = 0. \end{cases}$$

We find that the (reduced) echelon form of the augmented coefficient matrix of this system is

$$\begin{bmatrix} 1 & 0 & -3 & -2 & 0 \\ 0 & 1 & -4 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Hence, x_1 and x_2 are leading variables and x_3 and x_4 are free variables. We therefore see that the infinite solution set of the system is described by

$$x_4 = t, \ x_3 = s, \ x_2 = 4s - 3t, \ x_1 = 3s + 2t$$

in terms of the arbitrary parameters s and t. Now let us write the solution (x_1, x_2, x_3, x_4) in vector notation. We have

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 3s + 2t \\ 4s - 3t \\ s \\ t \end{bmatrix}$$

and "separating" the s and t parts gives

$$x = \begin{bmatrix} 3s \\ 4s \\ s \\ 0 \end{bmatrix} + \begin{bmatrix} 2t \\ -3t \\ 0 \\ t \end{bmatrix} = s \begin{bmatrix} 3 \\ 4 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} 2 \\ -3 \\ 0 \\ 1 \end{bmatrix}.$$

NOTE : This equation expresses in **vector form** the general solution of the given linear system. (It says that the vector x is a solution if and only if x is a *linear combination* of two particular solutions.)

7.3.8 DEFINITION. If $A = [a_{ij}]$ is an $m \times n$ matrix and $B = [b_{ij}]$ is an $n \times p$ matrix, their **product** AB is defined by

$$AB := [c_{ij}], \quad \text{where} \quad c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

NOTE : (1) The product AB is defined *only when* the number of columns of A is the same as the number of rows of B.

(2) The (i, j) entry in AB is obtained by using the ith row of A and the jth column of B. If $a_1, a_2, \ldots, a_m$ denote the m row vectors of A and $b_1, b_2, \ldots, b_n$ denote the n column vectors of B, then

$$AB = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} \begin{bmatrix} b_1 & b_2 & \ldots & b_n \end{bmatrix} = \begin{bmatrix} a_i b_j \end{bmatrix}, \quad \text{where} \quad a_i b_j := \sum_{k=1}^{n} a_{ik}b_{kj}.$$

One might ask *why matrix equality and matrix addition are defined elementwise while matrix multiplication appears to be much more complicated.* Only a thorough understanding of the composition of functions and the relationship that exists between matrices and what are called *linear mappings* would show that the definition of multiplication given here is the *natural* one.

7.3.9 EXAMPLE.   Let

$$A = \begin{bmatrix} 1 & 2 & -1 \\ 3 & 1 & 4 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} -2 & 5 \\ 4 & -3 \\ 2 & 1 \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} (1)(-2) + (2)(4) + (-1)(2) & (1)(5) + (2)(-3) + (-1)(1) \\ (3)(-2) + (1)(4) + (4)(2) & (3)(5) + (1)(-3) + (4)(1) \end{bmatrix} = \begin{bmatrix} 4 & -2 \\ 6 & 16 \end{bmatrix}.$$

7.3.10 EXAMPLE.   Let

$$A = \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} 2 & 3 \\ -2 & 2 \end{bmatrix} \quad \text{while} \quad BA = \begin{bmatrix} 1 & 7 \\ -1 & 3 \end{bmatrix}.$$

Thus $AB \neq BA$.

7.3.11 DEFINITION.   If $A = [a_{ij}]$ is an $m \times n$ matrix, the its **transpose** A^T is the $n \times m$ matrix defined by

$$A^T := [a_{ij}^T], \quad \text{where} \quad a_{ij}^T = a_{ji}.$$

Thus the transpose of A is obtained from A by interchanging the rows and columns of A.

7.3.12 EXAMPLE.   Let

$$A = \begin{bmatrix} 1 & 2 & 3 \\ -2 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 2 \\ 0 \\ 3 \end{bmatrix}.$$

Then

$$A^T = \begin{bmatrix} 1 & -2 \\ 2 & 0 \\ 3 & 1 \end{bmatrix} \quad \text{and} \quad B^T = \begin{bmatrix} 2 & 0 & 3 \end{bmatrix}.$$

The following (algebraic) properties of matrix operations hold :

Properties of matrix addition : *If* A, B *and* C *are matrices of appropriate size, then* :

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

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

Properties of scalar multiplication : *If* r *and* s *are real numbers, and* A *and* B *are matrices of appropriate size, then* :

(1) $(r + s)A = rA + sA$;

(2) $r(A + B) = rA + rB$;

(3) $r(sA) = (rs)A.$

Properties of matrix multiplication : *If* A, B *and* C *are matrices of appropriate size, then* :

(1) $A(BC) = (AB)C$;

(2) $(A + B)C = AC + BC$;

(3) $C(A + B) = CA + CB.$

Properties of transpose : *If* r *is a real number, and* A *and* B *are matrices of appropriate size, then* :

(1) $(A^T)^T = A$;

(2) $(A + B)^T = A^T + B^T$;

(3) $(rA)^T = rA^T$;

(4) $(AB)^T = B^T A^T$.

NOTE :   There are some differences between matrix multiplication and the multiplication of real numbers; for instance :

- AB need not equal BA ;

- AB may be the *zero matrix* (the matrix with all entries zero) with $A \neq O$ and $B \neq O$;

- AB may equal AC with $B \neq C$.

We introduce now some special types of matrices.

7.3.13 DEFINITION.   An $n \times n$ matrix $A = [a_{ij}]$ is called

- **diagonal matrix** if $a_{ij} = 0$ for $i \neq j$;

- the $n \times n$ **identity matrix**, denoted I_n, if $a_{ii} = 1$ and $a_{ij} = 0$ for $i \neq j$;

- **upper triangular matrix** if $a_{ij} = 0$ for $i > j$;

- **lower triangular matrix** if $a_{ij} = 0$ for $i < j$;

- **symmetric matrix** if $A^T = A$;

- **skew symmetric matrix** if $A^T = -A$;

- **orthogonal matrix** if $AA^T = I_n$;

- **nonsingular matrix** (or **invertible matrix**) if there exists an $n \times n$ matrix B such that $AB = BA = I_n$; such a B is called an **inverse** of A. (Otherwise, A is called **singular** or **noninvertible**.)

7.3.14 PROPOSITION.   *The inverse of a matrix, if it exists, is unique.*

PROOF :   Let B and C be inverses of A. Then

$$AB = BA = I_n \quad \text{and} \quad AC = CA = I_n.$$

We then have

$$B = BI_n = B(AC) = (BA)C = I_nC = C$$

which proves that the inverse of a matrix, if it exists, is unique.   □

Because of this uniqueness, we write the inverse of a nonsingular matrix A as A^{-1}. Thus

$$AA^{-1} = A^{-1}A = I_n.$$

7.3.15 EXAMPLE.   If

$$A = \begin{bmatrix} 4 & 9 \\ 3 & 7 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 7 & -9 \\ -3 & 4 \end{bmatrix}$$

then

$$AB = \begin{bmatrix} 4 & 9 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 7 & -9 \\ -3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \,;$$

By a similar computation we get $BA = I$.

7.3.16 EXAMPLE.   Let

$$A = \begin{bmatrix} 1 & -3 \\ -2 & 6 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

If the matrix B had the property that $AB = BA = I$, then

$$AB = \begin{bmatrix} 1 & -3 \\ -2 & 6 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a - 3c & b - 3d \\ -2a + 6c & -2b + 6d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Upon equating corresponding elements of AB and the 2×2 identity matrix, we find that

$$\begin{cases} a & - & 3c = 1 \\ -2a & + & 6c = 0 \\ b & - & 3d = 0 \\ -2b & + & 6d = 1. \end{cases}$$

It is clear that this system of linear equations is inconsistent (Why ?). Thus, there can exist *no* 2×2 matrix B such that $AB = I$.

NOTE :   *The* 2×2 *matrix*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is invertible if and only if $ad - bc \neq 0$, *in which case*

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

7.3.17 EXAMPLE.   If

$$A = \begin{bmatrix} 4 & 6 \\ 5 & 9 \end{bmatrix}$$

then $ad - bc = 36 - 30 = 6 \neq 0$, so

$$A^{-1} = \frac{1}{6} \begin{bmatrix} 9 & -6 \\ -5 & 4 \end{bmatrix} = \begin{bmatrix} \frac{3}{2} & -1 \\ -\frac{5}{6} & \frac{2}{3} \end{bmatrix}.$$

Properties of nonsingular matrices :   *If the matrices A and B of the same size are nonsingular, then :*

(1) A^{-1} *is nonsingular and* $(A^{-1})^{-1} = A$;

(2) A^T *is nonsingular and* $(A^T)^{-1} = (A^{-1})^T$;

(3) AB *is nonsingular and* $(AB)^{-1} = B^{-1}A^{-1}$.

Consider a system of n linear equations in variables $x_1, x_2, \ldots, x_n$

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \quad i = 1, 2, \ldots, n.$$

Recall that we can write this linear system in the compact form

$$A\,x = b$$

where

$$A = [a_{ij}], \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Suppose that A is nonsingular. Then A^{-1} exists and we can multiply $Ax = b$ by A^{-1} on both sides, obtaining

$$A^{-1}(Ax) = A^{-1}b$$

or

$$I_n x = x = A^{-1}b.$$

Moreover, $x = A^{-1}b$ is clearly a solution to the given linear system. Thus, if A is nonsingular, we have a *unique* solution.

7.3.18 EXAMPLE.   To solve the system

$$\begin{cases} 4x_1 & + & 6x_2 = 6 \\ 5x_1 & + & 9x_2 = 18 \end{cases}$$

we use the inverse of the coefficient matrix

$$A = \begin{bmatrix} 4 & 6 \\ 5 & 9 \end{bmatrix}.$$

We have

$$x = A^{-1}b = \begin{bmatrix} 4 & 6 \\ 5 & 9 \end{bmatrix}^{-1} \begin{bmatrix} 6 \\ 18 \end{bmatrix} = \begin{bmatrix} \frac{3}{2} & -1 \\ -\frac{5}{6} & \frac{2}{3} \end{bmatrix} \begin{bmatrix} 6 \\ 18 \end{bmatrix} = \begin{bmatrix} -9 \\ 7 \end{bmatrix}.$$

Thus $x_1 = -9$, $x_2 = 7$ is the unique solution.

The following result leads to a practical method for inverting matrices.

7.3.19 PROPOSITION.   *An $n \times n$ matrix is invertible if and only if it is row-equivalent to the $n \times n$ identity matrix I_n.*

Algorithm : Finding A^{-1}

To find the inverse A^{-1} of the nonsingular matrix A, carry out the following steps:

1. Find a sequence of elementary row operations that reduces A to the $n \times n$ identity matrix I_n.

2. Apply the same sequence of operations in the same order to I_n to transform it into A^{-1}.

NOTE :   As a practical matter, it generally is more convenient to carry out the two reductions - from A to I_n, and from I_n to A^{-1} - in parallel.

7.3.20 EXAMPLE.   Find the inverse of the 3×3 matrix

$$A = \begin{bmatrix} 4 & 3 & 2 \\ 5 & 6 & 3 \\ 3 & 5 & 2 \end{bmatrix}.$$

SOLUTION :   We want to reduce A to the 3×3 identity matrix I_3 while simultaneously performing the same sequence of row operations on I_3 to obtain A^{-1}. In order to carry out this process efficiently, we adjoin I_3 on the right of A to form the 3×6 matrix

$$\begin{bmatrix} 4 & 3 & 2 & 1 & 0 & 0 \\ 5 & 6 & 3 & 0 & 1 & 0 \\ 3 & 5 & 2 & 0 & 0 & 1 \end{bmatrix}.$$

We now apply the following sequence of elementary row operations to this 3×6 matrix (designed to transform its left half into the 3×3 identity matrix).

$$\begin{bmatrix} 4 & 3 & 2 & 1 & 0 & 0 \\ 5 & 6 & 3 & 0 & 1 & 0 \\ 3 & 5 & 2 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{(-1)R_3+R_1} \begin{bmatrix} 1 & -2 & 0 & 1 & 0 & 0 \\ 5 & 6 & 3 & 0 & 1 & 0 \\ 3 & 5 & 2 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{(-1)R_3+R_2}$$

$$\begin{bmatrix} 1 & -2 & 0 & 1 & 0 & -1 \\ 2 & 1 & 1 & 0 & 1 & -1 \\ 3 & 5 & 2 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{(-2)R_1+R_2} \begin{bmatrix} 1 & -2 & 0 & 1 & 0 & -1 \\ 0 & 5 & 1 & -2 & 1 & 1 \\ 3 & 5 & 2 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{(-3)R_1+R_3}$$

$$\begin{bmatrix} 1 & -2 & 0 & 1 & 0 & -1 \\ 0 & 5 & 1 & -2 & 1 & 1 \\ 0 & 11 & 2 & -3 & 0 & 4 \end{bmatrix} \xrightarrow{(-2)R_2+R_3} \begin{bmatrix} 1 & -2 & 0 & 1 & 0 & -1 \\ 0 & 5 & 1 & -2 & 1 & 1 \\ 0 & 1 & 0 & 1 & -2 & 2 \end{bmatrix} \xrightarrow{R_2 \leftrightarrow R_3}$$

$$\begin{bmatrix} 1 & -2 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 & -2 & 2 \\ 0 & 5 & 1 & -2 & 1 & 1 \end{bmatrix} \xrightarrow{(2)R_2+R_1} \begin{bmatrix} 1 & 0 & 0 & 3 & -4 & 3 \\ 0 & 1 & 0 & 1 & -2 & 2 \\ 0 & 5 & 1 & -2 & 1 & 1 \end{bmatrix} \xrightarrow{(-5)R_2+R_3}$$

$$\begin{bmatrix} 1 & 0 & 0 & 3 & -4 & 3 \\ 0 & 1 & 0 & 1 & -2 & 2 \\ 0 & 0 & 1 & -7 & 11 & -9 \end{bmatrix}.$$

Now that we have reduced the left half of the 3×6 matrix to I_3, we simply examine its right half to see that the inverse of A is

$$A^{-1} = \begin{bmatrix} 3 & -4 & 3 \\ 1 & -2 & 2 \\ -7 & 11 & -9 \end{bmatrix}.$$

7.4   Exercises

Exercise 91 Consider the linear system

$$\begin{cases} 2x_1 & - & x_2 = 5 \\ 4x_1 & - & 2x_2 = k. \end{cases}$$

(a) Determine a value of k so that the system is consistent.

(b) Determine a value of k so that the system is inconsistent.

(c) How many different values of k can be selected in part (b) ?

Exercise 92 Use elementary row operations to transform each augmented coefficient matrix to echelon form, and then solve the system by back substitution.

(a) $\begin{cases} 2x_1 & + & 8x_2 & + & 3x_3 = 2 \\ x_1 & + & 3x_2 & + & 2x_3 = 5 \\ 2x_1 & + & 7x_2 & + & 4x_3 = 8 \end{cases}$;

(b) $\begin{cases} 3x_1 & - & 6x_2 & + & x_3 & + & 13x_4 = & 15 \\ 3x_1 & - & 6x_2 & + & 3x_3 & + & 21x_4 = & 21 \\ 2x_1 & - & 4x_2 & + & 5x_3 & + & 26x_4 = & 23 \end{cases}$;

(c) $\begin{cases} 4x_1 & - & 2x_2 & - & 3x_3 & + & x_4 = & 3 \\ 2x_1 & - & 2x_2 & - & 5x_3 & & = & -10 \\ 4x_1 & + & x_2 & + & 2x_3 & + & x_4 = & 17 \\ 3x_1 & & & + & x_3 & + & x_4 = & 12 \end{cases}$

Exercise 93 Determine for what values of k each system has (i) a unique solution; (ii) no solution; (iii) infinitely many solutions.

(a) $\begin{cases} 3x & + & 2y = & 1 \\ 6x & + & 4y = & k \end{cases}$;

(b) $\begin{cases} 3x & + & 2y = & 0 \\ 6x & + & ky = & 0 \end{cases}$;

(c) $\begin{cases} 3x & + & 2y = & 1 \\ 7x & + & 5y = & k \end{cases}$;

(d) $\begin{cases} x & + & 2y & + & z = & 3 \\ 2x & - & y & - & 3z = & 5 \\ 4x & + & 3y & - & z = & k. \end{cases}$

Exercise 94 Under what condition on the constants a, b and c does the linear system

$$\begin{cases} 2x & - & y & + & 3z = & a \\ x & + & 2y & + & z = & b \\ 7x & + & 4y & + & 9z = & c \end{cases}$$

have a unique solution ? No solution ? Infinitely many solutions ?

Exercise 95 Find an equation relating a, b and c so that the linear system

$$\begin{cases} x & + & 2y & - & 3z = & a \\ 2x & + & 3y & + & 3z = & b \\ 5x & + & 9y & - & 6z = & c \end{cases}$$

is consistent for any values of a, b and c that satisfy that equation.

Exercise 96 For the matrices

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & -1 \\ 2 & 1 & 0 \\ 3 & 2 & 1 \end{bmatrix}, \quad D = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \quad E = \begin{bmatrix} 5 \end{bmatrix},$$

determine which of the 25 matrix products AA, AB, AC, ..., ED, EE are defined, and compute those which are defined.

Exercise 97

(a) Find a value of r and a value of s so that

$$AB^T = 0, \quad \text{where} \quad A = \begin{bmatrix} 1 & r & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} -2 & 2 & s \end{bmatrix}.$$

(b) If

$$\begin{bmatrix} a+b & c+d \\ c-d & a-b \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 10 & 2 \end{bmatrix},$$

find a, b, c and d.

Exercise 98 TRUE or FALSE ? For two invertible $n \times n$ matrices A and B

(a) $(I_n - A)(I_n + A) = I_n - A^2$.

(b) $(A + B)^2 = A^2 + 2AB + B^2$.

(c) A^2 is invertible, and $(A^2)^{-1} = (A^{-1})^2$.

(d) $A + B$ is invertible, and $(A + B)^{-1} = A^{-1} + B^{-1}$.

(e) $(A - B)(A + B) = A^2 - B^2$.

(f) $ABB^{-1}A^{-1} = I_n$.

(g) $ABA^{-1} = B$.

(h) $(ABA^{-1})^3 = AB^3A^{-1}$.

(i) $(I_n + A)(I_n + A^{-1}) = 2I_n + A + A^{-1}$

(j) $A^{-1}B$ is invertible, and $(A^{-1}B)^{-1} = B^{-1}A$.

Exercise 99

(a) If $A = [a_{ij}]$ is a $n \times n$ matrix, then the **trace** of A is defined as the sum of all elements on the main diagonal of A; that is,

$$\operatorname{tr}(A) := \sum_{i=1}^{n} a_{ii}.$$

Prove :

    i. $\operatorname{tr}(cA) = c \operatorname{tr}(A)$, where c is a real number.

    ii. $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$.

    iii. $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

    iv. $\operatorname{tr}(A^T) = \operatorname{tr}(A)$.

    v. $\operatorname{tr}(A^T A) \geq 0$.

(b) Show that there are *no* 2×2 matrices A and B such that

$$AB - BA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Exercise 100 Prove or disprove :

(a) For any $n \times n$ *diagonal* matrices A and B, $AB = BA$.

(b) For any $n \times n$ matrix A, $AA^T = A^T A$.

Exercise 101 Let A and B be matrices of appropriate size. Show that :

(a) A is *symmetric* if and only if

$$a_{ij} = a_{ji} \quad \text{for all} \quad i, j.$$

(b) A is *skew symmetric* if and only if

$$a_{ij} = -a_{ji} \quad \text{for all} \quad i, j.$$

(c) If A is *skew symmetric*, then the elements on the main diagonal of A are zero.

(d) If A is *symmetric*, then A^T is *symmetric*.

(e) AA^T and $A^T A$ are *symmetric*.

(f) $A + A^T$ is *symmetric* and $A - A^T$ is *skew symmetric*.

(g) If A and B are *symmetric*, then $A + B$ is *symmetric*.

(h) AB is *symmetric* if and only if $AB = BA$.

Exercise 102 Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Show that

$$A^2 = (a + d)A - (ad - bc)I_2.$$

This formula can be used to compute A^2 without an explicit matrix multiplication. It follows that

$$A^3 = (a + d)A^2 - (ad - bc)A$$

without an explicit matrix multiplication,

$$A^4 = (a + d)A^3 - (ad - bc)A^2,$$

and so on. Use this method to compute $A^2, A^3, A^4,$ and A^5 given

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Exercise 103 Find :

(a) a 2×2 matrix A with each element 1 or -1, such that $A^2 = I_2$.

(b) a 2×2 matrix A with each main diagonal element 0, such that $A^2 = I_2$.

(c) a 2×2 matrix A with each main diagonal element 0, such that $A^2 = -I_2$.

(d) all 2×2 matrices X such that

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} X = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

(e) all 2×2 matrices X which commute with $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.

(f) all 2×2 matrices X which commute with $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$.

(g) all 2×2 matrices X which commute with all 2×2 matrices.

Exercise 104 First find A^{-1} and then use A^{-1} to solve the linear system $Ax = b$.

(a) $A = \begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}$, $\quad b = \begin{bmatrix} 5 \\ 6 \end{bmatrix}$;

(b) $A = \begin{bmatrix} 7 & 9 \\ 5 & 7 \end{bmatrix}$, $\quad b = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$.

Exercise 105 Find the inverse A^{-1} of each given matrix A.

(a) $\begin{bmatrix} 1 & 5 & 1 \\ 2 & 5 & 0 \\ 2 & 7 & 1 \end{bmatrix}$;

(b) $\begin{bmatrix} 1 & 4 & 3 \\ 1 & 4 & 5 \\ 2 & 5 & 1 \end{bmatrix}$;

(c) $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 3 & 2 & 4 & 1 \end{bmatrix}$.

Chapter 8

Determinants

Topics :

1. DETERMINANTS

2. PROPERTIES OF DETERMINANTS

3. APPLICATIONS

Determinants are useful in further development of matrix theory and its applications. Throughout the 19th century determinants were considered the ultimate tool in linear algebra; recently, determinants have gone somewhat out of fashion. Nevertheless, it is still important to understand what a determinant is and to learn a few of its fundamental properties.

8.1   Determinants

In section **7.3** we found a criterion for the invertibility of a 2×2 matrix :

$$\text{the matrix } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ is invertible if (and only if) } ad - bc \neq 0.$$

8.1.1 DEFINITION.   The number $ad - bc$ is called the **determinant** of the matrix A.

There are several common notations for determinants :

$$\det(A) = \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

NOTE :   The determinant is actually a *function* that associates with each square matrix (of order 2) the number $\det(A)$.

If the matrix A is invertible, then its inverse can be expressed in terms of the determinant :

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} .$$

It is natural to ask whether the concept of a determinant can be generalized to square matrices of arbitrary size. Can we assign a number $\det(A)$ to any square matrix A (expressed in terms of the entries of A), such that A is invertible if (and only if) $\det(A)$?

The determinant of a 3×3 matrix

Let

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

be a 3×3 matrix. The following formula for the *determinant* of A may be obtained (by means of geometric considerations or otherwise) :

$$\det{(A)} = a_{11}a_{22}a_{33} - a_{11}a_{32}a_{23} + a_{21}a_{32}a_{13} - a_{21}a_{12}a_{33} + a_{31}a_{12}a_{23} - a_{31}a_{22}a_{13}.$$

Since the formula for the determinant of a 3×3 matrix is rather long, we may wonder how we can memorize it. Here is a convenient rule (stated by PIERRE F. SARRUS (1798-1861)) :

Sarrus' Rule : *To find the determinant of a 3×3 matrix A, write the first rows of A under A. Then multiply the entries along the six diagonals thus formed.*

$$
\begin{array}{ccc}
a_{11} & a_{12} & a_{13} \\
a_{21} & a_{22} & a_{23} \\
a_{31} & a_{32} & a_{33} \\
-\quad a_{11} & a_{12} & a_{13} \quad + \\
-\quad a_{21} & a_{22} & a_{23} \quad + \\
- & & +
\end{array}
$$

Add or subtract these diagonal products as shown in the diagram.

$$
\begin{aligned}
\det{(A)} \;=\;& a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} \\
& -a_{13}a_{22}a_{31} - a_{23}a_{32}a_{11} - a_{33}a_{12}a_{21}.
\end{aligned}
$$

8.1.2 EXAMPLE.   Find
$$
\det
\begin{bmatrix}
1 & 2 & 3 \\
4 & 5 & 6 \\
7 & 8 & 10
\end{bmatrix}.
$$

SOLUTION :   We have

$$\det{(A)} = 1 \cdot 5 \cdot 10 + 4 \cdot 8 \cdot 3 + 2 \cdot 6 \cdot 7 - 3 \cdot 5 \cdot 7 - 6 \cdot 8 \cdot 1 - 10 \cdot 2 \cdot 4 = -3.$$

This matrix is invertible.

8.1.3 EXAMPLE.   Find the determinant of the upper triangular matrix

$$
A =
\begin{bmatrix}
a & b & c \\
0 & d & e \\
0 & 0 & f
\end{bmatrix}.
$$

SOLUTION :   We find that $\det(A) = adf$ because all other contributions in Sarrus' formula are zero.

NOTE :   The determinant of an upper (or lower) triangular 3×3 matrix is the product of its diagonal entries.

The determinant of an $n \times n$ matrix

We may be tempted to define the determinant of an $n \times n$ matrix by generalizing Sarrus' rule. For a 4×4 matrix, a naïve generalization of Sarrus' rule produces the expression :

$a_{11}a_{22}a_{33}a_{44} + \cdots + a_{14}a_{21}a_{32}a_{41} - a_{14}a_{23}a_{32}a_{41} - \cdots - a_{13}a_{22}a_{31}a_{44}$ (8 terms).

For example, for the *invertible* matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

the expression given by a "generalization" of Sarrus' rule is 0. This shows that we cannot define the determinant by generalizing Sarrus' rule in this way : recall that the determinant of an invertible matrix must be nonzero.

We have a look for a more subtle structure in the formula

$$\begin{aligned} \det(A) \quad = \quad & a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} \\ & -a_{13}a_{22}a_{31} - a_{23}a_{32}a_{11} - a_{33}a_{12}a_{21} \end{aligned}$$

for the determinant of a 3×3 matrix. Note that each of the six terms in this expression is a product of three factors involving exactly one entry from each row and column of the matrix. For lack of a better word, we call such a choice of a number in each row and column of a square matrix a **pattern** in the matrix. Observe that each pattern corresponds to a *permutation* on

3 elements. For example, the *diagonal pattern* – were we choose all diagonal entries a_{ii} – corresponds to the identity $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$. Clearly, there are $3! = 6$ such patterns.

When we compute the determinant of a 3×3 matrix, the product associated with a pattern (and hence a permutation) is added if the permutation is even and is substracted if the permutation is odd. Using this observation as a guide, we now define the determinant of a general $n \times n$ matrix.

8.1.4 DEFINITION. For an $n \times n$ matrix $A = [a_{ij}]$, the **determinant** of A is defined to be the number

$$\boxed{\det(A) := \sum_{\alpha \in S_n} \operatorname{sgn}(\alpha)\, a_{1\alpha(1)} a_{2\alpha(2)} \cdots a_{n\alpha(n)}.}$$

NOTE : The determinant of a non-square matrix is not defined.

8.1.5 EXAMPLE. When A is a 2×2 matrix, there are $2! = 2$ patterns (permutations on 2 elements), namely (in cycle notation) $\iota = (1)(2)$ and $(1, 2)$. So $\det(A)$ contains two terms :

$$\operatorname{sgn}(\iota)\, a_{11} a_{22} \quad \text{and} \quad \operatorname{sgn}((1,2))\, a_{12} a_{21}.$$

Since $\operatorname{sgn}(\iota) = +1$ and $\operatorname{sgn}((1,2)) = -1$, we obtain the familiar formula

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11} a_{22} - a_{12} a_{21}.$$

8.1.6 EXAMPLE. Find $\det(A)$ for

$$A = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 0 & 9 \end{bmatrix}.$$

SOLUTION :   The diagonal pattern makes the contribution $2 \cdot 3 \cdot 5 \cdot 7 \cdot 9 = 1\,890$. All other patterns contain at least one zero and will therefore make no contribution toward the determinant. We can conclude that

$$\det (A) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 9 = 1\,890.$$

NOTE :   More generally, the determinant of a diagonal matrix is the product of the diagonal entries of the matrix.

8.1.7 EXAMPLE.   Evaluate

$$\det \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 3 & 4 & 5 \\ 0 & 0 & 3 & 4 & 5 \\ 0 & 0 & 0 & 4 & 5 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix} .$$

SOLUTION :   Note that the matrix is upper triangular. The diagonal pattern makes the contribution $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$. Any pattern other than the diagonal pattern contains at least one entry below the diagonal, and the contribution the pattern makes to the determinant is therefore 0. We conclude that

$$\det (A) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120.$$

We can easily generalize this result :

8.1.8 PROPOSITION.   *The determinant of an (upper or lower) triangular matrix is the product of the diagonal entries of the matrix.*

8.2   Properties of determinants

The main goal of this section is to show that *a square matrix of any size is invertible if (and only if) its determinant is nonzero.* As we work toward this goal, we will discuss a number of other properties of the determinant that are of interest in their own right.

Determinant of the transpose

8.2.1 EXAMPLE.   Let

$$
A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 8 \\ 7 & 6 & 5 & 4 & 3 \\ 2 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \end{bmatrix}.
$$

Express $\det(A^T)$ in terms of $\det(A)$. You need *not* compute $\det(A)$.

SOLUTION :   For each pattern in A we can consider the corresponding (transposed) pattern in A^T. The two patterns (in A and A^T) - viewed as permutations on 5 elements – are inverse to each other. But a permutation and its inverse have the same signature, and thus the two patterns make the same contributions to the respective determinants. Since these observations apply to all patterns of A, we can conclude that $\det(A^T) = \det(A)$.

Since we have not used any special properties of the matrix A in example above, we can state more generally :

Property 1 : *If A^T is the transpose of the matrix A, then* $\det(A^T) = \det(A)$.

NOTE :   Any property of the determinant expressed in terms of rows holds for the columns as well, and vice versa.

Linearity properties of the determinant

8.2.2 EXAMPLE.   Consider the matrix

$$
B = \begin{bmatrix} 1 & x_1 + y_1 & 4 \\ 2 & x_2 + y_2 & 5 \\ 3 & x_3 + y_3 & 6 \end{bmatrix}.
$$

Express $\det(B)$ in terms of

$$\det \begin{bmatrix} 1 & x_1 & 4 \\ 2 & x_2 & 5 \\ 3 & x_3 & 6 \end{bmatrix} \quad \text{and} \quad \det \begin{bmatrix} 1 & y_1 & 4 \\ 2 & y_2 & 5 \\ 3 & y_3 & 6 \end{bmatrix}.$$

SOLUTION :   We have

$$
\begin{aligned}
\det(B) &= 3(x_1 + y_1) - 6(x_2 + y_2) + 3(x_3 + y_3) \\
&= (3x_1 - 6x_2 + 3x_3) + (3y_1 - 6y_2 + 3y_3) \\
&= \det \begin{bmatrix} 1 & x_1 & 4 \\ 2 & x_2 & 5 \\ 3 & x_3 & 6 \end{bmatrix} + \det \begin{bmatrix} 1 & y_1 & 4 \\ 2 & y_2 & 5 \\ 3 & y_3 & 6 \end{bmatrix}.
\end{aligned}
$$

8.2.3 EXAMPLE.   Consider the matrix

$$B = \begin{bmatrix} 1 & kx & 4 \\ 2 & ky & 5 \\ 3 & kz & 6 \end{bmatrix}.$$

Express $\det(B)$ in terms of

$$\det \begin{bmatrix} 1 & x & 4 \\ 2 & y & 5 \\ 3 & z & 6 \end{bmatrix}.$$

SOLUTION :   We have

$$
\begin{aligned}
\det(B) &= 3kx - 6ky + 3kz \\
&= k(3x - 6y + 3z) \\
&= k \cdot \det \begin{bmatrix} 1 & x & 4 \\ 2 & y & 5 \\ 3 & z & 6 \end{bmatrix}.
\end{aligned}
$$

NOTE :   The mapping

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \mapsto \det \begin{bmatrix} 1 & x & 4 \\ 2 & y & 5 \\ 3 & z & 6 \end{bmatrix}$$

(satisfying the above two properties) is said to be *linear* (see section **10.1**).

We can generalize :

Property 2 : *Suppose that the matrices* $A_1, A_2,$ *and* B *are identical, except for their* j^{th} *column, and that the* j^{th} *column of* B *is the sum of the* j^{th} *columns of* A_1 *and* A_2. *Then*

$$\det(B) = \det(A_1) + \det(A_2).$$

This result also holds if rows are involved instead of columns.

Property 3 : *Suppose that the matrices* A *and* B *are identical, except for their* j^{th} *column, and that the* j^{th} *column of* B *is* k *times the* j^{th} *column of* A. *Then*

$$\det(B) = k \cdot \det(A).$$

This result also holds if rows are involved instead of columns.

Elementary row operations and determinants

Suppose we have to find the determinant of a 20×20 matrix. Since there are $20! \approx 2 \cdot 10^{18}$ patterns in this matrix, we would have to perform more than 10^{19} multiplications to compute the determinant using DEFINITION 8.1.4. Even if a computer performed 1 billion multiplications a second, it would still take over $1\,000$ years to carry out these computations. Clearly, we have to look for more efficient ways to compute the determinant.

So far, we have found Gaussian elimination (reduction) to be a powerful tool for solving numerical problems in *linear algebra*. If we could understand what happens to the determinant of a matrix as we *row-reduce* it, we could use Gaussian elimination to compute determinants as well.

We have to understand what happens to the determinant of a matrix as we perform the three elementary row operations : (a) swapping two rows, (b) multiplying a row by a scalar, and (c) adding a multiple of a row to another row.

One can prove the following results.

Property 4 : *If B is obtained from A by a row swap, then*

$$\det(B) = -\det(A).$$

Property 5 : *If B is obtained from A by multiplying a row of A by a scalar k, then*

$$\det(B) = k \cdot \det(A).$$

Property 6 : *If B is obtained from A by adding a multiple of a row of A to another row, then*

$$\det(B) = \det(A).$$

NOTE :   Analogous results hold for elementary column operations.

8.2.4 EXAMPLE.   If a matrix A has two equal rows, what can we say about $\det(A)$?

SOLUTION :   Swap the two equal rows and call the resulting matrix B. Since we have swapped two *equal* rows, we have $B = A$. Now

$$\det(A) = \det(B) = -\det(A)$$

so that

$$\det(A) = 0.$$

Now that we understand how elementary row operations affect determinants, we can describe the relationship between the determinant of a matrix A and that of its reduced row echelon form rref (A).

Suppose that in the course of the row-reduction we swap rows s times and *divide* various rows by scalars $k_1, k_2, \ldots, k_r$. Then

$$\det(\mathrm{rref}(A)) = (-1)^s \frac{1}{k_1 k_2 \cdots k_r} \det(A)$$

or

$$\det(A) = (-1)^s k_1 k_2 \cdots k_r \det(\mathrm{rref}(A)).$$

Let us examine the cases when A is invertible and when it is not.

If A is invertible, then $\mathrm{rref}\,(A) = I_n$, so that $\det\,(\mathrm{rref}\,(A)) = 1$, and

$$\det\,(A) = (-1)^s k_1 k_2 \cdots k_r.$$

Observe that this quantity is not 0 because all the scalars k_i are different from 0.

If A is not invertible, then $\mathrm{rref}\,(A)$ is an upper triangular matrix with some zeros on the diagonal, so that $\det\,(\mathrm{rref}\,(A)) = 0$ and $\det\,(A) = 0$. We have established the following fundamental result :

8.2.5 PROPOSITION.   *A square matrix A is invertible if and only if $\det\,(A) \neq 0$.*

If A is invertible, the discussion above also produces a convenient method to compute the determinant :

Algorithm : *Consider an invertible matrix. Suppose you swap rows s times as you row-reduce A and you divide various rows by the scalars $k_1, k_2, \ldots, k_r$. Then*

$$\boxed{\det\,(A) = (-1)^s k_1 k_2 \cdots k_r \,.}$$

NOTE :   Here, it is not necessary to reduce A all the way to $\mathrm{rref}\,(A)$. It suffices to bring A into upper triangular form with $1'$s on the diagonal.

8.2.6 EXAMPLE.   Evaluate

$$\begin{vmatrix} 0 & 2 & 4 & 6 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 2 & -1 \\ 1 & 1 & 1 & 2 \end{vmatrix}.$$

SOLUTION :   We have

$$
\begin{vmatrix} 0 & 2 & 4 & 6 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 2 & -1 \\ 1 & 1 & 1 & 2 \end{vmatrix} = - \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 2 & 4 & 6 \\ 1 & 1 & 2 & -1 \\ 1 & 1 & 1 & 2 \end{vmatrix} = -2 \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & -1 \\ 1 & 1 & 1 & 2 \end{vmatrix} = -2 \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & -2 \\ 0 & 0 & -1 & 1 \end{vmatrix}
$$

$$
= 2 \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -2 \end{vmatrix} = 2(-1)(-2) \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 4 \, .
$$

We made two swaps and performed row divisions by 2, −1, −2, so that

$$
\det\,(A) = (-1)^2 \cdot 2 \cdot (-1) \cdot (-2) = 4.
$$

The determinant of a product

Consider two $n \times n$ matrices A and B. What is the relationship between $\det\,(A)$ and $\det\,(B)$?

First suppose that A is invertible. On can show that

$$
\mathrm{rref}\,[A \;\; AB] = [I_n \;\; B] \, .
$$

Suppose we swap rows s times and divide rows by $k_1, k_2, \ldots k_r$ as we perform the elimination.

Considering the left and right "halves" of the matrices separately, we conclude that

$$
\det\,(A) = (-1)^s k_1 k_2 \cdots k_r \, \det\,(I_n) = (-1)^s k_1 k_2 \cdots k_r
$$

and

$$
\det\,(AB) = (-1)^s k_1 k_2 \cdots k_r \, \det\,(B) = \det\,(A) \cdot \det\,(B) \, .
$$

Therefore, $\det\,(AB) = \det\,(A) \cdot \det\,(B)$ when A is invertible. If A is not invertible, then neither is AB, so that $\det\,(AB) = \det\,(A) \cdot \det\,(B) = 0.$

We have obtained the following result :

Property 7 : *If A and B are square matrices, then*

$$\det{(AB)} = \det{(A)} \cdot \det{(B)}.$$

8.2.7 EXAMPLE.   If A is an invertible $n \times n$ matrix, what is the relationship between $\det{(A)}$ and $\det{(A^{-1})}$?

SOLUTION :   By definition of the inverse matrix, we have

$$AA^{-1} = I_n \,.$$

By taking the determinant of both sides, we find that

$$\det{(AA^{-1})} = \det{(A)} \cdot \det{(A^{-1})} = \det{(I_n)} = 1.$$

NOTE :   If A is an *invertible* matrix, then

$$\boxed{\det{(A^{-1})} = \frac{1}{\det{(A)}} \cdot}$$

8.2.8 EXAMPLE.   If S is an invertible $n \times n$ matrix, and A an arbitrary $n \times n$ matrix, what is the relationship between $\det{(A)}$ and $\det{(S^{-1}AS)}$?

SOLUTION :   We have

$$
\begin{aligned}
\det{(S^{-1}AS)} &= \det{(S^{-1})} \cdot \det{(A)} \cdot \det{(S)} \\
&= (\det{(S)})^{-1} \cdot \det{(A)} \cdot \det{(S)} \\
&= \det{(A)}.
\end{aligned}
$$

Thus, $\det{(S^{-1}AS)} = \det{(A)}$.

<div align="center">

Laplace expansion

</div>

Recall the formula

$$\det{(A)} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

for the determinat of a 3×3 matrix. Collecting the two terms involving a_{11} and then those involving a_{21} and a_{31}, we can write :

$$
\begin{aligned}
\det(A) \;=\; & a_{11}(a_{22}a_{33} - a_{32}a_{23}) + \\
& a_{21}(a_{32}a_{13} - a_{12}a_{33}) + \\
& a_{31}(a_{12}a_{23} - a_{22}a_{13}).
\end{aligned}
$$

Let us analyze the structure of this formula more closely. The terms $(a_{22}a_{33} - a_{32}a_{23})$, $(a_{32}a_{13} - a_{12}a_{33})$, and $(a_{12}a_{23} - a_{22}a_{13})$ can be thought of as the determinants of *submatrices* of A, as follows. The expression $a_{22}a_{33} - a_{32}a_{23}$ is the determinant of the matrix we get when we omit the first row and thew first column of A ; likewise for the other summands.

To state these observations more succintly, we introduce some terminology.

8.2.9 DEFINITION.   Let $A = [a_{ij}]$ be an $n \times n$ matrix. The (i,j) **minor** of A is the determinant M_{ij} of the $(n-1) \times (n-1)$ submatrix that remains after deleting the ith row and the jth column of A. The (i,j) **cofactor** A_{ij} of A is defined to be

$$
A_{ij} := (-1)^{i+j} M_{ij}.
$$

8.2.10 EXAMPLE.   Let

$$
A = \begin{bmatrix} 5 & -2 & -3 \\ 4 & 0 & 1 \\ 3 & -1 & 2 \end{bmatrix}.
$$

Then

$$
A_{11} = M_{11} = \begin{vmatrix} 0 & 1 \\ -1 & 2 \end{vmatrix}, \quad A_{12} = -M_{12} = -\begin{vmatrix} 4 & 1 \\ 3 & 2 \end{vmatrix}, \quad A_{13} = M_{13} = \begin{vmatrix} 4 & 0 \\ 3 & -1 \end{vmatrix},
$$

$$
A_{21} = -M_{21} = -\begin{vmatrix} -2 & -3 \\ -1 & 2 \end{vmatrix}, \quad A_{22} = M_{22} = \begin{vmatrix} 5 & -3 \\ 3 & 2 \end{vmatrix}, \quad A_{23} = -M_{23} = -\begin{vmatrix} 5 & -2 \\ 3 & -1 \end{vmatrix},
$$

$$
A_{31} = M_{31} = \begin{vmatrix} -2 & -3 \\ 0 & 1 \end{vmatrix}, \quad A_{32} = -M_{32} = -\begin{vmatrix} 5 & -3 \\ 4 & 1 \end{vmatrix}, \quad A_{33} = M_{33} = \begin{vmatrix} 5 & -2 \\ 4 & 0 \end{vmatrix}.
$$

We can now represent the determinant of a 3×3 matrix more succinctly :

$$\det(A) = a_{11}A_{11} + a_{21}A_{21} + a_{31}A_{31}.$$

This representation of the determinant is called the **Laplace expansion of** $\det(A)$ **down the first column** (named after the French mathematician PIERRE-SIMON LAPLACE (1749-1827)).

Likewise, we can expand along the first *row* (since $\det(A^T) = \det(A)$) :

$$\det(A) = a_{11}A_{11} + a_{12}A_{12} + a_{13}A_{13}.$$

In fact, we can expand along *any* row or down *any* column (we can verify this directly, or argue in terms of row and column swap).

Laplace expansion : *The determinant $\det(A) = |a_{ij}|$ of an $n \times n$ matrix $A = [a_{ij}]$ can be computed by Laplace expansion along any row or down any column.*

Expansion along the ith row :

$$\boxed{\det(A) = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}.}$$

Expansion down the jth column :

$$\boxed{\det(A) = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj}.}$$

8.2.11 EXAMPLE.   If

$$A = \begin{bmatrix} 5 & -2 & -3 \\ 4 & 0 & 1 \\ 3 & -1 & 2 \end{bmatrix}$$

then

$$\begin{aligned} \det(A) &= a_{11}A_{11} + a_{12}A_{12} + a_{13}A_{13} \\ &= (5)\begin{vmatrix} 0 & 1 \\ -1 & 2 \end{vmatrix} - (-2)\begin{vmatrix} 4 & 1 \\ 3 & 2 \end{vmatrix} + (-3)\begin{vmatrix} 4 & 0 \\ 3 & -1 \end{vmatrix} \\ &= (5)(1) + (2)(5) - (3)(-4) \\ &= 27. \end{aligned}$$

8.2.12 EXAMPLE. To evaluate the determinant of

$$A = \begin{bmatrix} 7 & 6 & 0 \\ 9 & -3 & 2 \\ 4 & 5 & 0 \end{bmatrix}$$

we expand along the third column because it has only a single nonzero entry. Thus

$$\det(A) = -(2) \begin{vmatrix} 7 & 6 \\ 4 & 5 \end{vmatrix} = (-2)(35 - 24) = -22.$$

NOTE : Computing the determinant using Laplace expansion is a bit more efficient than using the definition of the determinant, but is a lot less efficient than Gaussian elimination.

8.3   Applications

Cramer's rule

Suppose that we need to solve the linear system

$$Ax = b$$

where

$$A = \begin{bmatrix} a_{ij} \end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

We assume that the coefficient matrix A is invertible, so we know in advance that a unique solution x exists. The question is how to write x explicitly in terms of the coefficients a_{ij} and the constants b_i. In the following discussion we think of x as a fixed (though as yet unknown) column vector.

If we denote by $a_1, a_2, \ldots, a_n$ the column vectors of the matrix A, then

$$A = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \end{bmatrix}.$$

The column vector b is expressed in terms of the entries $x_1, x_2, \ldots, x_n$ of the solution vector x and the columns vectors of A by

$$b = \sum_{j=1}^{n} x_j a_j.$$

The *trick* for finding the ith unknown x_i is to compute the determinant of the matrix

$$\begin{bmatrix} a_1 & \ldots & b & \ldots & a_n \end{bmatrix} = \begin{bmatrix} a_{11} & \ldots & b_1 & \ldots & a_{1n} \\ a_{21} & \ldots & b_2 & \ldots & a_{2n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \ldots & b_n & \ldots & a_{nn} \end{bmatrix}$$

that we obtain by replacing the ith column a_i of A with the column vector b. We find that

$$\begin{aligned}
\det \begin{bmatrix} a_1 & \ldots & b & \ldots & a_n \end{bmatrix} &= \det \begin{bmatrix} a_1 & \ldots & \sum_{j=1}^{n} x_j a_j & \ldots & a_n \end{bmatrix} \\
&= \sum_{j=1}^{n} \det \begin{bmatrix} a_1 & \ldots & x_j a_j & \ldots & a_n \end{bmatrix} \\
&= \sum_{j=1}^{n} x_j \det \begin{bmatrix} a_1 & \ldots & a_j & \ldots & a_n \end{bmatrix} \\
&= x_i \det \begin{bmatrix} a_1 & \ldots & a_i & \ldots & a_n \end{bmatrix} \\
&= x_i \det(A).
\end{aligned}$$

We get the desired simple formula for x_i after we divide each side by $\det(A) \neq 0$. Thus, we have obtained the following result :

Cramer's Rule :   *Consider the $n \times n$ linear system*

$$Ax = b$$

with

$$A = \begin{bmatrix} a_1 & \ldots & a_i & \ldots & a_n \end{bmatrix}.$$

If $\det(A) \neq 0$, *then the* i^{th} *entry of the unique solution (vector)* x *is given by*

$$
x_i = \frac{\det \begin{bmatrix} a_1 & \dots & b & \dots & a_n \end{bmatrix}}{\det(A)} = \frac{1}{\det(A)} \begin{vmatrix} a_{11} & \dots & b_1 & \dots & a_{1n} \\ a_{21} & \dots & b_2 & \dots & a_{2n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & b_n & \dots & a_{nn} \end{vmatrix}
$$

where in the last expression the constant vector b *replaces the* i^{th} *column vector* a_i *of* A.

NOTE :   This result is due to the Swiss mathematician GABRIEL CRAMER (1704-1752).

8.3.1 EXAMPLE.   Use Cramer's rule to solve the system :

$$
\begin{cases}
x_1 & + & 4x_2 & + & 5x_3 & = 2 \\
4x_1 & + & 2x_2 & + & 5x_3 & = 3 \\
-3x_1 & + & 3x_2 & - & x_3 & = 1.
\end{cases}
$$

SOLUTION :   We find that

$$
\det(A) = \begin{vmatrix} 1 & 4 & 5 \\ 4 & 2 & 5 \\ -3 & 3 & -1 \end{vmatrix} = 29
$$

and then

$$
x_1 = \frac{1}{29} \begin{vmatrix} 2 & 4 & 5 \\ 3 & 2 & 5 \\ 1 & 3 & -1 \end{vmatrix} = \frac{33}{29}, \quad x_2 = \frac{1}{29} \begin{vmatrix} 1 & 2 & 5 \\ 4 & 3 & 5 \\ -3 & 1 & -1 \end{vmatrix} = \frac{35}{29}
$$

$$
\text{and} \quad x_3 = \frac{1}{29} \begin{vmatrix} 1 & 4 & 2 \\ 4 & 2 & 3 \\ -3 & 3 & 1 \end{vmatrix} = -\frac{23}{29}.
$$

The adjoint formula for the inverse matrix

We now use Cramer's rule to develop an explicit formula for the inverse A^{-1} of the invertible matrix A. First we need to rewrite Cramer's rule more concisely. We have

$$x_i = \frac{1}{\det{(A)}} \left(b_1 A_{1i} + b_2 A_{2i} + \cdots + b_n A_{ni} \right), \quad i = 1, 2, \ldots, n$$

because the cofactor of b_k is simply the (k, i)-cofactor A_{ki} of A, and so

$$
x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \frac{1}{\det{(A)}} \begin{bmatrix} b_1 A_{11} + b_2 A_{21} + \cdots + b_n A_{n1} \\ b_1 A_{12} + b_2 A_{22} + \cdots + b_n A_{n2} \\ \vdots \\ b_1 A_{1n} + b_2 A_{2n} + \cdots + b_n A_{nn} \end{bmatrix}
$$

$$
= \frac{1}{\det{(A)}} \begin{bmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & A_{22} & \ldots & A_{n2} \\ \vdots & \vdots & & \vdots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

$$
= \frac{1}{\det{(A)}} \left[A_{ij} \right]^T b.
$$

NOTE : The transpose of the cofactor matrix of A is called the **adjoint matrix** of A and is denoted by

$$\operatorname{adj}{(A)} := \left[A_{ij} \right]^T.$$

With the aid of this notation, *Cramer's rule can be written in the especially simple form*

$$x = \frac{1}{\det{(A)}} \operatorname{adj}{(A)}\, b.$$

The fact that the formula above gives the *unique* solution $x \left(= A^{-1} b \right)$ of $Ax = b$ implies

$$A^{-1} b = \frac{1}{\det{(A)}} \operatorname{adj}{(A)}\, b$$

and thus

$$A^{-1} = \frac{1}{\det{(A)}} \operatorname{adj}{(A)}.$$

Therefore, we have proved the following result :

8.3.2 PROPOSITION.   (THE ADJOINT FORMULA FOR THE INVERSE MATRIX)
The inverse of the invertible matrix A is given by the formula

$$\boxed{A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)}$$

where $\operatorname{adj}(A)$ *is the adjoint matrix of A.*

8.3.3 EXAMPLE.   Apply the adjoint formula to find the inverse of the matrix

$$A = \begin{bmatrix} 1 & 4 & 5 \\ 4 & 2 & 5 \\ -3 & 3 & -1 \end{bmatrix}.$$

SOLUTION :   First we calculate the cofactors of A :

$$A_{11} = + \begin{vmatrix} 2 & 5 \\ 3 & -1 \end{vmatrix} = -17, \quad A_{12} = - \begin{vmatrix} 4 & 5 \\ -3 & -1 \end{vmatrix} = -11, \quad A_{13} = + \begin{vmatrix} 4 & 2 \\ -3 & 3 \end{vmatrix} = 18,$$

$$A_{21} = - \begin{vmatrix} 4 & 5 \\ 3 & -1 \end{vmatrix} = 19, \quad A_{22} = + \begin{vmatrix} 1 & 5 \\ -3 & -1 \end{vmatrix} = 14, \quad A_{23} = - \begin{vmatrix} 1 & 4 \\ -3 & 3 \end{vmatrix} = -15,$$

$$A_{31} = + \begin{vmatrix} 4 & 5 \\ 2 & 5 \end{vmatrix} = 10, \quad A_{32} = - \begin{vmatrix} 1 & 5 \\ 4 & 5 \end{vmatrix} = 15, \quad A_{33} = + \begin{vmatrix} 1 & 4 \\ 4 & 2 \end{vmatrix} = -14.$$

Thus the cofactor matrix of A is

$$[A_{ij}] = \begin{bmatrix} -17 & -11 & 18 \\ 19 & 14 & -15 \\ 10 & 15 & -14 \end{bmatrix}.$$

We next interchange rows and columns to obtain the adjoint matrix

$$\operatorname{adj}(A) = \begin{bmatrix} -17 & 19 & 10 \\ -11 & 14 & 15 \\ 18 & -15 & -14 \end{bmatrix}.$$

Finally, we divide by $\det(A) = 29$ to get te inverse matrix

$$A^{-1} = \frac{1}{29} \begin{bmatrix} -17 & 19 & 10 \\ -11 & 14 & 15 \\ 18 & -15 & -14 \end{bmatrix}.$$

NOTE : Just like Cramer's rule, *the adjoint formula for the inverse matrix is computationally inefficient* and is therefore of more theoretical than practical importance. The Gaussian elimination should always be used to find inverses of 4×4 and larger matrices.

8.4 Exercises

Exercise 106 Use the determinant to find out which matrices are invertible.

(a) $\begin{bmatrix} 7 & 6 \\ 9 & 8 \end{bmatrix}$.

(b) $\begin{bmatrix} 3 & 2 \\ 6 & 4 \end{bmatrix}$.

(c) $\begin{bmatrix} a & b & c \\ 0 & b & c \\ 0 & 0 & c \end{bmatrix}$.

(d) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$.

(e) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 7 \end{bmatrix}$.

Exercise 107 Find *all* (real) numbers λ such that the matrix $A - \lambda I_n$ is *not* invertible.

(a) $\begin{bmatrix} 1 & 3 \\ 0 & 3 \end{bmatrix}$.

(b) $\begin{bmatrix} 4 & 2 \\ 2 & 7 \end{bmatrix}$.

(c) $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 2 & 3 \end{bmatrix}$.

(d) $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$.

(e) $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 8 & -2 \end{bmatrix}$.

Exercise 108 For which choices of $\alpha \in \mathbb{R}$ is the matrix A invertible ?

(a) $\begin{bmatrix} \cos \alpha & 1 & -\sin \alpha \\ 0 & 2 & 0 \\ \sin \alpha & 3 & \cos \alpha \end{bmatrix}$.

(b) $\begin{bmatrix} 1 & 1 & \alpha \\ 1 & \alpha & \alpha \\ \alpha & \alpha & \alpha \end{bmatrix}$.

Exercise 109 Use (i) Gaussian elimination *and/or* (ii) Laplace expansion to evaluate the following determinants.

(a) $\begin{vmatrix} 4 & 0 & 6 \\ 5 & 0 & 8 \\ 7 & -4 & -9 \end{vmatrix}$.

(b) $\begin{vmatrix} 0 & 0 & 3 \\ 4 & 0 & 0 \\ 0 & 5 & 0 \end{vmatrix}$.

(c) $\begin{vmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{vmatrix}$.

(d) $\begin{vmatrix} 1 & 0 & 0 & 0 \\ 2 & 0 & 5 & 0 \\ 3 & 6 & 9 & 8 \\ 4 & 0 & 10 & 7 \end{vmatrix}$.

(e) $\begin{vmatrix} 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 5 & 0 & 0 & 0 \end{vmatrix}.$

(f) $\begin{vmatrix} 3 & 0 & 11 & -5 & 0 \\ -2 & 4 & 13 & 6 & 5 \\ 0 & 0 & 5 & 0 & 0 \\ 7 & 6 & -9 & 17 & 7 \\ 0 & 0 & 8 & 2 & 0 \end{vmatrix}.$

Exercise 110 Evaluate each given determinant after first simplifying the computation by adding an appropriate multiple of some row or column to another.

(a) $\begin{vmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{vmatrix}.$

(b) $\begin{vmatrix} 2 & 3 & 4 \\ -2 & -3 & 1 \\ 3 & 2 & 7 \end{vmatrix}.$

(c) $\begin{vmatrix} 3 & -2 & 5 \\ 0 & 5 & 17 \\ 6 & -4 & 12 \end{vmatrix}.$

(d) $\begin{vmatrix} 1 & 2 & 3 & 4 \\ 0 & 5 & 6 & 7 \\ 0 & 0 & 8 & 9 \\ 2 & 4 & 6 & 9 \end{vmatrix}.$

(e) $\begin{vmatrix} 2 & 0 & 0 & -3 \\ 0 & 1 & 11 & 12 \\ 0 & 0 & 5 & 13 \\ -4 & 0 & 0 & 7 \end{vmatrix}.$

Exercise 111 Show that $\det(A) = 0$ without direct evaluation of the determinant.

(a) $A = \begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{a} & \frac{1}{b} & \frac{1}{c} \\ bc & ca & ab \end{bmatrix}$.

(b) $A = \begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ b+c & c+a & a+b \end{bmatrix}$.

Exercise 112 Evaluate the determinants :

(a) $\begin{vmatrix} 3 & 4 & 3 \\ 3 & 2 & 1 \\ -3 & 2 & 4 \end{vmatrix}$.

(b) $\begin{vmatrix} 3 & 2 & -3 \\ 0 & 3 & 2 \\ 2 & 3 & -5 \end{vmatrix}$.

(c) $\begin{vmatrix} -2 & 5 & 4 \\ 5 & 3 & 1 \\ 1 & 4 & 5 \end{vmatrix}$.

(d) $\begin{vmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & -2 & 0 \\ -2 & 3 & -2 & 3 \\ 0 & -3 & 3 & 3 \end{vmatrix}$.

(e) $\begin{vmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 3 & 2 \\ 4 & 2 & 1 & 3 \\ 3 & 3 & 1 & 4 \end{vmatrix}$.

(f) $\begin{vmatrix} 3 & 1 & -2 & 1 \\ 1 & 1 & -3 & 2 \\ 2 & 0 & 2 & 3 \\ 3 & 3 & 1 & -3 \end{vmatrix}$.

Exercise 113 Let A be an $n \times n$ matrix.

(a) If $\det(A) = 3$, what is $\det(A^T A)$?

(b) If A is invertible, what can you say about the sign of $\det(A^T A)$?

Exercise 114 If A is a matrix such that $A^2 = A$, show that $\det(A) = 0$ or $\det(A) = 1$.

Exercise 115 Prove or disprove.

  (a) If the matrix A is orthogonal, then $\det(A) = \pm 1$.

  (b) If the 3×3 matrix A is skew symmetric, then $\det(A) = 0$.

  (c) If $A^n = O$ for some positive integer n, then $\det(A) = 0$.

Exercise 116 Use *Cramer's rule* to solve each of the following linear systems.

  (a) $\begin{cases} ax & - & by = 1 \\ bx & + & ay = 0 \end{cases}$;

  (b) $\begin{cases} x_1 & - & 2x_2 & + & 2x_3 = & 3 \\ 3x_1 & & & + & x_3 = -1 \\ x_1 & - & x_2 & + & 2x_3 = & 2 \end{cases}$;

  (c) $\begin{cases} x_1 & + & 4x_2 & + & 2x_3 = & 3 \\ 4x_1 & + & 2x_2 & + & x_3 = & 1 \\ 2x_1 & - & 2x_2 & - & 5x_3 = -3 \end{cases}$;

  (d) $\begin{cases} 2x_1 & + & 3x_2 & - & 5x_3 = & 1 \\ & & 3x_2 & + & 2x_3 = -1 \\ 3x_1 & + & 2x_2 & - & 3x_3 = & 1 \end{cases}$

Exercise 117 Use *Cramer's rule* to solve for x and y in terms of u and v :

  (a) $u = 5x + 8y$ and $v = 3x + 5y$.

  (b) $u = x\cos\theta - y\sin\theta$ and $v = x\sin\theta + y\cos\theta$.

Exercise 118 Consider the 2×2 matrices

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} x \\ y \end{bmatrix}$$

where x and y denote the row vectors of B. Then the product AB can be written in the form

$$AB = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}.$$

Use this expression and the properties of the determinants to show that

$$\det(AB) = (ad - bc) \begin{vmatrix} x \\ y \end{vmatrix} = \det(A) \cdot \det(B).$$

Exercise 119 Use the *adjoint formula* to find the inverse A^{-1} of each matrix A given below.

(a) $\begin{bmatrix} -2 & 2 & -4 \\ 3 & 0 & 1 \\ 1 & -2 & 2 \end{bmatrix}$.

(b) $\begin{bmatrix} 3 & 5 & 2 \\ -2 & 3 & -4 \\ -5 & 0 & -5 \end{bmatrix}$.

(c) $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$.

Exercise 120 TRUE or FALSE ?

(a) If A is an $n \times n$ matrix, then $\det(2A) = 2 \cdot \det(A)$.

(b) Suppose that A and B are $n \times n$ matrices, and A is invertible. Then

$$\det(ABA^{-1}) = \det(B).$$

(c) If A is an $n \times n$ matrix, then

$$\det(AA^T) = \det A^T A.$$

(d) If all entries of a square matrix A are zeros and ones, then $\det(A)$ is 1, 0, or -1.

(e) If A and B are $n \times n$ matrices, then

$$\det(A + B) = \det(A) + \det(B).$$

(f) If all diagonal entries of a square matrix A are odd integers, and all other entries are even, then A is invertible.

Chapter 9

Vectors, Lines, and Planes

Topics :

1. VECTORS IN THE PLANE

2. VECTORS IN SPACE

3. LINES AND PLANES

A *vector* is usually defined as a "quantity having magnitude and direction", such as the *velocity vector* of an object moving through space. It is helpful to represent a vector as an "arrow" attached to a point of space. Vectors can be added to one another and can also be multiplied by real numbers (often called *scalars* in this context). They provide a source of ideas for studying more abstract mathematical subjects, like linear algebra or modern geometry.

9.1   Vectors in the plane

Consider the *plane* Π of "elementary (read : high school) plane geometry". We draw a pair of perpendicular *lines* intersecting at a *point* O, called the **origin**. One of the lines, the x-**axis**, is usually taken in a "horizontal" position. The other line, the y-**axis**, is then taken in a "vertical" position. The x- and y-axes together are called **coordinate axes** and they form a **Cartesian coordinate system** on Π. We now choose a point on the x-axis to the right of O and a point on the y-axis above O to fix the *units of length* and *positive directions* on the coordinate axes. Frequently, these points are chosen so that they are both equidistant from O. With each point P in the plane we associate an ordered pair (x, y) of real numbers, its **coordinates**. Conversely, we can associate a point in the plane with each ordered pair of real numbers. Point P with coordinates (x, y) is denoted by $P(x, y)$ or, simply, by (x, y). Thus, *the plane Π, equipped with a Cartesian coordinate system, may be identified with the set* $\mathbb{R}^2$ *of all pairs of real numbers.*

Throughout, the set $\mathbb{R}^2$ will be referred to as *the* **Euclidean 2-space** or, simply, the **plane**.

NOTE :   A **point** in the Euclidean 2-space is an ordered pair (x, y) of real numbers, and the **distance** between points (x_1, y_1) and (x_2, y_2) is given by

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

We are now going to introduce the concept of *(geometric) vector.*

NOTE :   One can think of a vector as an *instruction to move*; the instruction makes sense wherever you are (in the plane), even if it may be rather difficult to carry out. Not every instruction to move is a vector; for an instruction to be a vector, it must specify movement *through the same distance* and *in the same direction* for every point.

We make the following definition.

9.1.1 DEFINITION.   A **vector** (in the plane) is a 2×1 matrix

$$\vec{v} = \left[\begin{array}{c} x \\ y \end{array} \right]$$

where x and y are real numbers, called the **components** of $\vec{v}$.

With every vector $\vec{v}$ we can associate a *directed line segment*, with the initial point the origin and the terminal point $P(x,y)$. The directed line segment from O to P is denoted by $\overrightarrow{OP}$; O is called the **tail** and P the **head**.
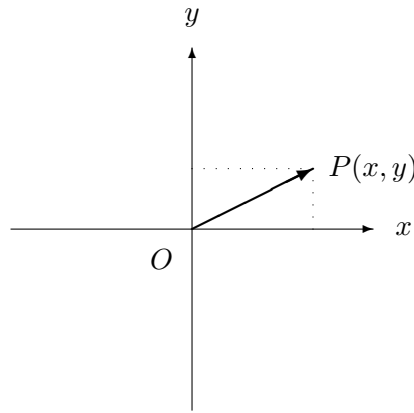
Directed line segment : $\overrightarrow{OP}$.

NOTE :   A directed line segment has a **direction**, indicated by an arrow pointing from O to P. The **magnitude** of a directed line segment is its length. Thus, *a directed line segment can be used to describe force, velocity, and acceleration.*

Conversely, with every directed line segment $\overrightarrow{OP}$, with tail $O(0,0)$ and head $P(x,y)$, we can associate the vector

$$\vec{v} = \left[\begin{array}{c} x \\ y \end{array} \right].$$

9.1.2 DEFINITION.   Two vectors

$$\vec{u} = \left[\begin{array}{c} u_1 \\ u_2 \end{array} \right] \quad \text{and} \quad \vec{v} = \left[\begin{array}{c} v_1 \\ v_2 \end{array} \right]$$

are said to be **equal** if $u_1 = v_1$ and $u_2 = v_2$. That is, two vectors are equal if their respective components are equal.

Frequently, in applications it is necessary to represent a vector $\vec{v}$ by a line segment $\overrightarrow{PQ}$ located at some point $P(x, y)$ (not the origin). In this case, if

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \quad \text{then} \quad Q \quad \text{has coordinates} \quad (x + v_1, y + v_2).$$

9.1.3 EXAMPLE.   Consider the points $P(3, 2)$, $Q(5, 5)$, $R(-3, 1)$ and $S(-1, 4)$. The vectors (represented by) $\overrightarrow{PQ}$ and $\overrightarrow{RS}$ are equal, since they have their respective components equal. We write

$$\overrightarrow{PQ} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \overrightarrow{RS}.$$
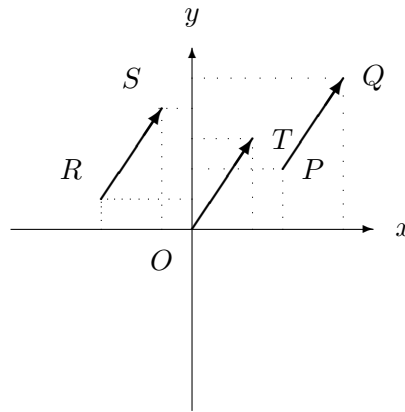
Equal vectors : $\overrightarrow{PQ} = \overrightarrow{RS} \ (= \overrightarrow{OT})$.

With every vector

$$\vec{v} = \begin{bmatrix} x \\ y \end{bmatrix}$$

we can also associate the unique point $P(x, y)$; conversely, with every point $P(x, y)$ we associate the unique vector

$$\vec{v} = \begin{bmatrix} x \\ y \end{bmatrix}.$$

This association is carried out by means of the directed line segment $\overrightarrow{OP}$, located at the origin. The directed line segment $\overrightarrow{OP}$ is one representation of a vector, sometimes denoted by $\vec{r}_P$ and called the **position vector** of the point P.

NOTE : The plane may be viewed both as *the set of all points* or *the set of all vectors* (in the plane).

Vector addition and scalar multiplication

9.1.4 DEFINITION. The **sum** of two vectors

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

is the vector

$$\vec{u} + \vec{v} := \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \end{bmatrix}.$$

We can interpret vector addition geometrically as follows. We take a representative of $\vec{u}$, say $\overrightarrow{PQ}$, and then a representative of $\vec{v}$ starting from the terminal point of $\vec{u}$, say $\overrightarrow{QR}$. The sum $\vec{u} + \vec{v}$ is then the vector (represented by the directed line segment) $\overrightarrow{PR}$. Thus

$$\vec{u} + \vec{v} = \overrightarrow{PQ} + \overrightarrow{QR} = \overrightarrow{PR}.$$
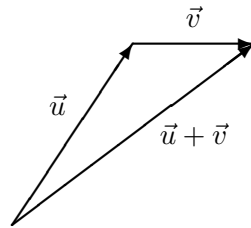
Sum of two vectors : $\vec{u} + \vec{v}$.

We can also describe $\vec{u} + \vec{v}$ as the diagonal of the parallelogram defined by $\vec{u}$ and $\vec{v}$. This description of vector addition is sometimes called the **parallelogram rule**.
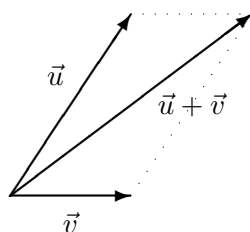
The parallelogram rule of vector addition.

9.1.5 Definition.   If

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$$

is a vector and λ is a real number (scalar), then the **scalar multiple** of $\vec{u}$ by λ is the vector

$$\lambda \vec{u} := \begin{bmatrix} \lambda u_1 \\ \lambda u_2 \end{bmatrix}.$$
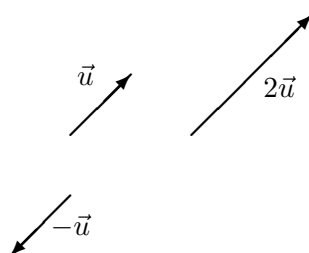
Scalar multiples of a vector : $2\vec{u}$ and $-\vec{u}$.

The vector

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

is called the **zero vector** and is denoted by $\vec{0}$. If $\vec{u}$ is a vector, it follows that

$$\vec{u} + \vec{0} = \vec{u}.$$

We can also show that

$$\vec{u} + (-1)\vec{u} = \vec{0},$$

and we write $(-1)\vec{u}$ as $-\vec{u}$ and call it the **opposite** of $\vec{u}$. Moreover, we write $\vec{u} + (-1)\vec{v}$ as $\vec{u} - \vec{v}$ and call it the **difference** between $\vec{u}$ and $\vec{v}$.

NOTE : While vector addition gives one diagonal of a parallelogram, vector subtraction gives the other diagonal.
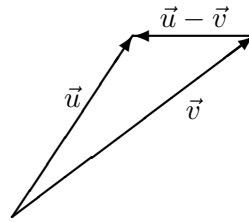
Difference between two vectors.

The following proposition summarizes the algebraic properties of vector addition and scalar multiplication of vectors.

9.1.6 PROPOSITION.   *If $\vec{u}$, $\vec{v}$ and $\vec{w}$ are vectors in $\mathbb{R}^2$ and r and s are scalars, then :*

(1) $\vec{u} + \vec{v} = \vec{v} + \vec{u}$.

(2) $\vec{u} + (\vec{v} + \vec{w}) = (\vec{u} + \vec{v}) + \vec{w}.$

(3) $\vec{u} + \vec{0} = \vec{0} + \vec{u} = \vec{u}.$

(4) $\vec{u} + (-\vec{u}) = (-\vec{u}) + \vec{u} = \vec{0}.$

(5) $r(\vec{u} + \vec{v}) = r\vec{u} + r\vec{v}.$

(6) $(r + s)\vec{u} = r\vec{u} + s\vec{u}.$

(7) $r(s\vec{u}) = (rs)\vec{u}.$

(8) $1\vec{u} = \vec{u}.$

NOTE :   The properties listed above may be summarize by saying that $\mathbb{R}^2$ *is a vector space* (over the field of real numbers).

Magnitude and distance

9.1.7 DEFINITION.   The **length** (or the **magnitude**) of the vector

$$\vec{v} = \begin{bmatrix} a \\ b \end{bmatrix}$$

is defined to be the distance from the point (a, b) to the origin ; that is,

$$\boxed{\|\vec{v}\| := \sqrt{a^2 + b^2}\,.}$$

9.1.8 EXAMPLE.   The length of the vector

$$\vec{v} = \begin{bmatrix} 3 \\ -4 \end{bmatrix}$$

is

$$\|\vec{v}\| = \sqrt{3^2 + (-4)^2} = 5.$$

9.1.9 PROPOSITION.   *If $\vec{u}$ and $\vec{v}$ are vectors, and r is a real number, then :*

(1) $\|\vec{u}\| \geq 0\,;$ $\|\vec{u}\| = 0$ *if and only if* $\vec{u} = 0.$

(2) $\|r\vec{u}\| = |r|\,\|\vec{u}\|$.

(3) $\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$ (*the* **triangle inequality**).

PROOF :   Exercise.

If

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

are vectors in $\mathbb{R}^2$, then the **distance** between $\vec{u}$ and $\vec{v}$ is defined as $\|\vec{u} - \vec{v}\|$. Thus

$$\|\vec{u} - \vec{v}\| = \sqrt{(u_1 - v_1)^2 + (u_2 - v_2)^2}.$$

NOTE :   This equation also gives the distance between the points (u_1, u_2) and (v_1, v_2).

9.1.10 EXAMPLE.   Compute the distance between the vectors

$$\vec{u} = \begin{bmatrix} -1 \\ 5 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}.$$

SOLUTION :   The distance between $\vec{u}$ and $\vec{v}$ is

$$\|\vec{u} - \vec{v}\| = \sqrt{(-1 - 3)^2 + (5 - 2)^2} = \sqrt{4^2 + 3^2} = 5.$$

Dot product and angle

9.1.11 DEFINITION.   Let

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

be vectors in $\mathbb{R}^2$. The **dot product** of $\vec{u}$ and $\vec{v}$ is defined as the *number*

$$\boxed{\vec{u} \bullet \vec{v} := u_1 v_1 + u_2 v_2.}$$

NOTE :   The dot product is also called the **standard inner product** on $\mathbb{R}^2$.

9.1.12 EXAMPLE.   If

$$\vec{u} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 4 \\ -2 \end{bmatrix}$$

then

$$\vec{u} \bullet \vec{v} = (2)(4) + (3)(-2) = 2.$$

NOTE :   (1)   We can write the dot product of $\vec{u}$ and $\vec{v}$ in terms of matrix multiplication as $\vec{u}^T \vec{v}$, where we have ignored the brackets around the 1×1 matrix $\vec{u}^T \vec{v}$.

(2)   If $\vec{v}$ is a vector in $\mathbb{R}^2$, then

$$\|\vec{v}\| = \sqrt{\vec{v} \bullet \vec{v}}.$$

Let us now consider the problem of determining the **angle** θ, $0 \leq \theta \leq \pi$, between two *nonzero* vectors in $\mathbb{R}^2$. Let

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

be two vectors in $\mathbb{R}^2$.
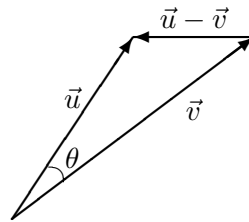
The angle between two vectors.

Using the *law of cosines*, we have

$$\|\vec{v} - \vec{u}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2 - 2\|\vec{u}\|\|\vec{v}\| \cos \theta.$$

Hence

$$\begin{aligned}
\cos\theta &= \frac{\|\vec{u}\|^2 + \|\vec{v}\|^2 - \|\vec{v} - \vec{u}\|^2}{2\|\vec{u}\|\|\vec{v}\|} \\
&= \frac{(u_1^2 + u_2^2) + (v_1^2 + v_2^2) - (v_1 - u_1)^2 - (v_2 - u_2)^2}{2\|\vec{u}\|\|\vec{v}\|} \\
&= \frac{u_1 v_1 + u_2 v_2}{\|\vec{u}\|\|\vec{v}\|} \\
&= \frac{\vec{u} \bullet \vec{v}}{\|\vec{u}\|\|\vec{v}\|} \, .
\end{aligned}$$

That is,

$$\boxed{\cos\theta = \frac{\vec{u} \bullet \vec{v}}{\|\vec{u}\|\|\vec{v}\|} \, .}$$

NOTE :   The zero vector in $\mathbb{R}^2$ has no specific *direction*. The law of cosines expression above is true, for any angle θ, if $\vec{v} \neq \vec{0}$ and $\vec{u} = \vec{0}$. Thus, *the zero vector can be assigned any direction*.

9.1.13 EXAMPLE.   The angle θ between the vectors

$$\vec{u} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} -1 \\ 1 \end{bmatrix}$$

is determined by

$$\cos\theta = \frac{(1)(-1) + (0)(1)}{\sqrt{1^2 + 0^2}\,\sqrt{(-1)^2 + 1^2}} = -\frac{1}{\sqrt{2}} \, .$$

Since $0 \leq \theta \leq \pi$, it follows that $\theta = \frac{3\pi}{4}$.

9.1.14 DEFINITION.   Two (nonzero) vectors $\vec{u}$ and $\vec{v}$ are

- **collinear** (or **parallel**) provided $\theta = 0$ or $\theta = \pi$.

- **orthogonal** (or **perpendicular**) provided $\theta = \frac{\pi}{2}$.
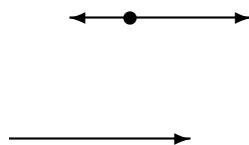
Collinear (or parallel) vectors.
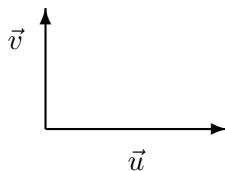
Orthogonal vectors : $\vec{u} \perp \vec{v}$.

NOTE :   (1)   We regard the zero vector as both collinear with and orthogonal to *every* vector.

(2)   If $\vec{v} \neq \vec{0}$, then vectors $\vec{u}$ and $\vec{v}$ are *collinear* $\iff$ $\vec{u} = r\,\vec{v}$ for some $r \in \mathbb{R}$. (See **Exercise 23** (b))

(3)   Vectors $\vec{u}$ and $\vec{v}$ are *orthogonal* $\iff$ $\vec{u} \bullet \vec{v} = 0$.

9.1.15 EXAMPLE.   The vectors

$$\vec{u} = \begin{bmatrix} 2 \\ -4 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$$

are orthogonal, since

$$\vec{u} \bullet \vec{v} = (2)(4) + (-4)(2) = 0.$$

Each of the properties of the dot product listed below is easy to establish.

9.1.16 PROPOSITION.   *If $\vec{u}$, $\vec{v}$, and $\vec{w}$ are vectors in $\mathbb{R}^2$, and r is a real number, then :*

(1) $\vec{u} \bullet \vec{u} \geq 0$; $\vec{u} \bullet \vec{u} = 0$ *if and only if* $\vec{u} = \vec{0}$.

(2) $\vec{v} \bullet \vec{u} = \vec{u} \bullet \vec{v}$.

(3) $(\vec{u} + \vec{v}) \bullet \vec{w} = \vec{u} \bullet \vec{w} + \vec{v} \bullet \vec{w}$.

(4) $(r\vec{u}) \bullet \vec{v} = r(\vec{u} \bullet \vec{v})$.

PROOF :   Exercise.

A **unit vector** in $\mathbb{R}^2$ is a vector whose length is 1. If $\vec{v}$ is a nonzero vector, then the vector

$$\frac{1}{\|\vec{v}\|}\vec{v}$$

is a unit vector (in the direction of $\vec{v}$).

There are two unit vectors in $\mathbb{R}^2$ that are of special importance. These are

$$\vec{i} := \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \vec{j} := \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

the unit vectors along the positive x- and y-axes. Observe that $\vec{i}$ and $\vec{j}$ are orthogonal.
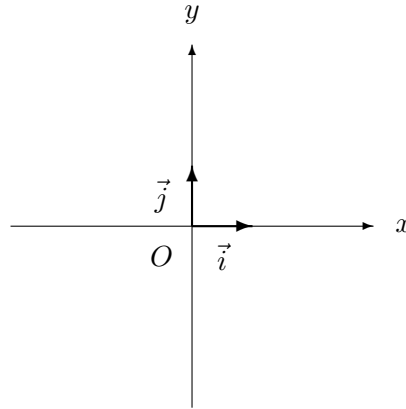
The standard unit vectors : $\vec{i}$ and $\vec{j}$.

NOTE :   Every vector in $\mathbb{R}^2$ can be written (uniquely) as a *linear combination* of the vectors $\vec{i}$ and $\vec{j}$; that is,

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = v_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + v_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = v_1\vec{i} + v_2\vec{j}.$$
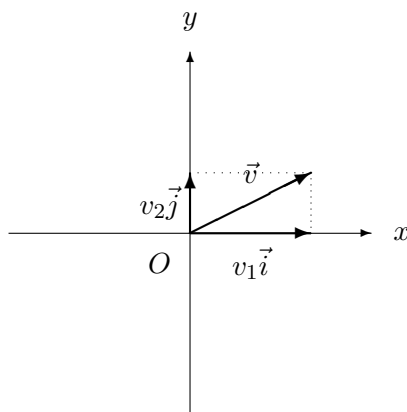
Linear combination of two vectors : $\vec{v} = v_1\vec{i} + v_2\vec{j}$.

9.2   Vectors in space

The foregoing discussion of vectors in the plane can be generalized to vectors in space, as follows.

Consider the (three-dimensional) *space* Σ of "elementary (read : high school) solid geometry". We first fix a **Cartesian coordinate system** by choosing a *point*, called the **origin**, and three *lines*, called the **coordinate axes**, each passing through origin, so that each line is perpendicular to the other two. These lines are individually called the x-, y-, and z-**axes**. On each of these axes we choose a point fixing the *units of length* and *positive directions* on the coordinate axes. Frequently, these points are chosen so that they are both equidistant from the origin O. With each point P in space we associate an ordered triple (x, y, z) of real numbers, its **coordinates**. Conversely, we can associate a point in space with each ordered triple of real

numbers. Point P with coordinates (x, y, z) is denoted by $P(x, y, z)$ or, simply, by (x, y, z). Thus, *the space Σ, equipped with a Cartesian coordinate system, may be identified with the set $\mathbb{R}^3$ of all triples of real numbers.*

Throughout this section, the set $\mathbb{R}^3$ will be referred to as *the* **Euclidean 3-space** or, simply, the **space**.

NOTE : A **point** in the Euclidean 3-space is an ordered triple (x, y, z) of real numbers, and the **distance** between points (x_1, y_1, z_1) and (x_2, y_2, z_2) is given by

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2}.$$

We now introduce the concept of *vector* in space.

9.2.1 DEFINITION. A **vector** (in space) is a 3×1 matrix

$$\vec{v} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

where x, y, and z are real numbers, called the **components** of $\vec{v}$.

With every vector $\vec{v}$ we can associate a *directed line segment*, with the initial point the origin and the terminal point $P(x, y, z)$. The directed line segment from O to P is denoted by $\overrightarrow{OP}$; O is called the **tail** and P the **head**. Conversely, with every directed line segment $\overrightarrow{OP}$, with tail $O(0, 0, 0)$ and head $P(x, y, z)$, we can associate the vector

$$\vec{v} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$
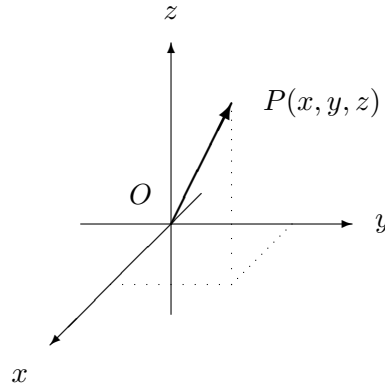
Directed line segment : $\overrightarrow{OP}$.

9.2.2 DEFINITION.   Two vectors

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

are said to be **equal** if $u_1 = v_1$, $u_2 = v_2$, and $u_3 = v_3$. That is, two vectors are equal if their respective components are equal.

Frequently, in applications it is necessary to represent a vector $\vec{v}$ by a line segment $\overrightarrow{PQ}$ located at some point $P(x, y, z)$ (not the origin). In this case, if

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}, \quad \text{then} \quad Q \quad \text{has coordinates} \quad (x + v_1, y + v_2, z + v_3).$$

9.2.3 EXAMPLE.   Consider the points $P(3, 2, 1)$, $Q(5, 5, 0)$, $R(-3, 1, 4)$ and $S(-1, 4, 3)$. The vectors (represented by) $\overrightarrow{PQ}$ and $\overrightarrow{RS}$ are equal, since they have their respective components equal. We write

$$\overrightarrow{PQ} = \begin{bmatrix} 2 \\ 3 \\ -1 \end{bmatrix} = \overrightarrow{RS}.$$

With every vector

$$\vec{v} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

we can also associate the unique point $P(x, y, z)$; conversely, with every point $P(x, y, z)$ we associate the unique vector

$$\vec{v} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

This association is carried out by means of the directed line segment $\overrightarrow{OP}$, located at the origin. The directed line segment $\overrightarrow{OP}$ is one representation of a vector, sometimes denoted by $\vec{r}_P$ and called the **position vector** of the point P.

NOTE : The space may be viewed both as *the set of all points* or *the set of all vectors* (in space).

Vector addition and scalar multiplication

9.2.4 DEFINITION. The **sum** of two vectors

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

is the vector

$$\vec{u} + \vec{v} := \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \\ u_3 + v_3 \end{bmatrix}.$$

The parallelogram rule, as a description (geometric interpretation) of vector addition remains valid.

9.2.5 DEFINITION.   If

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}$$

is a vector and λ is a real number (scalar), then the **scalar multiple** of $\vec{u}$ by λ is the vector

$$\lambda\vec{u} := \begin{bmatrix} \lambda u_1 \\ \lambda u_2 \\ \lambda u_3 \end{bmatrix}.$$

The vector

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

is called the **zero vector** and is denoted by $\vec{0}$. If $\vec{u}$ is a vector, it follows that

$$\vec{u} + \vec{0} = \vec{u}.$$

Again, we can show that

$$\vec{u} + (-1)\vec{u} = \vec{0}$$

and we write $(-1)\vec{u}$ as $-\vec{u}$ and call it the **opposite** of $\vec{u}$. We write $\vec{u}+(-1)\vec{v}$ as $\vec{u} - \vec{v}$ and call it the **difference** between $\vec{u}$ and $\vec{v}$.

NOTE :   While vector addition gives one diagonal of a parallelogram, vector subtraction gives the other diagonal.

The following proposition summarizes the algebraic properties of vector addition and scalar multiplication of vectors.

9.2.6 PROPOSITION.   *If $\vec{u}$, $\vec{v}$ and $\vec{w}$ are vectors in $\mathbb{R}^3$ and r and s are scalars, then :*

(1) $\vec{u} + \vec{v} = \vec{v} + \vec{u}.$

(2) $\vec{u} + (\vec{v} + \vec{w}) = (\vec{u} + \vec{v}) + \vec{w}.$

(3) $\vec{u} + \vec{0} = \vec{0} + \vec{u} = \vec{u}.$

(4) $\vec{u} + (-\vec{u}) = (-\vec{u}) + \vec{u} = \vec{0}.$

(5) $r(\vec{u} + \vec{v}) = r\vec{u} + r\vec{v}.$

(6) $(r + s)\vec{u} = r\vec{u} + s\vec{u}.$

(7) $r(s\vec{u}) = (rs)\vec{u}.$

(8) $1\vec{u} = \vec{u}.$

NOTE :   The properties listed above may be summarize by saying that $\mathbb{R}^3$ *is a vector space* (over the field of real numbers).

Magnitude and distance

9.2.7 DEFINITION.   The **length** (or the **magnitude**) of the vector

$$\vec{v} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

is defined to be the distance from the point (a, b, c) to the origin ; that is,

$$\boxed{\|\vec{v}\| := \sqrt{a^2 + b^2 + c^2}.}$$

9.2.8 EXAMPLE.   The length of the vector

$$\vec{v} = \begin{bmatrix} 3 \\ -4 \\ 0 \end{bmatrix}$$

is

$$\|\vec{v}\| = \sqrt{3^2 + (-4)^2 + 0^2} = 5.$$

9.2.9 PROPOSITION.   *If $\vec{u}$ and $\vec{v}$ are vectors, and r is a real number, then :*

(1) $\|\vec{u}\| \geq 0$; $\|\vec{u}\| = 0$ *if and only if* $\vec{u} = 0.$

(2) $\|r\vec{u}\| = |r| \, \|\vec{u}\|.$

(3) $\|\vec{u} + \vec{v}\| \le \|\vec{u}\| + \|\vec{v}\|$ (*the* **triangle inequality**).

PROOF :   Exercise.

If

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

are vectors in $\mathbb{R}^3$, then the **distance** between $\vec{u}$ and $\vec{v}$ is defined as $\|\vec{u} - \vec{v}\|$.
Thus

$$\|\vec{u} - \vec{v}\| = \sqrt{(u_1 - v_1)^2 + (u_2 - v_2)^2 + (u_3 - v_3)^2}.$$

NOTE :   This equation also gives the distance between the points (u_1, u_2, u_3) and
(v_1, v_2, v_3).

9.2.10 EXAMPLE.   Compute the distance between the vectors

$$\vec{u} = \begin{bmatrix} -1 \\ 5 \\ -4 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 3 \\ 2 \\ -4 \end{bmatrix}.$$

SOLUTION :   The distance between $\vec{u}$ and $\vec{v}$ is

$$\|\vec{u} - \vec{v}\| = \sqrt{(-1 - 3)^2 + (5 - 2)^2 + (-4 + 4)^2} = \sqrt{4^2 + 3^2 + 0^2} = 5.$$

Dot product and angle

9.2.11 DEFINITION.   Let

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

be vectors in $\mathbb{R}^3$. The **dot product** of $\vec{u}$ and $\vec{v}$ is defined as the number

$$\boxed{\vec{u} \bullet \vec{v} := u_1 v_1 + u_2 v_2 + u_3 v_3.}$$

NOTE : The dot product is also called the **standard inner product** on $\mathbb{R}^3$.

9.2.12 EXAMPLE. If

$$\vec{u} = \begin{bmatrix} 2 \\ 3 \\ -1 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 4 \\ -2 \\ 2 \end{bmatrix}$$

then

$$\vec{u} \bullet \vec{v} = (2)(4) + (3)(-2) + (-1)(2) = 0.$$

NOTE : (1) We can write the dot product of $\vec{u}$ and $\vec{v}$ in terms of matrix multiplication as $\vec{u}^T \vec{v}$, where we have ignored the brackets around the 1×1 matrix $\vec{u}^T \vec{v}$.

(2) If $\vec{v}$ is a vector in $\mathbb{R}^3$, then

$$\|\vec{v}\| = \sqrt{\vec{v} \bullet \vec{v}}.$$

Let us now consider the problem of determining the **angle** θ, $0 \le \theta \le \pi$, between two *nonzero* vectors in $\mathbb{R}^3$. Let

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

be two vectors in $\mathbb{R}^3$. Using the *law of cosines*, we have

$$\|\vec{v} - \vec{u}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2 - 2\|\vec{u}\|\|\vec{v}\| \cos \theta .$$

Hence

$$
\begin{aligned}
\cos \theta &= \frac{\|\vec{u}\|^2 + \|\vec{v}\|^2 - \|\vec{v} - \vec{u}\|^2}{2\|\vec{u}\|\|\vec{v}\|} \\
&= \frac{(u_1^2 + u_2^2 + u_3^2) + (v_1^2 + v_2^2 + v_3^2) - (v_1 - u_1)^2 + (v_2 - u_2)^2 + (v_3 - u_3)^2}{2\|\vec{u}\|\|\vec{v}\|} \\
&= \frac{u_1 v_1 + u_2 v_2 + u_3 v_3}{\|\vec{u}\|\|\vec{v}\|} \\
&= \frac{\vec{u} \bullet \vec{v}}{\|\vec{u}\|\|\vec{v}\|} .
\end{aligned}
$$

That is,

$$\cos\theta = \frac{\vec{u} \bullet \vec{v}}{\|\vec{u}\|\,\|\vec{v}\|}\,.$$

NOTE :   The zero vector in $\mathbb{R}^2$ has no specific *direction*. The law of cosines expression above is true, for any angle θ, if $\vec{v} \neq \vec{0}$ and $\vec{u} = \vec{0}$. Thus, *the zero vector can be assigned any direction*.

9.2.13 EXAMPLE.   The angle θ between the vectors

$$\vec{u} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

is determined by

$$\cos\theta = \frac{(1)(0) + (1)(1) + (0)(1)}{\sqrt{1^2 + 1^2 + 0^2}\,\sqrt{0^2 + 1^2 + 1^2}} = \frac{1}{2}\,.$$

Since $0 \leq \theta \leq \pi$, it follows that $\theta = \frac{\pi}{3}$.

9.2.14 DEFINITION.   Two (nonzero) vectors $\vec{u}$ and $\vec{v}$ are

- **collinear** (or **parallel**) provided $\theta = 0$ or $\theta = \pi$.

- **orthogonal** (or **perpendicular**) provided $\theta = \frac{\pi}{2}$.

NOTE :   (1)   We regard the zero vector as both collinear with and orthogonal to *every* vector.

(2)   If $\vec{v} \neq \vec{0}$, then vectors $\vec{u}$ and $\vec{v}$ are *collinear* $\iff \vec{u} = r\,\vec{v}$ for some $r \in \mathbb{R}$. (See **Exercise 23** (b))

(3)   Vectors $\vec{u}$ and $\vec{v}$ are *orthogonal* $\iff \vec{u} \bullet \vec{v} = 0$.

9.2.15 PROPOSITION.   *If $\vec{u}$, $\vec{v}$, and $\vec{w}$ are vectors in $\mathbb{R}^2$, and r is a real number, then :*

     (1) $\vec{u} \bullet \vec{u} \geq 0$; $\vec{u} \bullet \vec{u} = 0$ *if and only if* $\vec{u} = \vec{0}$.

    (2) $\vec{v} \bullet \vec{u} = \vec{u} \bullet \vec{v}.$

    (3) $(\vec{u} + \vec{v}) \bullet \vec{w} = \vec{u} \bullet \vec{w} + \vec{v} \bullet \vec{w}.$

    (4) $(r\vec{u}) \bullet \vec{v}) = r(\vec{u} \bullet \vec{v}).$

PROOF :   Exercise.

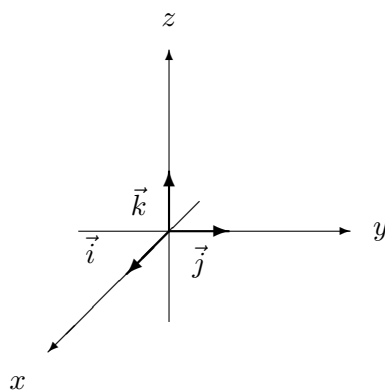A **unit vector** in $\mathbb{R}^3$ is a vector whose length is 1. If $\vec{v}$ is a nonzero vector, then the vector

$$\frac{1}{\|\vec{v}\|} \vec{v}$$

is a unit vector (in the direction of $\vec{v}$).

There are three unit vectors in $\mathbb{R}^3$ that are of special importance. These are

$$\vec{i} := \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \vec{j} := \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad \vec{k} := \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

the unit vectors along the positive x-, y-, and z-axes. Observe that $\vec{i}$, $\vec{j}$, and $\vec{k}$ are mutually orthogonal.

The standard unit vectors : $\vec{i}$, $\vec{j}$, and $\vec{k}$.

NOTE :   Every vector in $\mathbb{R}^3$ can be written (uniquely) as a *linear combination* of the vectors $\vec{i}$, $\vec{j}$, and $\vec{k}$; that is,

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = v_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + v_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + v_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = v_1\vec{i} + v_2\vec{j} + v_3\vec{k}.$$
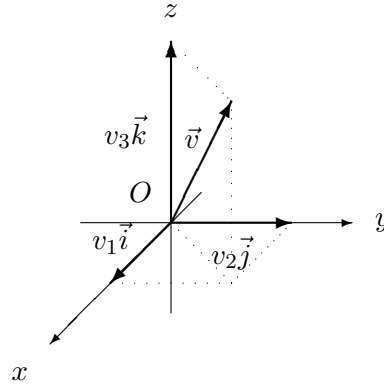
Linear combination of three vectors : $\vec{v} = v_1\vec{i} + v_2\vec{j} + v_3\vec{k}$.

Cross product

9.2.16 DEFINITION.   Let

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

be vectors in $\mathbb{R}^3$. The **cross product** of $\vec{u}$ and $\vec{v}$ is defined to be the vector

$$\vec{u} \times \vec{v} := \begin{bmatrix} u_2v_3 - u_3v_2 \\ u_3v_1 - u_1v_3 \\ u_1v_2 - u_2v_1 \end{bmatrix} = (u_2v_3 - u_3v_2)\vec{i} + (u_3v_1 - u_1v_3)\vec{j} + (u_1v_2 - u_2v_1)\vec{k}.$$

The cross product is also called the **vector product**.

9.2.17 EXAMPLE.   Let $\vec{u} = 2\vec{i} + \vec{j} + 2\vec{k}$ and $\vec{v} = 3\vec{i} - \vec{j} - 3\vec{k}$. Then

$$\vec{u} \times \vec{v} = -\vec{i} + 12\vec{j} - 5\vec{k}.$$

NOTE :   (1)   The cross product $\vec{u} \times \vec{v}$ is orthogonal to both $\vec{u}$ and $\vec{v}$.

(2)   A common way of remembering the definition of the cross product $\vec{u} \times \vec{v}$ is to observe that it results from a *formal* expansion along the first row in the determinant

$$\vec{u} \times \vec{v} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix}.$$
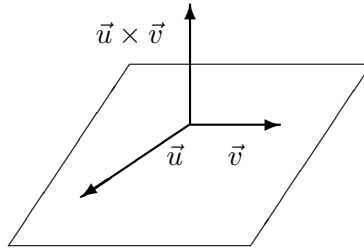
The cross product of two vectors : $\vec{u} \times \vec{v}$.

9.2.18 PROPOSITION.   *If $\vec{u}$, $\vec{v}$, and $\vec{w}$ are vectors in $\mathbb{R}^3$, and r is a real number, then :*

(1) $\vec{u} \times \vec{v} = -\vec{v} \times \vec{u}$.

(2) $\vec{u} \times (\vec{v} + \vec{w}) = \vec{u} \times \vec{v} + \vec{u} \times \vec{w}$.

(3) $(\vec{u} + \vec{v}) \times \vec{w} = \vec{u} \times \vec{w} + \vec{v} \times \vec{w}$.

(4) $r(\vec{u} \times \vec{v}) = (r\vec{u}) \times \vec{v} = \vec{u} \times (r\vec{v})$.

PROOF :   Exercise.

One can show that (tedious computation)

$$\|\vec{u} \times \vec{v}\|^2 = \|\vec{u}\|^2 \|\vec{v}\|^2 - (\vec{u} \bullet \vec{v})^2.$$

Recall that

$$\vec{u} \bullet \vec{v} = \|\vec{u}\| \, \|\vec{v}\| \cos\theta$$

where θ is the angle between $\vec{u}$ and $\vec{v}$. Hence,

$$\|\vec{u} \times \vec{v}\|^2 = \|\vec{u}\|^2 \, \|\vec{v}\|^2 - \|\vec{u}\|^2 \, \|\vec{v}\|^2 \cos^2\theta = \|\vec{u}\|^2 \|\vec{v}\|^2 (1 - \cos^2\theta) = \|\vec{u}\|^2 \, \|\vec{v}\|^2 \sin^2\theta.$$

Taking square roots, we obtain

$$\boxed{\|\vec{u} \times \vec{v}\| = \|\vec{u}\| \, \|\vec{v}\| \sin\theta.}$$

Observe that we do not have to write $|\sin\theta|$, since $\sin\theta$ is nonnegative for $0 \le \theta \le \pi$.

NOTE :   Vectors $\vec{u}$ and $\vec{v}$ (in $\mathbb{R}^3$) are *collinear* $\iff$ $\vec{u} \times \vec{v} = \vec{0}$.

Applications : area and volume

We now consider several applications of cross product.

$\boxed{A}$ (Area of a Triangle)   Consider a triangle with vertices P_1, P_2 and P_3. The *area* of this triangle is $\frac{1}{2}bh$, where b is the *base* and h is the *height*. If we take the segment between P_1 and P_2 to be the base and denote $\overrightarrow{P_1 P_2}$ by the vector $\vec{u}$, then

$$b = \|\vec{u}\|.$$

Letting $\overrightarrow{P_1 P_3} = \vec{v}$, we find that the height h is given by

$$h = \|\vec{v}\| \sin\theta$$

θ being the angle betweeen $\vec{u}$ and $\vec{v}$.
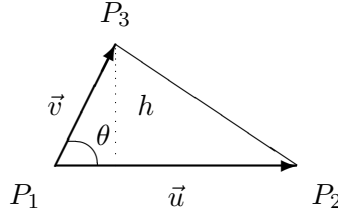
Area of a triangle : $\frac{1}{2}\|\vec{u} \times \vec{v}\|$.

Hence, *the area* A_t *of the triangle is*

$$\boxed{A_t = \tfrac{1}{2}\|\vec{u}\|\,\|\vec{v}\|\sin\theta = \tfrac{1}{2}\|\vec{u} \times \vec{v}\|.}$$

9.2.19 EXAMPLE.   Find the area of the triangle with vertices

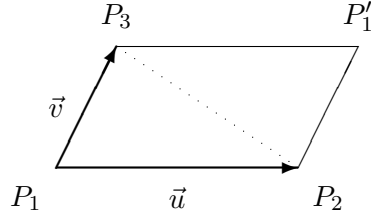$$P_1(2,2,4), \quad P_2(-1,0,5), \quad \text{and} \quad P_3(3,4,3)\,.$$

SOLUTION :   We have

$$\vec{u} = \overrightarrow{P_1 P_2} = -3\vec{i} - 2\vec{j} + \vec{k} \quad \text{and} \quad \vec{v} = \overrightarrow{P_1 P_3} = \vec{i} + 2\vec{j} - \vec{k}.$$

Then

$$A_t = \frac{1}{2}\|(-3\vec{i} - 2\vec{j} + \vec{k}) \times (\vec{i} + 2\vec{j} - \vec{k})\| = \frac{1}{2}\| - 2\vec{j} - 4\vec{k}\| = \sqrt{5}.$$

$\boxed{\text{B}}$ (Area of a Parallelogram)   The area A_p of the parallelogram with adjacent sides $\vec{u}$ and $\vec{v}$ is $2A_t$, so

$$\boxed{A_p = \|\vec{u} \times \vec{v}\|.}$$

Area of a parallelogram : $\|\vec{u} \times \vec{v}\|$.

$\boxed{\text{C}}$ (**Volume of a Parallelepiped**)   Consider the parallelepiped with a vertex at the origin and edges $\vec{u}$, $\vec{v}$, and $\vec{w}$. Then the volume V of the parallelepiped is the product of the area of the face containing $\vec{v}$ and $\vec{w}$ and the distance h from this face to the face parallel to it.
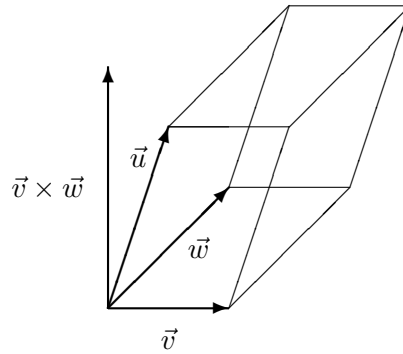
Volume of a parallelepiped : $|\vec{u} \bullet (\vec{v} \times \vec{w})|$.

Now

$$h = \|\vec{u}\| \cos \theta$$

where θ is the angle between $\vec{u}$ and $\vec{v} \times \vec{w}$, and the area of the face determined by $\vec{v}$ and $\vec{w}$ is $\|\vec{v} \times \vec{w}\|$. Hence,

$$\boxed{V = \|\vec{v} \times \vec{w}\|\, \|\vec{u}\|\, |\cos \theta| = |\vec{u} \bullet (\vec{v} \times \vec{w})|.}$$

NOTE :   The volume of the parallelepiped determined by the vectors $\vec{u}$, $\vec{v}$, and $\vec{w}$, can be expressed as follows

$$\text{volume} = \pm \begin{vmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{vmatrix}.$$

9.2.20 EXAMPLE.   Find the volume of the parallelepiped with a vertex at the origin and edges

$$\vec{u} = \vec{i} - 2\vec{j} + 3\vec{k}, \quad \vec{v} = \vec{i} + 3\vec{j} + \vec{k}, \quad \text{and} \quad \vec{w} = 2\vec{i} + \vec{j} + 2\vec{k}.$$

SOLUTION :   We have

$$\vec{v} \times \vec{w} = 5\vec{i} - 5\vec{k}.$$

Hence, $\vec{u} \bullet (\vec{v} \times \vec{w}) = -10$, and thus the volume V is given by

$$V = |\vec{u} \bullet (\vec{v} \times \vec{w})| = |-10| = 10.$$

Alternatively, we have

$$\text{volume} = \pm \begin{vmatrix} 1 & -2 & 3 \\ 1 & 3 & 1 \\ 2 & 1 & 2 \end{vmatrix} = \pm(-10) = 10.$$

9.3   Lines and planes

Lines

In elementary geometry a *straight line* in space is determined by any two points that lie on it. Here, we take the alternative approach that a *straight line in space is determined by a single point P_0 on it and a vector $\vec{v}$ that determines the direction of the line.*

9.3.1 DEFINITION.   By the **straight line** $\mathcal{L}$ that passes through the point $P_0(x_0, y_0, z_0)$ and is parallel to the (nonzero) vector $\vec{v} = a\vec{i} + b\vec{j} + c\vec{k}$ is meant

the set of all points $P(x, y, z)$ in $\mathbb{R}^3$ such that the vector $\overrightarrow{P_0 P} = \vec{r} - \vec{r}_0$ is collinear to $\vec{v}$. (Here, $\vec{r}$ and $\vec{r}_0$ stand for the position vectors of the points P and P_0, respectively.)
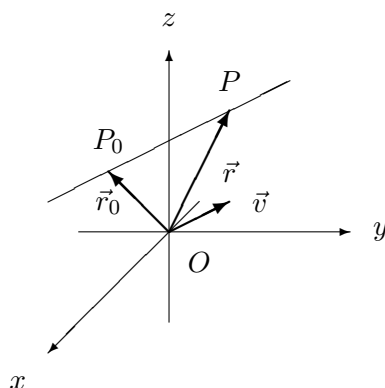
Vector equation of a line : $\vec{r} = \vec{r}_0 + t\vec{v}$.

Thus, the point P lies on $\mathcal{L}$ if and only if

$$\vec{r} - \vec{r}_0 = t\vec{v}, \quad \text{for some scalar } t\,;$$

that is, if and only if

$$\vec{r} = \vec{r}_0 + t\vec{v}, \quad t \in \mathbb{R}.$$

NOTE : We can visualize the point P as moving along the straight line $\mathcal{L}$, with $\vec{r}_0 + t\vec{v}$ being its location at "time" t.

The equation

$$\boxed{\vec{r} = \vec{r}_0 + t\vec{v}, \quad t \in \mathbb{R}}$$

is a **vector equation** of the line $\mathcal{L}$.

By equating components of the vectors in this equation, we get the scalar equations

$$\begin{cases} x = x_0 + at \\ y = y_0 + bt \\ z = z_0 + ct. \end{cases}$$

These are **parametric equations** (with **parameter** t) of the line $\mathcal{L}$.

Alternatively, one can write the equations

$$\boxed{\frac{x - x_0}{a} = \frac{y - y_0}{b} = \frac{z - z_0}{c} \,.}$$

These are called **symmetric equations** of the line $\mathcal{L}$.

9.3.2 EXAMPLE. Write parametric equations of the line $\mathcal{L}$ that passes through the points $P_1(1, 2, 2)$ and $P_2(3, -1, 3)$.

SOLUTION : The *direction* of the line $\mathcal{L}$ is given by the vector $\vec{v} = \overrightarrow{P_1 P_2} = 2\vec{i} - 3\vec{j} + \vec{k}$. With P_1 as the fixed point, we get the following parametric equations

$$x = 1 + 2t\,, \quad y = 2 - 3t\,, \quad z = 2 + t.$$

NOTE : If we take P_2 as the fixed point and $-2\vec{v} = -4\vec{i} + 6\vec{j} - 2\vec{k}$ as the direction vector, then we get different parametric equations

$$x = 3 - 4t\,, \quad y = -1 + 6t\,, \quad z = 3 - 2t.$$

Thus, the parametric equations of a line are *not* unique.

9.3.3 EXAMPLE. Determine whether the lines

$$\vec{r} = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} + t \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} \quad \text{and} \quad \frac{x - 1}{2} = \frac{y - 2}{3} = \frac{z - 3}{4}$$

intersect.

SOLUTION : We write parametric equations for the first line; that is,

$$x = 1 + 3t\,, \quad y = 1 + 2t\,, \quad z = 2 + t.$$

Now we determine whether there exists $t \in \mathbb{R}$ such that

$$\frac{1 + 3t - 1}{2} = \frac{1 + 1t - 2}{3} = \frac{2 + t - 3}{4}\,.$$

The linear system

$$\begin{cases} 6t = 4t - 2 \\ 12t = 2t - 2 \end{cases}$$

is clearly inconsistent (Why ?), and thus the given lines do not intersect.

9.3.4 EXAMPLE.   Find the *shortest* distance between the point $P(3, -1, 4)$ and the line given by

$$x = -2 + 3t\,, \quad y = -2t\,, \quad z = 1 + 4t.$$

SOLUTION :   First, we shall find a formula for the distance from a point P to a line $\mathcal{L}$.

Let $\vec{u}$ be the *direction vector* for $\mathcal{L}$ and A a point on the line. Let δ be the distance from P to the given line $\mathcal{L}$.
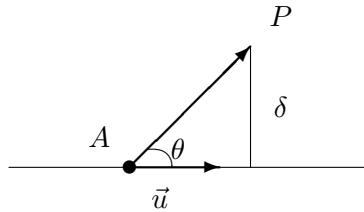
The shortest distance between a point and a line : $\dfrac{\|\overrightarrow{AP} \times \vec{u}\|}{\|\vec{u}\|}$.

Then

$$\delta = \|\ \overrightarrow{AP}\ \|\ \sin\theta\,,$$

where θ is the angle between $\vec{u}$ and $\overrightarrow{AP}$. We have

$$\|\vec{u}\|\ \|\ \overrightarrow{AP}\ \|\sin\theta = \|\vec{u} \times \overrightarrow{AP}\ \| = \|\ \overrightarrow{AP}\ \times \vec{u}\|.$$

Consequently,

$$\delta = \| \overrightarrow{AP} \| \sin\theta = \frac{\| \overrightarrow{AP} \times \vec{u} \|}{\|\vec{u}\|} \,.$$

In our case, we have $\vec{u} = \begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix}$ and to find a point on $\mathcal{L}$, let $t = 0$ and

obtain $A(-2, 0, 1)$. Thus

$$\overrightarrow{AP} = \begin{bmatrix} 5 \\ -1 \\ 3 \end{bmatrix} \quad \text{and} \quad \overrightarrow{AP} \times \vec{u} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ 5 & -1 & 3 \\ 3 & -2 & 4 \end{vmatrix} = 2\vec{i} - 11\vec{j} - 7\vec{k} = \begin{bmatrix} 2 \\ -11 \\ -7 \end{bmatrix}.$$

Finally, we can find the distance to be

$$\delta = \frac{\| \overrightarrow{AP} \times \vec{u} \|}{\|\vec{u}\|} = \frac{\sqrt{174}}{\sqrt{29}} = \sqrt{6} \,.$$

NOTE :   In the xy-plane, parametric equations of a line $\mathcal{L}$ take the form

$$\begin{cases} x = x_0 + at \\ y = y_0 + bt. \end{cases}$$

Alternatively, one can write

$$\frac{x - x_0}{a} = \frac{y - y_0}{b}$$

or

$$y = y_0 + \frac{b}{a}(x - x_0)$$

or even

$$y = mx + n$$

where m is the *slope* of the line and n is the y-intercept. Furthermore, we observe that this "familiar" equation can be rewritten as

$$Ax + By + C = 0.$$

It is not difficult to show that the graph of such an equation, where $A, B, C \in \mathbb{R}$ (with A and B not all zero) is a straight line (in the plane) with slope $m = -\frac{A}{B} \cdot$

9.3.5 EXAMPLE.   Show that the lines

$$(\mathcal{L}) \quad ax + by + c = 0 \quad \text{and} \quad (\mathcal{M}) \quad dx + ey + f = 0$$

are parallel if and only if $ae = bd$ and are perpendicular if and only if $ad + be = 0$.

SOLUTION :   The direction vectors of $\mathcal{L}$ and $\mathcal{M}$ are

$$\vec{u} = \begin{bmatrix} -b \\ a \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} -e \\ d \end{bmatrix},$$

respectively. Then

$$\mathcal{L} \parallel \mathcal{M} \iff \vec{u}_1 = \lambda \vec{u}_2 \iff \vec{u}_1 \times \vec{u}_2 = \vec{0} \iff (ae - bd)\vec{k} = \vec{0} \iff ae = bd\,;$$

$$\mathcal{L} \perp \mathcal{M} \iff \vec{u}_1 \bullet \vec{u}_2 = 0 \iff ad + be = 0.$$

In particular, the lines

$$y = m_1 x + n_1 \quad \text{and} \quad y = m_2 x + n_2$$

are *parallel* if and only if $m_1 = m_2$ and are *perpendicular* if and only if $m_1 m_2 + 1 = 0$.

Planes

A *plane* in space is determined by any point that lies on it and any line through that point orthogonal to the plane. Alternatively, *a plane in space is determined by a single point P_0 on it and a vector $\vec{n}$ that is orthogonal to the plane.*

9.3.6 DEFINITION.   By the **plane** α through the point $P_0(x_0, y_0, z_0)$ with **normal vector** $\vec{n} = a\vec{i} + b\vec{j} + c\vec{k}$ is meant the set of all points $P(x, y, z)$ in $\mathbb{R}^3$ such that the vectors $\overrightarrow{P_0P} = \vec{r} - \vec{r}_0$ and $\vec{n}$ are orthogonal. (Again, $\vec{r}$ and $\vec{r}_0$ stand for the position vectors of the points P and P_0, respectively.)
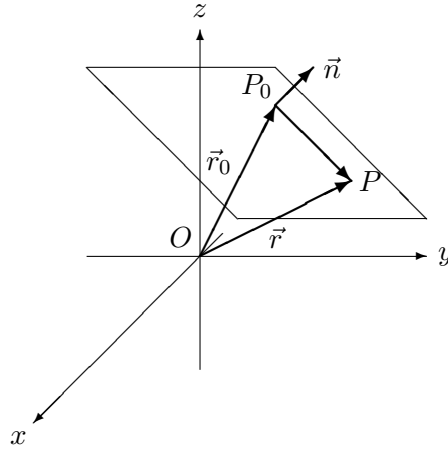
Vector equation of a plan : $\vec{n} \bullet (\vec{r} - \vec{r}_0) = 0$.

Thus, the point P lies on α if and only if

$$\vec{n} \bullet (\vec{r} - \vec{r}_0) = 0 \,.$$

This is a **vector equation** of the plane α.

By substituting the components of the vectors involved in this equation, we get the scalar equation

$$a(x - x_0) + b(y - y_0) + c(z - z_0) = 0.$$

This is a **point-normal equation** (or **standard equation**) of the plane α.

NOTE : The equation above can be rewritten as

$$ax + by + cz + d = 0.$$

It is not difficult to show that the graph of such an equation, where $a, b, c, d \in \mathbb{R}$ (with a, b, and c not all zero) is a plane with normal $\vec{n} = a\vec{i} + b\vec{j} + c\vec{k}$.

9.3.7 EXAMPLE. Find an equation of the plane passing through the point $(3, 4, -3)$ and perpendicular to the vector $\vec{v} = 5\vec{i} - 2\vec{j} + 4\vec{k}$.

SOLUTION : We obtain an equation of the plane as

$$5(x - 3) - 2(y - 4) + 4(z + 3) = 0.$$

9.3.8 EXAMPLE.   Find an equation of the plane passing through points $P_1(2, -2, 1)$, $P_2(-1, 0, 3)$, and $P_3(5, -3, 4)$.

SOLUTION :   The (noncollinear) vectors $\overrightarrow{P_1 P_2} = -3\vec{i} + 2\vec{j} + 3\vec{k}$ and $\overrightarrow{P_1 P_3} = 3\vec{i} - \vec{j} + 3\vec{k}$ lie in the plane, since the points P_1, P_2, and P_3 lie in the plane. The vector

$$\vec{v} = \overrightarrow{P_1 P_2} \times \overrightarrow{P_1 P_3} = 8\vec{i} + 15\vec{j} - 3\vec{k}$$

is then perpendicular to both $\overrightarrow{P_1 P_2}$ and $\overrightarrow{P_1 P_3}$, and is thus a normal to the plane. Using the vector $\vec{v}$ and the point $P_1(2, -2, 1)$, we obtain

$$8(x - 2) + 15(y + 2) - 3(z - 1) = 0$$

as an equation of the plane.

NOTE :   The general equation for a plane passing through three noncollinear points $P_i(x_i, y_i, z_i)$,
$i = 1, 2, 3$ may be written in the form :

$$\begin{vmatrix} x & y & z & 1 \\ x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \end{vmatrix} = 0$$

or, equivalently,

$$\begin{vmatrix} x - x_1 & y - y_1 & z - z_1 \\ x_2 - x_1 & y_2 - y_1 & z_2 - z_1 \\ x_3 - x_1 & y_3 - y_1 & z_3 - z_1 \end{vmatrix} = 0.$$
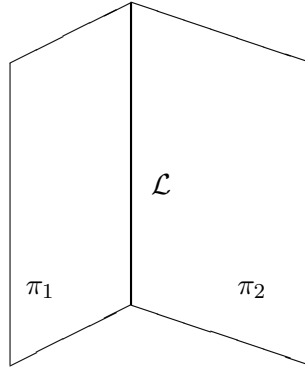
9.3.9 EXAMPLE.   Find parametric equations of the line of intersection of the planes

$$(\pi_1) \quad 2x + 3y - 2z + 4 = 0 \quad \text{and} \quad (\pi_2) \quad x - y + 2z + 3 = 0 \,.$$

SOLUTION :   Solving the linear system consisting of the equations of π_1 and π_2, we obtain (verify !)

$$x = -\frac{13}{5} - \frac{4}{5}t \,, \quad y = \frac{2}{5} + \frac{6}{5}t \,, \quad z = t$$

as parametric equations of the line $\mathcal{L}$ of intersection of the planes.

The line of intersection of two plans : $\mathcal{L} = \pi_1 \cap \pi_2$.

NOTE : (1) The line in the xy-plane, described by the (general) equation

$$ax + by + d = 0$$

may be viewed as the intersection of the planes

$$ax + by + cz + d = 0 \quad \text{and} \quad z = 0.$$

(2) The equations

$$x = y = 0$$

define a line (the z-axis). Alternative ways of describing the same line are, for instance :

(1) $\vec{r} = t\vec{k},\ t \in \mathbb{R}$; (2) $x = 0,\ y = 0,\ z = t$; $t \in \mathbb{R}$; (3) $\dfrac{x}{0} = \dfrac{y}{0} = \dfrac{z}{1}$.

9.3.10 EXAMPLE. Find a formula for the *shortest* distance d between two skew lines $\mathcal{L}_1$ and $\mathcal{L}_2$.

SOLUTION : The lines are *skew* if they are not parallel and do not intersect. Choose points P_1, Q_1 on $\mathcal{L}_1$ and P_2, Q_2 on $\mathcal{L}_2$; so, the direction vectors for the lines $\mathcal{L}_1$ and $\mathcal{L}_2$ are

$$\vec{v}_1 = \overrightarrow{P_1 Q_1} \quad \text{and} \quad \vec{v}_2 = \overrightarrow{P_2 Q_2}\,,$$

respectively.
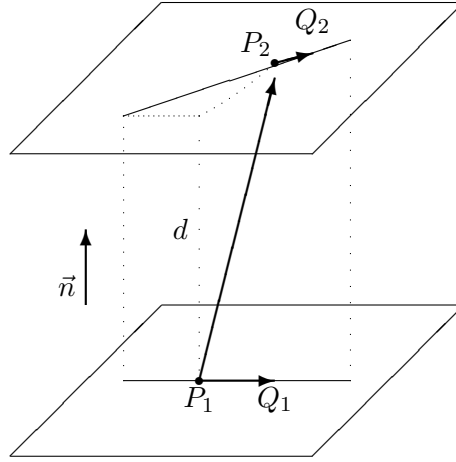
The shortest distance between two skew lines : $\frac{|(\vec{v}_1 \times \vec{v}_2) \bullet \overrightarrow{P_1 P_2}|}{\|\vec{v}_1 \times \vec{v}_2\|}$.

Then $\vec{v}_1 \times \vec{v}_2$ is orthogonal to both $\vec{v}_1$ and $\vec{v}_2$ and hence a *unit vector* $\vec{n}$ orthogonal to both $\vec{v}_1$ and $\vec{v}_2$ is

$$\vec{n} = \frac{1}{\|\vec{v}_1 \times \vec{v}_2\|} (\vec{v}_1 \times \vec{v}_2) .$$

Let us consider planes through P_1 and P_2, respectively, each having normal vector $\vec{n}$. These planes are parallel and contain $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively. The distance d between the planes is measured along a line parallel to the common normal $\vec{n}$. It follows that d is the shortest distance between $\mathcal{L}_1$ and $\mathcal{L}_2$. So

$$\boxed{d = |\vec{n} \bullet \overrightarrow{P_1 P_2}| = \frac{|(\vec{v}_1 \times \vec{v}_2) \bullet \overrightarrow{P_1 P_2}|}{\|\vec{v}_1 \times \vec{v}_2\|}}$$

where $\vec{v}_1 = \overrightarrow{P_1 Q_1}$ and $\vec{v}_2 = \overrightarrow{P_2 Q_2}$ are the direction vectors for the lines $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively.

9.4   Exercises

Exercise 121

(a) Sketch a directed line segment representing each of the following vectors :

$$(1) \quad \vec{u} = \begin{bmatrix} -2 \\ 3 \end{bmatrix} ; \quad (2) \quad \vec{v} = \begin{bmatrix} -2 \\ -2 \end{bmatrix} ; \quad (3) \quad \vec{w} = \begin{bmatrix} 0 \\ -3 \end{bmatrix} .$$

(b) Determine the head of the vector

$$\vec{u} = \begin{bmatrix} -2 \\ 5 \end{bmatrix}$$

whose tail is $(-3, 2)$. Make a sketch.

(c) Determine the tail of the vector

$$\vec{v} = \begin{bmatrix} 2 \\ 6 \end{bmatrix}$$

whose head is $(1, 2)$. Make a sketch.

Exercise 122 For what values of a and b are the vectors

$$\begin{bmatrix} a - b \\ 2 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 4 \\ a + b \end{bmatrix} \quad \text{equal ?}$$

Exercise 123 Compute $\vec{u} + \vec{v}$, $\vec{u} - \vec{v}$, $3\vec{u} - 2\vec{v}$, $\| -2\vec{u}\|$, $\|\vec{u} + \vec{v}\|$ for

$$\vec{u} = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 0 \\ 2 \end{bmatrix}.$$

Exercise 124 Prove that the vectors

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

are collinear if and only if

$$\begin{vmatrix} u_1 & v_1 \\ u_2 & v_2 \end{vmatrix} = 0.$$

Exercise 125 Use the dot product to find the angle between the vectors $\vec{u}$ and $\vec{v}$.

(a) $\vec{u} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $\vec{v} = \begin{bmatrix} 0 \\ -2 \end{bmatrix}$;

(b) $\vec{u} = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$, $\vec{v} = \begin{bmatrix} -3 \\ -3 \end{bmatrix}$.

Exercise 126

(a) Find r so that the vector $\vec{v} = \vec{i} + r\vec{j}$ is orthogonal to $\vec{w} = 2\vec{i} - \vec{j}$.

(b) Find k so that the vectors $k\vec{i} + 4\vec{j}$ and $2\vec{i} + 5\vec{j}$ are collinear.

Exercise 127 Use the fact that $|\cos\theta| \leq 1$ for all θ to show that the **Cauchy-Schwarz inequality**

$$|\vec{u} \bullet \vec{v}| \leq \|\vec{u}\| \, \|\vec{v}\|$$

holds for all vectors $\vec{u}$ and $\vec{v}$ in $\mathbb{R}^2$ (or $\mathbb{R}^3$).

Exercise 128 Use the dot product to find the angle between $\vec{u}$ and $\vec{v}$.

(a) $\vec{u} = \begin{bmatrix} -1 \\ 0 \\ 2 \end{bmatrix}$ and $\vec{v} = \begin{bmatrix} 3 \\ 4 \\ -5 \end{bmatrix}$;

(b) $\vec{u} = 2\vec{i} + \vec{j} + 2\vec{k}$ and $\vec{v} = 3\vec{i} - \vec{j} - 3\vec{k}$.

Exercise 129 Compute

$$\vec{v} \times \vec{w}, \quad \vec{u} \times (\vec{v} \times \vec{w}), \quad (\vec{u} \bullet \vec{w})\vec{v} - (\vec{u} \bullet \vec{v})\vec{w}, \quad (\vec{u} \times \vec{v}) \bullet \vec{w}, \quad \vec{u} \bullet (\vec{v} \times \vec{w})$$

for

$$\vec{u} = \vec{i} + \vec{j} + \vec{k}, \quad \vec{v} = \vec{j} - \vec{k}, \quad \text{and} \quad \vec{w} = w_1\vec{i} + w_2\vec{j} + w_3\vec{k}.$$

Exercise 130 Use the cross product to find a nonzero vector $\vec{c}$ orthogonal to both of $\vec{a}$ and $\vec{b}$.

(a) $\vec{a} = \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$, $\vec{b} = \begin{bmatrix} 4 \\ 1 \\ 3 \end{bmatrix}$; (b) $\vec{a} = \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix}$, $\vec{b} = \begin{bmatrix} 5 \\ 1 \\ -1 \end{bmatrix}$.

Exercise 131 Find :

(a) the angles of the triangle with vertices

$$A(1,1,1), \quad B(3,-2,3), \quad \text{and} \quad C(3,4,6).$$

(b) the area of the triangle with vertices

$$P_1(1,-2,3), \ P_2(-3,1,4), \quad \text{and} \quad P_3(0,4,3).$$

(c) the area of the triangle with vertices P_1, P_2, and P_3, where

$$\overrightarrow{P_1P_2} = 2\vec{i} + 3\vec{j} - \vec{k} \quad \text{and} \quad \overrightarrow{P_1P_3} = \vec{i} + 2\vec{j} + 2\vec{k}.$$

(d) the area of the parallelogram with adjacent sides

$$\vec{u} = \vec{i} + 3\vec{j} - 2\vec{k} \quad \text{and} \quad \vec{v} = 3\vec{i} - \vec{j} - \vec{k}.$$

(e) the volume of the parallelepiped with the vertex at the origin and edges

$$\vec{u} = 2\vec{i} - \vec{j}, \quad \vec{v} = \vec{i} - 2\vec{j} - 2\vec{k} \quad \text{and} \quad \vec{w} = 3\vec{i} - \vec{j} + \vec{k}.$$

Exercise 132 Establish the **triangle inequality**

$$\|\vec{u} + \vec{v}\| \le \|\vec{u}\| + \|\vec{v}\|$$

(for all $\vec{u}$ and $\vec{v}$ in $\mathbb{R}^3$) by first squaring both sides and then using the Cauchy-Schwarz inequality (see **Exercise 137**).

Exercise 133 Find the vector equation and parametric equations for the line passing through the points $(2, 1, 8)$ and $(4, 4, 12)$.

Exercise 134 Show that the line through the points $(2, -1, -5)$ and $(8, 8, 7)$ is parallel to the line through the points $(4, 2, -6)$ and $(8, 8, 2)$.

Exercise 135 Find the equation of the line through the point $(0, 2, -1)$ which is parallel to the line

$$x = 1 + 2t, \quad y = 3t, \quad z = 5 - 7t.$$

Exercise 136 Find the equation of the plane through the points

$$A(1, 0, -3), \quad B(0, -2, -4), \quad \text{and} \quad C(4, 1, 6).$$

Exercise 137 Find the equation of the plane which passes through the point $(6, 5, -2)$ and is parallel to the plane $x + y - z = 5$.

Exercise 138 Find the equation of the plane which is perpendicular to the line segment joining the points $(-3, 2, 1)$ and $(9, 4, 3)$, and which passes through the midpoint of the line segment.

Exercise 139 Find the point of intersection of the planes

$$(\pi_1) \quad x + 2y - z = 6, \quad (\pi_2) \quad 2x - y + 3z + 13 = 0, \quad (\pi_3) \quad 3x - 2y + 3z = -16.$$

Exercise 140 Find the equation of the plane passing through the point $(-3, 2, -4)$ and the line of intersection of the planes

$$(\alpha) \quad 3x + y - 5z + 7 = 0 \quad \text{and} \quad (\beta) \quad x - 2y + 4z = 3.$$

Exercise 141 Find the shortest distance between the lines

$$(\mathcal{L}_1) \quad \vec{r} = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} 2 \\ 0 \\ -1 \end{bmatrix} \quad \text{and} \quad (\mathcal{L}_2) \quad \vec{r} = \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} + s \begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}.$$

Exercise 142 Find the point of intersection of the lines

$$(\mathcal{L}_1) \quad \vec{r} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + t \begin{bmatrix} 0 \\ -2 \\ 0 \end{bmatrix} \quad \text{and} \quad (\mathcal{L}_2) \quad \vec{r} = \begin{bmatrix} -1 \\ 1 \\ 2 \end{bmatrix} + s \begin{bmatrix} 2 \\ 0 \\ -1 \end{bmatrix}.$$

Exercise 143 Find the line of intersection of the planes

$$(\alpha) \quad x + y - z = 2 \quad \text{and} \quad (\beta) \quad (2\vec{i} - \vec{k}) \bullet \vec{r} = 2.$$

Exercise 144 Find the line which passes through the origin and intersects the plane

$$x + y + 2z = 6$$

orthogonally.

Exercise 145

(a) Find the distance from the point $(0, 2, 4)$ to the plane

$$x + 2y + 2z = 3.$$

(b) Show that the distance from the point $P_0(x_0, y_0, z_0)$ to the plane with equation $ax + by + cz + d = 0$ is

$$\delta = \frac{|ax_0 + by_0 + cz_0 + d|}{\sqrt{a^2 + b^2 + c^2}}.$$

(c) Use the formula above to show that the distance between the two parallel planes

$$(\alpha) \quad ax + by + cz = d \quad \text{and} \quad (\beta) \quad ax + by + cz = e$$

is

$$\delta = \frac{|d - e|}{\sqrt{a^2 + b^2 + c^2}}.$$

Chapter 10

Complex Numbers

Topics :

1. NUMBER SYSTEMS

2. ALGEBRAIC OPERATIONS ON COMPLEX NUMBERS

3. DE MOIVRE'S FORMULA

4. APPLICATIONS

Beginning with the *natural* numbers such as 0, 1 and 2, we proceed to the *integers*, then to the *rational* numbers, then to the *real* numbers, and then to the *complex* numbers. Each stage is motivated by our desire to be able to solve a certain kind of equation. Real numbers were understood remarkably well by the ancient Greeks. Complex numbers were used freely many years before they could be treated rigorously; that was how the word "imaginary" acquired its technical meaning.

10.1   Number systems

The first *numbers* that we consider in arithmetic are the **natural numbers**, forming a sequence that begins with 0 and never ends. On the *set* of natural numbers

$$\mathbb{N} := \{0, 1, 2, 3, \dots\}$$

the operations of *addition* and *multiplication* can be defined, and we shall call the triple $(\mathbb{N}, +, \cdot)$ the **natural number system**.

    The problem of solving such an equation as

$$x + 2 = 1$$

motivates the discovery of the **integers**, which include not only the natural numbers (the "non-negative integers") but also the *negative* integers. The sequence of integers, which has neither beginning nor end, is conveniently represented by *points* evenly spaced along a straight line (which we may think of as the x-axis of ordinary analytic geometry). In this representation, addition and subtraction appear as *translations* : the transformation $x \mapsto x + a$ shifts each point through a spaces to the right if a is positive, and through $-a$ spaces to the left if a is negative; that is, the operation of adding a is the translation that transforms 0 into a.

    The *set* of integers

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

is considered together with operations of *addition* and *multiplication*, and we shall call the triple $(\mathbb{Z}, +, \cdot)$ the **system of integers**.

NOTE :   These new operations on $\mathbb{Z}$ are not the *same* as the ones on $\mathbb{N}$, but they are defined such that when the integers are just natural numbers, the operations reduce to the operations of the natural numbers system. Clearly,

$$\mathbb{N} \subseteq \mathbb{Z}$$

and anything that can be done with natural numbers, can be done with integers. In this sense, *the system of integers extends the natural number system.*

The problem of solving such an equation as

$$2x = 1$$

motivates the discovery of the **rational numbers** $r = \frac{m}{n}$, where m is an integer and n is a natural number ; these include not only the integers $m = \frac{m}{1}$, but also *fractions* such as $\frac{1}{2}$ and $-\frac{4}{3}$.

NOTE :   We usually write each fraction in its "lowest terms", so that the numerator and the denominator have no common factor.

The rational numbers cannot be written down successively in their natural order, because between any two of them there is another, and consequently and infinity of others. The corresponding points are *dense* on the x-axis, and at first sight seem to cover it completely. Multiplication and division appear as *dilations* : the transformation $x \mapsto rx$ is the dilation of ratio r and center O, where O is the origin; that is, multiplication by r is the dilation of center O that transforms 1 into r. Of course, r may be either positive or negative. In particular, multiplication by -1 is the *half-turn* about O.

The *set* of rational numbers

$$\mathbb{Q} := \left\{ \frac{m}{n} \,|\, m, n \in \mathbb{Z}, \ n \neq 0 \right\}$$

is considered together with operations of *addition* and *multiplication*, and we shall call the triple $(\mathbb{Q}, +, \cdot)$ the **system of rational numbers**.

NOTE :   Again, the operations on $\mathbb{Q}$ are denoted by the same symbols as the ones on $\mathbb{Z}$ and $\mathbb{N}$ and *the system of rational numbers extends the system of integers* in the same sense as before. So we have

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

The problem of solving such an equation as

$$x^2 = 2$$

motivates the discovery of the **real numbers**, which include not only the rational numbers but also the *irrational* numbers (such as $\sqrt{2}$ and π), which cannot be expressed as fractions. Roughly speaking, rational numbers have a *decimal representation* that terminates in zeros or which has a repeating block of digits. The *set* $\mathbb{R}$ of real numbers is taken to be the set of *all* decimal expansions. Geometrically, this means that the *number line* has now become a *continuum*. [A real number may be defined to be the *limit* of a convergent sequence of rational numbers, or (more precisely) the set of all sequences "equivalent" (in a specified sense) to a given sequence; for example, the real number π is the limit of the sequence

$$3, \ 3.1, \ 3.14, \ 3.141, \ 3.1415, \ \ldots]$$

NOTE :   The operations of addition and multiplication on $\mathbb{Q}$ can also be extended to the larger set $\mathbb{R}$ and we shall call the triple $(\mathbb{R}, +, \cdot)$ the **real number system**. We have

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

with the operations of addition and multiplication being extended all the way up, retaining the symbols $+$ and $\cdot$ as we go.

The problem of solving such an equation as

$$x^2 + 1 = 0$$

motivates the discovery of the **complex numbers**, which include not only the real numbers but also such "imaginary" numbers as the *the square root of* -1.

Complex numbers

Since the real numbers occupy the whole x-axis, it is natural to try to represent the complex numbers by all *points* (or *vectors*) in the (x, y)-plane (called the **complex plane**); that is, to define them as *ordered pairs of real numbers with suitable rules for their addition and multiplication.*

In the complex plane (also called the **Argand diagram**), points are added like the corresponding vectors from the origin O :

$$(x, y) + (a, b) := (x + a, y + b). \tag{10.1}$$

In other words, to add (a, b) we apply the translation that takes $(0, 0)$ to (a, b).

Multiplication by an integer still appears as a dilation; for instance,

$$2(x, y) = (x, y) + (x, y) = (2x, 2y).$$

In particular, multiplication by -1 is the half-turn about O. What, then, is multiplication by the "square root of -1" ? This must be a transformation whose "square" is the half-turn about O. The obvious answer is a *quater-turn* (or *rotation* through an angle of $90°$) about O.

Then multiplication by an arbitrary complex number should be a transformation which leaves O invariant and includes both dilations and rotations as special cases. The obvious transformation of this kind is a *rotation-dilation* (the product of a rotation and a dilation about O). It turns out that the rule for multiplication is

$$(a, b) \cdot (x, y) := \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = (ax - by, bx + ay). \tag{10.2}$$

NOTE : We shall use *juxtaposition* $(a, b)(x, y)$ to denote $(a, b) \cdot (x, y)$, just as we often do with real numbers.

The *set* of complex numbers is denoted by $\mathbb{C}$ and we shall call the triple $(\mathbb{C}, +, \cdot)$ the **complex number system**.

The mapping

$$\varphi : \mathbb{R} \to \mathbb{C}, \quad x \mapsto (x, 0)$$

is a one-to-one mapping that "preserves" addition and multiplication ; that is,

$$\varphi(x + y) = \varphi(x) + \varphi(y) \quad \text{and} \quad \varphi(xy) = \varphi(x)\varphi(y)$$

for all $x, y \in \mathbb{R}$. It follows that $\varphi(\mathbb{R}) \subseteq \mathbb{C}$ *is a faithful copy of the (number system)* $\mathbb{R}$. We therefore *identify* $\mathbb{R}$ with $\varphi(\mathbb{R}) \subseteq \mathbb{C}$ and write x for $(x, 0)$.

NOTE :   We shall allow ourselves to think of $\mathbb{R}$ as a *subset* of $\mathbb{C}$, and shall call members of $\varphi(\mathbb{R})$ "real". In other words, via this identification, $\mathbb{C}$ becomes a (number system) *extension* of $\mathbb{R}$ and thus we have

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

Introducing the special symbol

$$\boxed{i := (0, 1) \in \mathbb{C}}$$

we have

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1.$$

The number i is often called the **imaginary unit** of $\mathbb{C}$.

10.1.1 EXAMPLE.   Find

$$i^3, \ i^4, \ i^5, \ i^{23}, \quad \text{and} \quad i^{2000}.$$

SOLUTION :   We have

$$
\begin{aligned}
i^3 &= i^2 i = -i, \\
i^4 &= i^3 i = -i^2 = 1, \\
i^5 &= i^4 i = i, \\
i^{23} &= (i^4)^5 i^3 = -i, \\
i^{2000} &= (i^4)^{500} = 1.
\end{aligned}
$$

Every complex number $z = (x, y) \in \mathbb{C}$ admits a *unique representation*

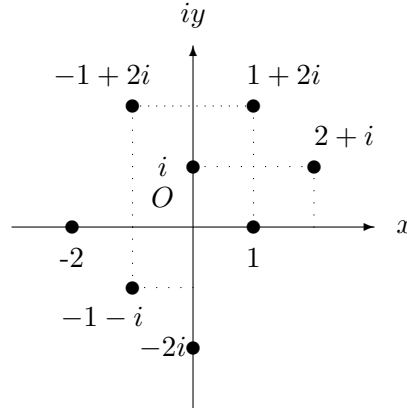$$z = (x, y) = (x, 0) + (0, y) = x + y(0, 1) = x + yi = x + iy;$$

that is

$$\boxed{z = x + iy}$$

with $x, y \in \mathbb{R}$. This is the usual way to write complex numbers and will be called the **normal form**. The real numbers x and y are called the **real part** and the **imaginary part** of z, respectively, and we write

$$x = \operatorname{Re}(z) \quad \text{and} \quad y = \operatorname{Im}(z).$$

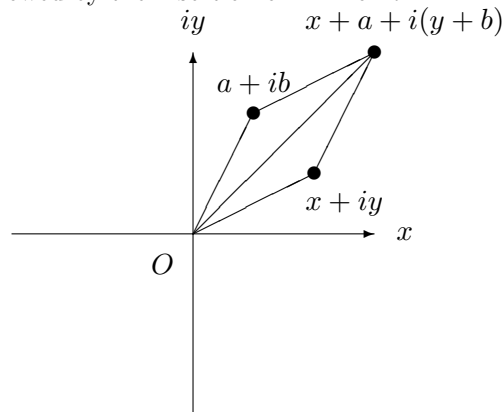A complex number of the form iy (with $x = 0$) is called **imaginary**.

Complex numbers as points (in the plane).

NOTE : In this notation, the rules (1) and (2) become

$$(x + iy) + (a + ib) = (x + a) + i(y + b)$$

$$(a + ib)(x + iy) = ax - by + i(ay + bx)$$

which may be thought of as ordinary addition and multiplication, treating the symbol i as an indeterminate, followed by the insertion of -1 for i^2.

The sum of two complex numbers.

10.1.2 EXAMPLE.   Consider a nonzero complex number z. What is the geometric relationship between z and iz in the complex plane ?

SOLUTION :   If $z = a + ib$, then $iz = -b + ia$. We obtain the vector $\begin{bmatrix} -b \\ a \end{bmatrix}$ (representing iz) by rotating the vector $\begin{bmatrix} a \\ b \end{bmatrix}$ (representing z) through an angle of $90°$ in the counterclockwise direction.

10.1.3 EXAMPLE.   If $z = 3 + 4i$ and $w = 1 + i$, find

$$\mathrm{Im}\,(z + 2w^2).$$

SOLUTION :   We have

$$z + 2w^2 = 3 + 4i + 2(1 + i)^2 = 3 + 4i + 4i = 3 + 8i$$
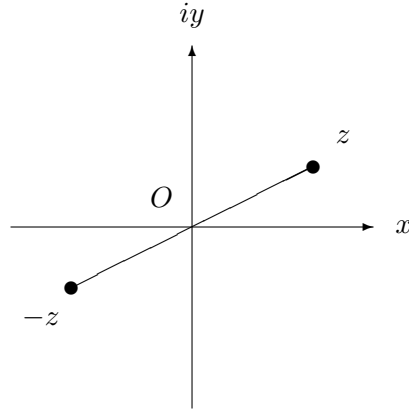
and hence

$$\mathrm{Im}\,(z + 2w^2) = 8.$$

10.2   Algebraic operations on complex numbers

For a complex number $z = x + iy$ we define

$$\boxed{-z := -x - iy}$$ (the **opposite** of z)

and (for $z \neq 0$)

$$\boxed{z^{-1} := \frac{1}{x^2 + y^2}(x - iy).}$$ (the **inverse** of z).

The opposite of a complex number : $-z$.

If z_1, z_2 are two complex numbers, we write $z_1 - z_2$ instead of $z_1 + (-z_2)$ and $\frac{z_1}{z_2}$ instead of $z_1 z_2^{-1}$ (for $z_2 \neq 0$), just as we did with real numbers.

10.2.1 EXAMPLE.   Find the inverse of $2 + i$.

SOLUTION :   We have

$$(2 + i)^{-1} = \frac{1}{5}(2 - i).$$

We see that

$$(2 + i)(2 + i)^{-1} = \frac{1}{5}(2 + i)(2 - i) = \frac{5}{5} = 1.$$

10.2.2 EXAMPLE.   Write

$$E = \left(\frac{1 + 2i}{2 + i}\right)^3$$

in the normal form.

SOLUTION :   We have

$$E = \left[(1 + 2i)(2 + i)^{-1}\right]^3 = \left(\frac{1}{5}(1 + 2i)(2 - i)\right)^3 = \left(\frac{1}{5}(4 - 3i)\right)^3 = \frac{1}{125}(-44 + 117i)\cdot$$

The following proposition summarizes the algebraic properties of the addition and multiplication of complex numbers.

10.2.3 PROPOSITION.   *If $z, z_1, z_2, z_3 \in \mathbb{C}$, then :*

(1) $z_1 + z_2 = z_2 + z_1$.

(2) $z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$.

(3) $z + 0 = 0 + z = z$.

(4) $z + (-z) = (-z) + z = 0$.

(5) $z_1 \cdot z_2 = z_2 \cdot z_1$.

(6) $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$.

(7) $z \cdot 1 = 1 \cdot z = z$.

(8) $z \cdot z^{-1} = z^{-1} \cdot z = 1 \quad (z \neq 0)$.

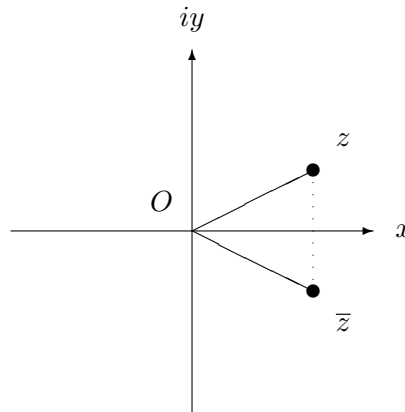(9) $z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$.

PROOF :   Exercise.

NOTE :   The properties listed above may be summarized by saying that the complex number system $(\mathbb{C}, +, \cdot)$ is a (commutative) *field*.

For a complex number $z = x + iy$ we define

$$\boxed{\bar{z} := x - iy}\qquad \text{(the \textbf{conjugate} of } z).$$

Geometrically, the conjugate $\bar{z}$ is the *reflection* of z in the x-axis (the so-called **real axis**).

The conjugate of a complex number : $\overline{z}$.

10.2.4 PROPOSITION.   *If $z, z_1, z_2 \in \mathbb{C}$, then :*

    (1) $\overline{z_1 + z_2} = \bar{z}_2 + \bar{z}_1$.

    (2) $\overline{z_1 - z_2} = \bar{z}_1 - \bar{z}_2$.

    (3) $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$.

    (4) $\bar{\bar{z}} = z$.

    (5) $\overline{\left(\dfrac{z_1}{z_2}\right)} = \dfrac{\bar{z}_1}{\bar{z}_2}$.

    (6) $\mathrm{Re}\,(z) = \frac{1}{2}(z + \bar{z})$.

    (7) $\mathrm{Im}\,(z) = \frac{1}{2i}(z - \bar{z})$.

    (8) $z \in \mathbb{R} \iff z = \bar{z}$.

    (9) $z \in i\,\mathbb{R} \iff z = -\bar{z}$.

PROOF :   Exercise.
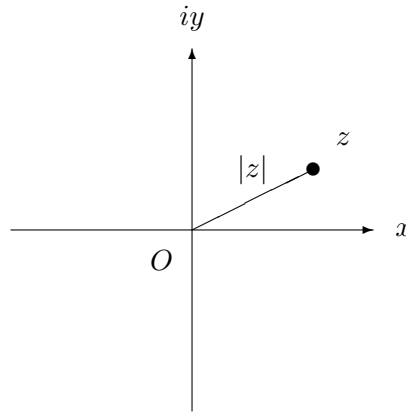
If $z = x + iy \in \mathbb{C}$, then the real number

$$\boxed{|z| := \sqrt{x^2 + y^2}}$$

is called the **modulus** (or **absolute value**) of z. In other words, $|z|$ is nothing but the *distance* from the origin to the point (x, y) ; alternatively, $|z|$ is the *length* of the (geometric) vector $\begin{bmatrix} x \\ y \end{bmatrix}$.

The modulus of a complex number : $|z|$.

NOTE :   If $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, then $|z_1 - z_2|$ is the distance between the points (x_1, y_1) and (x_2, y_2).

10.2.5 PROPOSITION.   *If* $z, z_1, z_2 \in \mathbb{C}$, *then :*

(1) $|z| \geq 0$, *and* $|z| = 0 \iff z = 0$.

(2) $z \cdot \bar{z} = |z|^2$.

(3) $|z_1 \cdot z_2| = |z_1||z_2|$.

(4) $|z| = |-z| = |\bar{z}|$.

(5) $\left| \dfrac{z_1}{z_2} \right| = \dfrac{|z_1|}{|z_2|}$ $(z_2 \neq 0)$.

(6) $\mathrm{Re}\,(z) \leq |\mathrm{Re}\,(z)| \leq |z|$.

(7) $\mathrm{Im}\,(z) \leq |\mathrm{Im}\,(z)| \leq |z|$.

(8) $\big|\,|z_1| - |z_2|\,\big| \leq |z_1 - z_2|$.

PROOF :   Exercise.

10.2.6 EXAMPLE.   Let $z, w \in \mathbb{C}$. Then

$$|z + w| \leq |z| + |w|.$$

(This result is known as the **triangle inequality**).

SOLUTION :   We have

$$
\begin{aligned}
|z + w|^2 &= (z + w) \cdot (\overline{z + w}) \\
&= (z + w) \cdot (\bar{z} + \bar{w}) \\
&= z \cdot \bar{z} + z \cdot \bar{w} + \bar{z} \cdot w + w \cdot \bar{w} \\
&= |z|^2 + z \cdot \bar{w} + \bar{z} \cdot w + |w|^2 \\
&= |z|^2 + 2\mathrm{Re}\,(z \cdot \bar{w}) + |w|^2 \\
&\leq |z|^2 + 2|z \cdot \bar{w}| + |w|^2 \\
&= |z|^2 + 2|z|\,|\bar{w}| + |w|^2 \\
&= |z|^2 + 2|z|\,|w| + |w|^2 \\
&= (|z| + |w|)^2.
\end{aligned}
$$

The result now follows.

10.3   De Moivre's formula

Sometimes it is useful to describe a complex number in *polar coordinates*.

If $z = x + iy \in \mathbb{C} \setminus \{0\}$, then we can write

$$
\begin{aligned}
z = x + iy &= \sqrt{x^2 + y^2}\left(\frac{x}{\sqrt{x^2 + y^2}} + i\frac{y}{\sqrt{x^2 + y^2}}\right) \\
&= |z|\left(\frac{\mathrm{Re}\,(z)}{|z|} + i\frac{\mathrm{Im}\,(z)}{|z|}\right) \\
&= r(\cos\theta + i\sin\theta)
\end{aligned}
$$

where $r = |z|$ and θ is an *angle* such that

$$
\cos\theta = \frac{x}{r} \quad \text{and} \quad \sin\theta = \frac{y}{r}.
$$

NOTE :   The existence of θ is assured since $\left(\frac{x}{r}\right)^2 + \left(\frac{y}{r}\right)^2 = 1$ and, in fact, there are many such θ. Geometrically, r is the distance (in the complex plane) between the origin and the point z, and θ measures the angle between the real axis and the vector z.

Any real number θ such that $z = |z|(\cos\theta + i\sin\theta)$ is said to be an **argument** of z. We denote by $\mathrm{Arg}\,z$ the set of all arguments of z ; that is,

$$
\mathrm{Arg}\,z := \left\{\theta \in \mathbb{R} \mid \cos\theta = \frac{\mathrm{Re}\,(z)}{|z|} \text{ and } \sin\theta = \frac{\mathrm{Im}\,(z)}{|z|}\right\}.
$$

The number $\arg z \in \mathrm{Arg}\,z$ such that $-\pi < \arg z \leq \pi$ is caled the **principal argument** of z. We have

$$
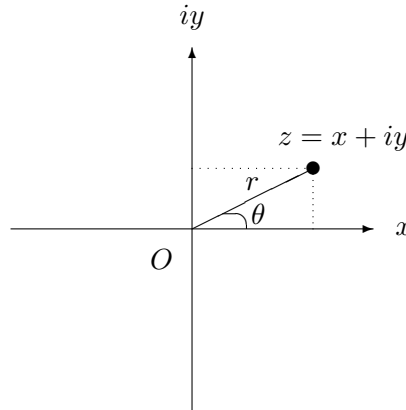\mathrm{Arg}\,z = \{\arg z + 2k\pi \mid k \in \mathbb{Z}\}.
$$

NOTE :   Our *normalization* of θ to the interval $(-\pi, \pi]$ was arbitrary; in general, any half-open interval of length 2π is suitable.

The representation

$$z = r(\cos\theta + i\sin\theta)$$

is called the **polar form** of the complex number z. The real numbers $r = |z|$ and $\theta = \arg z$ are the **polar coordinates** of z.

The polar form of a complex number : $r(\cos\theta + i\sin\theta)$.

10.3.1 EXAMPLE.   Find the modulus and the (principal) argument of $z = -2 + 2i$.

SOLUTION :   We have

$$r = |z| = \sqrt{(-2)^2 + 2^2} = \sqrt{8} = 2\sqrt{2}\,.$$

Representing z in the complex plane, we see that $\frac{3\pi}{4}$ is an argument of z (in fact, its principal argument).

10.3.2 EXAMPLE.   Determine $\mathrm{Arg}\,(-1)$ and $\mathrm{Arg}\,(1-i)$.

SOLUTION :   We have

$$
\begin{aligned}
\mathrm{Arg}\,(-1) &= \left\{\theta \mid \cos\theta = \frac{-1}{1} \ \text{ and } \ \sin\theta = \frac{0}{1}\right\}\\
&= \{\theta \mid \cos\theta = -1 \ \text{ and } \ \sin\theta = 0\}\\
&= \{\pi + 2k\pi \mid k \in \mathbb{Z}\}
\end{aligned}
$$

and

$$\begin{aligned}\text{Arg}\,(1-i) \ &= \ \left\{\theta \mid \cos\theta = \frac{1}{\sqrt 2}\ \text{ and }\ \sin\theta = -\frac{1}{\sqrt 2}\right\} \\ &= \ \left\{-\frac{\pi}{4}+2k\pi \mid k\in\mathbb{Z}\right\}.\end{aligned}$$

10.3.3 EXAMPLE.   Let $z\in\mathbb{C}\setminus\{0\}$. Then

$$\text{Arg}\,\bar z = \text{Arg}\,(z^{-1}).$$

SOLUTION :   Let $z = r(\cos\theta + i\sin\theta)$, where $\theta = \arg z$; then $\bar z = r(\cos\theta - i\sin\theta) = r(\cos(-\theta)+i\sin(-\theta))$ and hence

$$\text{Arg}\,\bar z = \{-\theta + 2k\pi \mid k\in\mathbb{Z}\}.$$

On the other hand,

$$\begin{aligned}z^{-1} \ &= \ \frac{\bar z}{|z|^2} \\ &= \ \frac{r(\cos(-\theta)+i\sin(-\theta))}{r^2} \\ &= \ \frac{1}{r}(\cos(-\theta)+i\sin(-\theta))\end{aligned}$$

and so

$$\text{Arg}\,(z^{-1}) = \{-\theta + 2k\pi \mid k\in\mathbb{Z}\}.$$

10.3.4 EXAMPLE.   Write the complex numbers -3, i, and $-1+i$ in the polar form.

SOLUTION :   We have

$$\begin{aligned}-3 \ &= \ 3(\cos\pi + i\sin\pi), \\ i \ &= \ \cos\frac{\pi}{2}+i\sin\frac{\pi}{2}, \\ -1+i \ &= \ \sqrt 2\left(\cos\frac{3\pi}{4}+i\sin\frac{3\pi}{4}\right).\end{aligned}$$

The most important property of the polar form is given in the proposition below. It will allow us to have a very good geometric interpretation for the product of two complex numbers.

10.3.5 PROPOSITION.   *Let* $z = \cos\alpha + i\sin\alpha$ *and* $w = \cos\beta + i\sin\beta$. *Then*

$$zw = \cos(\alpha + \beta) + i\sin(\alpha + \beta).$$

SOLUTION :   We have

$$
\begin{aligned}
zw &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\
&= \cos\alpha\cos\beta - \sin\alpha\sin\beta + i(\sin\alpha\cos\beta + \sin\beta\cos\alpha) \\
&= \cos(\alpha + \beta) + i\sin(\alpha + \beta).
\end{aligned}
$$

We observe that the modulus of zw is 1, and $\alpha + \beta$ is an argument of zw.□

In general, if $z = r(\cos\alpha + i\sin\beta)$ and $w = s(\cos\beta + i\sin\beta)$, then

$$zw = rs(\cos(\alpha + \beta) + i\sin(\alpha + \beta)).$$

From this we see that *when we multiply two complex numbers, we multiply the moduli and we add the arguments.* Thus

$$\boxed{|zw| = |z|\,|w| \quad \text{and} \quad \mathrm{Arg}\,(zw) = \mathrm{Arg}\,z + \mathrm{Arg}\,w.}$$
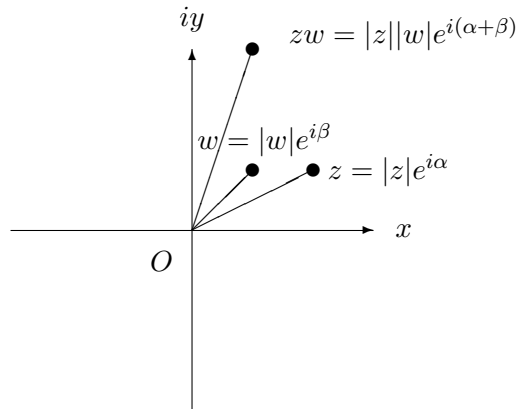
The product of two complex numbers.

10.3.6 EXAMPLE.   Describe the transformation $T : \mathbb{C} \to \mathbb{C}, \quad z \mapsto (3 + 4i)z$ geometrically.

SOLUTION :   We have

$$
\begin{aligned}
|T(z)| &= |3 + 4i|\,|z| = 5|z| \\
\operatorname{Arg}\left(T(z)\right) &= \operatorname{Arg}\left(3 + 4i\right) + \operatorname{Arg} z = \arctan\left(\frac{4}{3}\right) + \operatorname{Arg} z \approx 53° + \operatorname{Arg} z\,.
\end{aligned}
$$

The transformation T is a *rotation-dilation* in the complex plane.

If $z \in \mathbb{C}$ and $n \in \mathbb{N}$, we define the *power* z^n by

$$
z^n := \underbrace{z \cdot z \cdots z}_{n \text{ factors}}.
$$

We put $z^0 := 1$ and for a negative integer $m = -n$ with $n \in \mathbb{N}$, we define

$$
z^m = z^{-n} := \left(z^{-1}\right)^n.
$$

The following result is due to ABRAHAM DE MOIVRE (1667-1754).

10.3.7 THEOREM.   (DE MOIVRE'S FORMULA) *For* $\theta \in \mathbb{R}$ *and* $n \in \mathbb{Z}$

$$
(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).
$$

PROOF :   We first use induction to prove that the result holds for all $n \in \mathbb{N}$.
If $n = 0$, then

$$
(\cos\theta + i\sin\theta)^n = (\cos\theta + i\sin\theta)^0 = 1 = \cos 0 + i\sin 0 = \cos(n\theta) + i\sin(n\theta)\,.
$$

Assume that the formula is true for some $n \in \mathbb{N}$; then

$$
\begin{aligned}
(\cos\theta + i\sin\theta)^{n+1} &= (\cos\theta + i\sin\theta)(\cos\theta + i\sin\theta)^n \\
&= (\cos\theta + i\sin\theta)(\cos n\theta + i\sin n\theta) \\
&= \cos\theta\cos n\theta - \sin\theta\sin n\theta + i(\cos\theta\sin n\theta + \sin\theta\cos n\theta) \\
&= \cos(n+1)\theta + i\sin(n+1)\theta.
\end{aligned}
$$

It follows that the formula is true for all $n \in \mathbb{N}$.

If n is a negative integer, let $n = -m$ with $m \in \mathbb{N}$. Then

$$
\begin{aligned}
(\cos \theta + i \sin \theta)^n &= (\cos \theta + i \sin \theta)^{-m} \\
&= \left(\frac{1}{\cos \theta + i \sin \theta} \right)^m \\
&= (\cos(-\theta) + i \sin(-\theta))^m \\
&= \cos(-m\theta) + i \sin(-m\theta) \\
&= \cos n\theta + i \sin n\theta.
\end{aligned}
$$

$\square$

It is easy matter to check that the rules of exponents extend to complex numbers. Namely :

10.3.8 PROPOSITION.   *Let $z, w \in \mathbb{C}$ and $m, n \in \mathbb{N}$. Then :*

(1) $(zw)^n = z^n w^n$.

(2) $z^{mn} = (z^m)^n$.

(3) $z^m z^n = z^{m+n}$.

(4) $\frac{z^m}{z^n} = z^{m-n}$.

PROOF :   Exercise.

10.3.9 EXAMPLE.   Evaluate the following expression

$$
E = (1 + i)^{10} + (1 - i)^{10}.
$$

SOLUTION :   We have (for $n \in \mathbb{N}$) :

$$
\begin{aligned}
E(n) &= (1 + i)^n + (1 - i)^n \\
&= \left[\sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) \right]^n + \left[\sqrt{2} \left(\cos(-\frac{\pi}{4}) + i \sin(-\frac{\pi}{4}) \right) \right]^n \\
&= 2^{\frac{n}{2}} \left(\cos \frac{n\pi}{4} + i \sin \frac{n\pi}{4} \right) + 2^{\frac{n}{2}} \left(\cos \frac{n\pi}{4} - i \sin \frac{n\pi}{4} \right) \\
&= 2 \cdot 2^{\frac{n}{2}} \cos \frac{n\pi}{4} = 2^{\frac{n}{2}+1} \cos \frac{n\pi}{4} .
\end{aligned}
$$

In particular, for $n = 10$, we get :

$$E = E(10) = (1 + i)^{10} + (1 - i)^{10} = 2^6 \cos \frac{5\pi}{2} = 0.$$

10.4 Applications

$\boxed{\text{A}}$ (Complex-valued functions)   A **complex-valued function** $t \mapsto z = f(t)$ is a function from $\mathbb{R}$ to $\mathbb{C}$: the *input* t is real, and the *output* z is complex.

10.4.1 EXAMPLE.   Here are two examples of complex-valued functions :

$$z = t + it^2 \quad \text{and} \quad z = \cos t + i \sin t.$$

For each t, the output z can be represented as a point in the *complex plane*. As we let t vary, we trace out a *trajectory* in the complex plane (a *parabola* and a *circle*, respectively).

   Consider the complex-valued function

$$f : \mathbb{R} \to \mathbb{C}, \quad f(t) := \cos t + i \sin t.$$

This function has remarkable properties. For instance,

   (1) $f(t) \cdot f(s) = f(t + s)$.
   (2) $\frac{d}{dt} f(t) = i \, f(t)$.
   (3) $f(0) = 1$.

It can be shown that *there exists a unique complex-valued function that satisfies conditions (2) and (3)*; this function also satisfies condition (1).

NOTE :   The *exponential function*

$$\exp : \mathbb{R} \to \mathbb{R}, \quad t \mapsto \exp(t) := e^{at} \quad (a \in \mathbb{R})$$

has the properties :

$$\frac{d}{dt} \exp(t) = a \exp(t) \quad \text{and} \quad \exp(0) = 1.$$

This motivates us to write

EULER'S FORMULA : *For any real number θ*

$$\boxed{e^{i\theta} := \cos\theta + i\sin\theta.}$$

NOTE: It has been known since the 18th century that the exponential function and the trigonometric functions are related. This remarkable relationship was discovered by LEONHARD EULER (1707-1783). The case $\theta = \pi$ leads to the intriguing formula $e^{i\pi} + 1 = 0$; this has been called the most beautiful formula in all mathematics.

Euler's formula can be used to write the polar form of a complex number more succintly :

$$z = r(\cos\theta + i\sin\theta) = re^{i\theta}.$$

This representation is known as the **exponential form** of the complex number z.

10.4.2 PROPOSITION.   *If $z = re^{i\theta} \in \mathbb{C}$, then :*

$$z^n = r^n e^{in\theta}, \quad n \in \mathbb{Z}.$$

In particular, $z^{-1} = \frac{1}{r}e^{-i\theta}$ and hence $\overline{z} = re^{-i\theta}$.

PROOF :   Exercise.

10.4.3 EXAMPLE.   Write $z = i$ in exponential form.

SOLUTION :   We have $r = 1$ and $\theta = \arg z = \frac{\pi}{2} \cdot$ Hence

$$z = e^{i\frac{\pi}{2}}.$$

10.4.4 EXAMPLE.   Write $z = 2\,e^{i\pi}$ in normal form.

SOLUTION :   Here we are given $r = 2$ and $\theta = \arg z = \pi$. Hence

$$z = 2(\cos\pi + i\sin\pi) = 2(-1 + i0) = -2.$$

10.4.5 EXAMPLE. Find the real and imaginary parts of $(1 + 2i) \, e^{-it}$.

SOLUTION : Let $z(t) = (1 + 2i) \, e^{-it}$. Then

$$z(t) = (1 + 2i)(\cos t + i \sin t) = (\cos t + 2 \sin t) + i(2 \cos t - \sin t).$$

Hence

$$\operatorname{Re}(z(t)) = \cos t + 2 \sin t$$
$$\operatorname{Im}(z(t)) = 2 \cos t - \sin t.$$

If $\theta \in \mathbb{R}$, then

$$e^{i\theta} = \cos \theta + i \sin \theta$$
$$e^{-i\theta} = \cos \theta - i \sin \theta.$$

Adding these and dividing by 2, we obtain :

$$\cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \cdot$$

Subtracting these and dividing by $2i$, we obtain :

$$\sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i} \cdot$$

Thus the familiar trigonometric functions can be expressed in terms of complex-valued functions. This finds application in a number of situations.

10.4.6 EXAMPLE. Express $\cos 4\theta$ in terms of sines and cosines of θ.

SOLUTION : We have

$$
\begin{aligned}
\cos 4\theta &= \operatorname{Re}(e^{i4\theta}) \\
&= \operatorname{Re}(\cos \theta + i \sin \theta)^4 \\
&= \operatorname{Re}\left(\cos^4 \theta + 4 \cos^3 \theta(i \sin \theta) + 6 \cos^2 \theta(i \sin \theta)^2 + 4 \cos \theta(i \sin \theta)^3 + (i \sin \theta)^4\right) \\
&= \operatorname{Re}\left((\cos^4 \theta - 6 \cos^2 \theta \sin^2 \theta + \sin^4 \theta) + i(4 \cos^3 \theta \sin \theta - 4 \cos \theta \sin^3 \theta)\right) \\
&= \cos^4 \theta - 6 \cos^2 \theta \sin^2 \theta + \sin^4 \theta.
\end{aligned}
$$

10.4.7 EXAMPLE.   Express $\sin^5 \theta$ in terms of sines and cosines of multiples of θ.

SOLUTION :   We have

$$
\begin{aligned}
\sin^5 \theta &= \left(\frac{e^{i\theta} - e^{-i\theta}}{2i} \right)^5 \\
&= \frac{1}{(2i)^5} \left(e^{i5\theta} - 5e^{i4\theta}e^{-i\theta} + 10e^{i3\theta}e^{-i2\theta} - 10e^{2\theta}e^{-i3\theta} + 5e^{i\theta}e^{-i4\theta} - e^{-i5\theta} \right) \\
&= \frac{1}{32i} \left((e^{i5\theta} - e^{-i5\theta}) - 5(e^{i3\theta} - e^{-i3\theta}) + 10(e^{i\theta} - e^{-i\theta}) \right) \\
&= \frac{1}{16} (\sin 5\theta - 5 \sin 3\theta + 10 \sin \theta).
\end{aligned}
$$

10.4.8 EXAMPLE.   Evaluate the sum

$$
S = \sum_{k=0}^{n-1} \sin k\theta \, .
$$

SOLUTION :   The trick is to write each $\sin k\theta$ as $\operatorname{Im}\left(e^{ik\theta} \right)$ and note that the sum is a geometric series with ratio $e^{i\theta}$. We have

$$
S = \sum_{k=0}^{n-1} \sin k\theta = \operatorname{Im} \left(1 + e^{i\theta} + e^{i2\theta} + \cdots + e^{i(n-1)\theta} \right) .
$$

If the ratio $e^{i\theta}$ is 1, then the sum is simply n. We therefore assume that

$e^{i\theta} \neq 1$. Thus

$$
\begin{aligned}
S = \sum_{k=0}^{n-1} \sin k\theta \;&=\; \operatorname{Im}\left(\frac{1 - e^{in\theta}}{1 - e^{i\theta}}\right) \\
&=\; \operatorname{Im}\left(\frac{1 - e^{in\theta}}{1 - e^{i\theta}} \cdot \frac{e^{-i\frac{\theta}{2}}}{e^{-i\frac{\theta}{2}}}\right) \\
&=\; \operatorname{Im}\left(\frac{e^{i(n-\frac{1}{2})\theta} - e^{-i\frac{\theta}{2}}}{e^{i\frac{\theta}{2}} - e^{-i\frac{\theta}{2}}}\right) \\
&=\; \operatorname{Im}\left(\frac{e^{i(n-\frac{1}{2})\theta} - e^{-i\frac{\theta}{2}}}{2i\sin\frac{\theta}{2}}\right) \\
&=\; \operatorname{Im}\left(-i\,\frac{e^{i(n-\frac{1}{2})\theta} - e^{-i\frac{\theta}{2}}}{2\sin\frac{\theta}{2}}\right) \\
&=\; \frac{\cos\frac{\theta}{2} - \cos(n-\frac{1}{2})\theta}{2\sin\frac{\theta}{2}} \\
&=\; \frac{\sin\frac{n\theta}{2}\,\sin\frac{(n-1)\theta}{2}}{\sin\frac{\theta}{2}} \,.
\end{aligned}
$$

Since $e^{i\theta} \neq 1$, we know that $\sin\frac{\theta}{2} \neq 0$ and so calculations above are meaningful.

$\boxed{\text{B}}$ (Solutions of equations)

Equations of the form $x^n = w$

Equations of the form

$$x^n = w$$

where w is a fixed complex number, can be solved by writing x and w in polar (or exponential) form. If we let $x = r(\cos\theta + i\sin\theta) = re^{i\theta}$, then we obtain equations for r and θ which we can then solve.

10.4.9 EXAMPLE. Solve

$$x^2 = -d^2\,, \quad d > 0.$$

SOLUTION :   We write

$$x = r(\cos\theta + i\sin\theta) \quad \text{and} \quad -d^2 = d^2(\cos\pi + i\sin\pi)\,.$$

Then we have (using de Moivre's formula)

$$r^2(\cos 2\theta + i\sin 2\theta) = d^2(\cos\pi + i\sin\pi).$$

We obtain

$$r^2 = d^2 \quad \text{and} \quad 2\theta = \pi + 2k\pi\,, \quad k \in \mathbb{Z}$$

and hence

$$r = d \quad \text{and} \quad \theta = \frac{\pi}{2} + k\pi\,, \quad k \in \mathbb{Z}.$$

The set of solutions is

$$\left\{ d(\cos\theta + i\sin\theta) \,|\, \theta = \frac{\pi}{2} + k\pi\,,\ k \in \mathbb{Z} \right\} = \left\{ d(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}),\ d(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}) \right\}$$
$$= \{di,\ -di\}.$$

10.4.10 EXAMPLE.   Solve

$$x^4 = -1.$$

SOLUTION :   We write

$$x = re^{i\theta} \quad \text{and} \quad -1 = e^{i\pi}.$$

Then we have

$$r^4 e^{i4\theta} = e^{i\pi}$$

and hence

$$r^4 = 1 \quad \text{and} \quad 4\theta = \pi + 2k\pi\,, \quad k \in \mathbb{Z}.$$

We get

$$r = 1 \quad \text{and} \quad \theta = \frac{\pi}{4} + k\frac{\pi}{2}\,, \quad k \in \mathbb{Z}.$$

The solution are (for $k = 0, 1, 2, 3$) :

$$
\begin{aligned}
x_0 &= e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}}(1 + i)\,; \\
x_1 &= e^{i\frac{3\pi}{4}} = \frac{1}{\sqrt{2}}(-1 + i)\,; \\
x_2 &= e^{i\frac{5\pi}{4}} = \frac{1}{\sqrt{2}}(-1 - i)\,; \\
x_3 &= e^{i\frac{7\pi}{4}} = \frac{1}{\sqrt{2}}(1 - i).
\end{aligned}
$$

For $k \geq 4$ we get only repeats of these four roots.

NOTE : The roots are complex-conjugate pairs.

10.4.11 EXAMPLE. Find all the solutions (roots) of

$$
x^n = 1\,, \quad n \in \mathbb{N}.
$$

SOLUTION : We write

$$
x = re^{i\theta} \quad \text{and} \quad 1 = e^{i0}
$$

and thus

$$
x^n = r^n e^{in\theta} = e^{i0}.
$$

It follows that

$$
r^n = 1 \quad \text{and} \quad n\theta = 2k\pi\,, \quad k \in \mathbb{Z}.
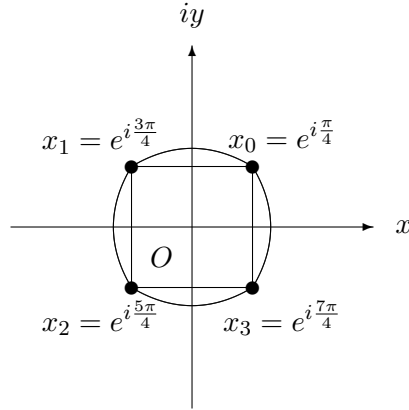$$

Hence

$$
r = 1 \quad \text{and} \quad \theta = \frac{2k\pi}{n}\,, \quad k = 0, 1, 2, \ldots, n - 1.
$$

[For $k \geq n$ we get only repeats of these n roots.]

The solution are

$$
x_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\,, \quad k = 0, 1, 2, \ldots, n - 1.
$$

NOTE : The roots are either real (for instance $x_0 = 1$) or in complex-conjugate pairs.

The roots of the equation $x^4 = -1$.

Quadratic equations

If $a, b,$ and c are real numbers, then the *quadratic equation*

$$ax^2 + bx + c = 0$$

has real solutions given by

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

if $\Delta := b^2 - 4ac \geq 0$. However, if $\Delta < 0$ the solutions are complex.

Let $-\Delta := d^2, \quad d > 0$. We complete the square to obtain

$$a \left[\left(x + \frac{b}{2a} \right)^2 + \frac{4ac - b^2}{4a^2} \right] = 0$$

which leads to

$$\left(x + \frac{b}{2a} \right)^2 = -\frac{d^2}{4a^2} \, .$$

Thus

$$x + \frac{b}{2a} = \pm i \, \frac{d}{2a}$$

and hence

$$\boxed{x_{1,2} = \frac{-b \pm i \sqrt{4ac - b^2}}{2a} \, .}$$

NOTE : (1) If $a, b, c \in \mathbb{R}$, the roots of the *polynomial* of degree 2 $p(x) = ax^2 + bx + c$ are either real or a complex-conjugate pair.

(2) The formula above remains valid if the coefficients a, b, c are complex numbers: we can still employ the method of the square to find the roots.

Polynomial equations of degree n

Let $p_n(x)$ be a *polynomial* of degree n (with complex coefficients). Then, after multiplying through by the reciprocal of the coefficient of x^n, we may assume that $p_n(x)$ has the form

$$p_n(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Polynomials whose highest power has coefficient 1 are called **monic**.

Perhaps the most remarkable property of the complex numbers is expressed in the *fundamental theorem of algebra*, first demonstrated by CARL F. GAUSS (1777-1855).

10.4.12 THEOREM. (FUNDAMENTAL THEOREM OF ALGEBRA) *Every polynomial with complex coefficients has at least one (complex) root.*

Suppose that $x = w$ is a root of $p_n(x)$. This means that

$$p_n(w) = w^n + a_{n-1}w^{n-1} + \cdots + a_1 w + a_0 = 0.$$

If $p_n(x)$ is divided by $x - w$, we obtain the identity

$$\frac{p_n(x)}{x - w} = q_{n-1}(x) + \frac{R}{x - w}$$

where R is a constant and $q_{n-1}(x)$ is a polynomial of degree $n - 1$. Hence,

$$p_n(x) = (x - w)q_{n-1}(x) + R.$$

But this is an *identity* in x, so that by setting $x = w$, we see that $R = 0$ if and only if $p_n(w) = 0$; that is, if and only if w is a root of $p_n(x)$. By

repeated use of this result, we obtain that *every polynomial of degree n with complex coefficients has precisely n roots (if they are properly counted with their multiplicities)*. We can restate this result as follows :

10.4.13 PROPOSITION.   *Any polynomial of degree n*

$$p_n(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with complex coefficients can be written as a product of linear factors

$$p_n(x) = (x - w_1)(x - w_2) \cdots (x - w_n)$$

for some complex numbers $w_1, w_2, \ldots, w_n$. The numbers (roots) w_i need not be distinct.

A common situation arising particularly often in applications is the case in which all the coefficients of the polynomial $p_n(x)$ are real. The following result is easy to prove.

10.4.14 PROPOSITION.   *Let $p_n(x)$ be a polynomial with real coefficients. If $w = a + ib$, $b \neq 0$ is a root of $p_n(x)$ then so is its conjugate $\overline{w} = a - ib$.*

PROOF :   Exercise.

From these two results (PROPOSITION 12.4.13 and PROPOSITION 12.4.14) we obtain

10.4.15 PROPOSITION.   *Any polynomial of degree n*

$$p_n(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with real coefficients can be written as a product of linear and irreducible quadratic factors

$$p_n(x) = (x - r_1)(x - r_2) \cdots (x - r_k)(x^2 + \alpha_1 x + \beta_1) \cdots (x^2 + \alpha_l x + \beta_l)$$

for some real numbers r_1, r_2, ..., r_k, α_1, β_1, ..., α_l, β_l. The numbers (roots) r_i as well as the numbers α_j, β_j need not be distinct.

10.4.16 EXAMPLE. Find the roots of $p(x) = x^4 - 1$ and factor this polynomial.

SOLUTION : Since $x^4 - 1$ is a difference of two squares, we have

$$p(x) = x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x-1)(x+1)(x^2 + 1) = (x-1)(x+1)(x-i)(x+i).$$

Thus the roots are

$$x_1 = 1, \ x_2 = -1, \ x_3 = i, \ x_4 = -i.$$

10.4.17 EXAMPLE. Find a (monic) polynomial of degree 3 whose roots are $0, \ 1, \ 2$.

SOLUTION : Since $(x - 0)$, $(x - 1)$ and $(x - 2)$ must be factors of any such polynomial, we have

$$p_3(x) = x(x - 1)(x - 2) = x^3 - 3x^2 + 2x.$$

10.4.18 EXAMPLE. Find a (monic) polynomial of lowest degree with real coefficients having the roots $1, \ 1$ and $1 - i$.

SOLUTION : Because the roots of a polynomial with real coefficients come in complex-conjugate pairs, the fact that $1 - i$ is a root implies that $1 + i$ is also a root. Hence,

$$(x - (1 - i))(x - (1 + i)) = x^2 - 2x + 2$$

is a factor of $p(x)$. Likewise, $(x - 1)^2$ ia also a factor. Therefore,

$$p(x) = (x^2 - 2x + 2)(x - 1)^2 = x^4 - 4x^3 + 7x^2 - 6x + 2$$

has the required roots. No lower degree polynomial could have four roots, so this is the monic polynomial of least degree with these roots.

10.4.19 EXAMPLE. Solve the equation

$$x^3 + 3x - 4 = 0.$$

SOLUTION : Let $p(x) = x^3 + 3x - 4$. We first try, by inspection, to find a real root of $p(x)$. We spot $p(1) = 0$ and this means that $(x - 1)$ is a factor. Dividing $(x - 1)$ into $p(x)$ we obtain

$$p(x) = (x - 1)(x^2 + x - 4).$$

Thus $p(x)$ is a product of a linear and an irreducible quadratic factor. The solutions of the equation $p(x) = 0$ are (the roots of $p(x)$) :

$$1 \quad \text{and} \quad -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}.$$

10.5 Exercises

Exercise 146 Find
$$i^{17}, \; i^{23}, \; i^{467}.$$

Exercise 147 If $z = 3 + 4i$ and $w = 1 + i$, find :

    (a) $z + w$.

    (b) z^2.

    (c) $i\,w$.

    (d) $(z - 3w)^{100}$.

    (e) $\text{Re}\,(z + 2\omega^2)$.

    (f) $\text{Im}\,(z - w)$.

Exercise 148 Find $\bar{z}$, $\text{Re}\,(z)$, $\text{Im}\,(z)$ and $|z|$ if

$$(a) \quad z = 7, \quad (b) \quad z = -2i, \quad (c) \quad z = (3 + 5i)^2, \quad (d) \quad z = \frac{2 + 3i}{4 - 5i}.$$

Exercise 149 Show that the points (complex numbers) z_1, z_2, z_3 are collinear if and only if $\dfrac{z_2 - z_1}{z_3 - z_1} \in \mathbb{R}$.

Exercise 150 Prove that if $z, w \in \mathbb{C}$, then

$$|z + w|^2 + |z - w|^2 = 2(|z|^2 + |w|^2).$$

This is known as the *parallelogram law*. Justify the name.

Exercise 151 Prove that for $z \in \mathbb{C}$

$$(1 - z)(1 + z + z^2 + \cdots + z^{n-1}) = 1 - z^n$$

and hence deduce that (for $z \neq 1$) :

$$\sum_{k=0}^{n-1} z^k = \frac{1 - z^n}{1 - z} \cdot$$

Exercise 152 Write in the polar (and exponential) form :

(a) $1 + \sqrt{3}\, i$.

(b) $-1 - i$.

(c) $-5 + 5i$.

(d) $\left(\dfrac{1 + \sqrt{3}\, i}{1 - \sqrt{3}\, i} \right)^{10}$.

Exercise 153 Let $z = x + iy \in \mathbb{C}$ and define

$$e^z := e^x (\cos y + i \sin y).$$

Show that (for $z, w \in \mathbb{C}$ and $n \in \mathbb{N}$) :

(a) $e^{z+w} = e^z \cdot e^w$.

(b) $e^{nz} = (e^z)^n$.

(c) $|e^z| = e^x$.

(d) $\overline{e^z} = e^{\bar{z}}$.

(e) $e^z = e^w \iff z = w + 2k\pi, \quad k \in \mathbb{Z}$.

Solve the equation

$$e^z = 1 + i.$$

Exercise 154 Evaluate

$$e^{-i}, \quad 2^i \quad \text{and} \quad \sqrt{i}.$$

Exercise 155 Show that :

(a) $\sin 5\theta = 5 \cos^4 \theta \sin \theta - 10 \cos^2 \theta \sin^3 \theta + \sin^5 \theta$.

(b) $\cos 5\theta = 16 \cos^5 \theta - 20 \cos^3 \theta + 5 \cos \theta$.

Exercise 156 Show that :

(a) $\sin^4 \theta = \frac{3}{8} - \frac{1}{2} \cos 2\theta + \frac{1}{8} \cos 4\theta$.

(b) $\cos^4 \theta = \frac{3}{8} + \frac{1}{2} \cos 2\theta + \frac{1}{8} \cos 4\theta$.

Exercise 157 Prove that

$$\sum_{k=0}^{n-1} \cos k\theta = \frac{\sin \frac{n\theta}{2} \cos \frac{(n-1)\theta}{2}}{\sin \frac{\theta}{2}} .$$

Determine the values of θ for which this is valid and sum the (finite) series for these values of θ.

Exercise 158 Evaluate the following sums :

$$C = \sum_{k=0}^{n-1} 2^k \cos k\theta \quad \text{and} \quad S = \sum_{k=0}^{n-1} 2^k \sin k\theta.$$

Exercise 159 Solve the following equations and then represent the roots as points in the complex plane.

(a) $5x^2 + 2x + 10 = 0$.

(b) $x^2 + (2i - 3)x + 5 - i = 0$.

(c) $x^5 = 1$.

(d) $x^2 = i$.

(e) $x^3 = -1 + i$.

(f) $x^6 + \sqrt{2}x^3 + 1 = 0$.

(g) $x^{10} + 6ix^5 - 12 = 0$.

(h) $x^5 - 2x^4 - x^3 + 6x - 4 = 0$.

Exercise 160 Consider a polynomial of degree n

$$p_n(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with complex coefficients, and let w_1, w_2, ..., w_n denote its roots. Show that :

(a) $w_1 + w_2 + \cdots + w_n = -a_{n-1}$.

(b) $w_1 \cdot w_2 \cdots w_n = (-1)^n a_0$.

Appendix A

Answers and Hints to Selected Exercises

Propositions and Predicates

1. FALSE. (The negation of an implication is *not* an implication.)

2. *FTT   FF*.

3. *TTT*.

4. (a) Always FALSE.

(b) Always TRUE.

(c) Always TRUE.

(d) Always TRUE.

(e) TRUE *only when* $\tau(p) = \tau(q) = 0$ or $\tau(p) = \tau(q) = 1$.

(f) FALSE *only when* $\tau(p) = 0$ and $\tau(q) = 1$.

(g) Always TRUE.

(h) Always TRUE.

(i) FALSE *only when* $\tau(p) = \tau(r) = 1$ and $\tau(q) = 0$.

(j) FALSE *only when* $\tau(p) = \tau(r) = 1$ and $\tau(q) = 0$.

5. Observe that $RHS = \tau(\neg(p \leftrightarrow q))$.

8. When $\tau(p) = \tau(r) = 0$, then $\tau((p \to q) \to r) = 0$ and $\tau(p \to (q \to r)) = 1$.

9. (a), (c), (k).

10. (c), (d).

13. (a) $\forall x\, F(x, Bob)$.

(b) $\forall y\, F(Kate, y)$.

(c) $\forall x\, \exists y\, F(x, y)$.

(d) $\neg\exists x\, \forall y\, F(x, y)$.

(e) $\forall y\, \exists x\, F(x, y)$.

(f) $\neg\exists x\, (F(x, Fred) \wedge F(x, Jerry))$.

(g) $\neg\exists x\, F(x, x)$.

14. $FTF \quad FTT \quad TFF$.

15. (a) $\exists x\, (x^2 + 2x - 3 \neq 0)$: TRUE.

(b) $\forall x\, (x^2 - 2x + 5 > 0)$: TRUE.

(c) $\exists x\, \forall r\, (xr \neq 1)$: TRUE.

(d) $\exists x\, \forall m\, (x^2 \geq m)$: FALSE.

(e) $\forall m\, \exists x\, (x^2 \geq m)$: TRUE.

(f) $\forall m\, \exists x\, \left(\frac{x}{|x|+1} \geq m \right)$: FALSE.

(g) $\exists x\, \exists y\, (x^2 + y^2 < xy)$: FALSE.

Sets and Numbers

16. $FTF \quad FTF \quad TFT$.

17. $LHS - RHS = \frac{1}{2}\left[(a-b)^2 + (b-c)^2 + (c-a)^2 \right]$.

18. (a) See EXAMPLE 2.1.5.

(b) $RHS - LHS = (a_1 b_2 - a_2 b_1)^2$.

(c) $RHS - LHS \geq 0$.

19. (a) $B \subseteq A$.

(b) $B \subseteq A$.

   (c) $A = B$.

   (d) $A \subseteq B$.

   (e) $A \cap B = \emptyset$.

   (f) $A = B = \emptyset$.

   (g) $A = B$.

20. (a) No.

   (b) No.

   (c) Yes.

21. (a) $\{1, 4\}$.

   (b) Use set identities.

   (c) $B = \emptyset$.

22. (a) TRUE.

   (b) FALSE. For example, if $A = \emptyset$ and $B = \{1\}$, then $|A \setminus B| = 0 \neq 0 - 1 = |A| - |B|$.

   (c) FALSE. For example, if $A = \{1, 2\}$ and $B = \{1, 3\}$, then $|A \cup B| = 3 \neq 2 + 2 = |A| + |B|$.

   (d) TRUE.

   (e) FALSE. Observe that $(5, 6) \notin A \times B \iff 5 \notin A$ or $6 \notin B$ and use the fact that $p \vee q$ does *not* imply $p \wedge q$. Counterexample : $A = B = \{5\}$.

   (f) TRUE (p *does* logically imply $p \vee q$).

   (g) TRUE.

   (h) TRUE.

23. Use set identities.

24. Use the definition of *divisibility*. (For instance, $a \mid b \iff b = ak \Rightarrow bc = a(ck) \iff a \mid bc$.)

25. (a) No.

   (b) Yes.

   (c) No.

(d) No.

26. (a) 2 and 5.

(b) -10 and 9.

(c) 77 and 0.

(d) 0 and 0.

(e) -1 and 4.

27. (a) $39 = 3 \cdot 13$.

(b) $81 = 3^4$.

(c) $101 = 101$ (prime number).

(d) $289 = 17^2$.

(e) $899 = 29 \cdot 31$.

28. (a) 6.

(b) 3.

(c) 11.

(d) 1.

29. (a) $1 = (-1) \cdot 10 + 1 \cdot 11$.

(b) $1 = 21 \cdot 21 + (-10) \cdot 44$.

(c) $12 = (-1) \cdot 36 + 1 \cdot 48$

(d) $1 = 13 \cdot 55 + (-21) \cdot 34$

(e) $3 = 11 \cdot 213 + (-20) \cdot 117$.

(f) $223 = 1 \cdot 0 + 1 \cdot 223$.

30. (a) FALSE. (The integers are *not* necessarily positive.)

(b) FALSE.

(c) TRUE. (One implication is immediate.)

Functions

32. (a) Injective but not surjective.

(b) Injective but not surjective.

(c) Surjective but not injective.

(d) Surjective but not injective.

(e) Neither injective nor surjective.

(f) Bijective : $k^{-1} = k$.

(g) Bijective.

(h) Neither injective nor surjective.

(i) Bijective : $n^{-1}(x) = \sqrt[4]{x}$.

(j) Bijective.

(k) Injective but not surjective.

(l) Bijective : $w^{-1} = w$.

33. (a) *Eight* functions : $f_1 = \{(1,4),(2,4),(3,4)\}$, $f_2 = \{(1,4),(2,4),(3,5)\}$, etc. None is one-to-one but *six* are onto.

(b) *Nine* functions. *Six* are one-to-one but none is onto.

(c) *Four* functions. *Two* are one-to-one and onto.

34. (a) $n \mapsto n + 1$.

(b) $0 \mapsto 0$, $n \mapsto n - 1$.

(c) $2k \mapsto 2k + 1$, $2k + 1 \mapsto 2k$.

(d) $2k \mapsto 2k + 1$, $2k + 1 \mapsto 2k + 1$.

35. (a) No. Counterexample : $f(x) = x$ and $g(x) = -x$.

(b) No. Counterexample : $f(x) = g(x) = x$.

(c) Yes. Prove that $(f \circ g)(x_1) = (f \circ g)(x_2) \Rightarrow x_1 = x_2$.

(d) No. Give a counterexample.

(e) No. Give a counterexample.

(f) Yes. Prove that $\forall z \in \mathbb{R}$, $\exists x \in \mathbb{R}$ such that $(f \circ g)(x) = z$.

36. $ad + b = bc + d$.

37. (a) $(1, 3, 5, 2, 4)$.

(b) $(1, 2, 4)(3, 6, 5)$.

(c) $(1, 2, 3, 4, 5, 6)$.

(d) $(1, 3, 5)(2, 4, 6)$.

(e) $(1, 6, 5, 4, 3, 2)$.

(f) $(1)(2)(3)(4)(5)$.

(g) $(1)(2, 3, 4, 5)$.

38. (a) $(1, 4, 7, 6, 9, 3, 2, 5, 8)$.

(b) $(1, 3, 6, 9, 8, 2, 5, 4, 7)$.

(c) $(1)(2, 4)(3, 5)(6, 8)(7, 9)$.

(d) $(1)(2, 5, 4, 3)(6, 9, 8, 7)$.

(e) $(1, 8, 6, 4, 2, 9, 7, 5, 3)$.

(f) $(1)(2)(3)(4)(5)(6)(7)(8)(9) = \iota$.

(g) $(1, 9)(2, 8)(3, 5)(4, 6)(7)$.

39. (a) $a = 3$, $b = 5$, $c = 4$, $d = 1$, $e = 2$.

(b) $(1, 5, 2)(3, 4) = (1, a, b)(3, c) \Rightarrow a = 5$, $b = 2$, $c = 4$.

40. (a) $(1)(2)(3) = \iota$, $(1, 2) = (1, 2)(3)$, $(1, 3) = (1, 3)(2)$, $(2, 3) = (1)(2, 3)$, $(1, 2, 3)$, $(1, 3, 2)$.

(b) $(1)(2)(3)(4) = \iota$, $(1, 2)$, $(1, 3)$, $(1, 4)$, $(2, 3)$, $(2, 4)$, $(3, 4)$, $(1, 2, 3)$, $(1, 3, 2)$, $(1, 2, 4)$, $(1, 4, 2)$, $(1, 3, 4)$, $(1, 4, 3)$, $(2, 3, 4)$, $(2, 4, 3)$, $(1, 2, 3, 4)$, $(1, 4, 3, 2)$, $(1, 3, 2, 4)$, $(1, 4, 2, 3)$, $(1, 2, 4, 3)$, $(1, 3, 4, 2)$, $(1, 2)(3, 4)$, $(1, 3)(2, 4)$, $(1, 4)(2, 3)$.

41. (a) FALSE. Give a counterexample.

(b) FALSE : $(i, j)(j, k) = (i, j, k) \neq (i, k, j) = (j, k)(i, j)$.

(c) FALSE. Give a counterexample.

(d) TRUE.

42. (a) Multiply both sides (from the right) by β^{-1}.

(b) $\alpha\beta = \alpha\gamma \Rightarrow (\alpha^{-1}\alpha)\beta = (\alpha^{-1}\alpha)\gamma \Rightarrow \beta = \gamma$.

43. • $(1, 3, 2)$.

• $(1, 4, 3, 2)$.

• $(1, 5, 4, 3, 2)$.

- $(1, n, n-1, \ldots, 3, 2)$.

44.
- $(2, 4)(2, 3)$.

- $(2, 8)(2, 6)(2, 4)$.

- $(1, 2)(3, 5)(3, 4)(6, 9)(6, 8)(6, 7)$.

- $(1, 5)(1, 6)(2, 9)(3, 4)(3, 8)$.

45. (a) Even.

(b) Odd.

(c) Odd.

(d) Odd.

Mathematical Induction

46. (a) $3\left(2^{11} - 1\right)$.

(b) $\frac{1}{2}\left(3^{11} + 1\right)$.

(c) $\frac{1}{2}\left(3^{11} - 2^{12} + 1\right)$.

(d) $3^{11} + 3 \cdot 2^{11} - 4$.

(e) 138.

47. (a) $500\ 497$.

(b) $9\ 150$.

(c) $\frac{k^2 - k - 2}{2}$.

(d) $2^{26} - 1$.

(e) $\frac{3}{2}\left(3^n - 1\right)$.

(f) $2\left(1 - \frac{1}{2^{n+1}}\right)$.

(g) $\frac{1}{3}\left(1 + (-1)^n \cdot 2^{n+1}\right)$.

48. (b) $\frac{n}{n+1}$.

(c) $\frac{1}{4} - \frac{1}{2(n+1)(n+2)}$.

(d) $1 - \frac{1}{(n+1)!}$.

56. (a)   i. $\sum_{k=1}^{n}(3k) = \frac{3n(n+1)}{2}$.

     ii. $\sum_{k=1}^{n}(2k - 1) = n^2$.

iii. $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$.

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

v. $\sum_{k=1}^{n} (3k + 1)(3k + 4) = 3n(n + 1)(n + 3) + 4n$.

Counting

61. (a) $9 + 9 \cdot 9 + 9 \cdot 9 \cdot 8 = 738$.

(b) $1\,999 - 199 = 1\,800$.

(c) $5 \cdot 9 \cdot 9 \cdot 9 \cdot 9 = 32\,805$.

62. (a) $36^4 = 1\,679\,616$.

(b) $P(36, 4) = 36 \cdot 35 \cdot 34 \cdot 33 = 1\,413\,720$.

63. (a) $7! = 5\,040$.

(b) $6! = 720$.

(c) $2 \cdot 6! = 1\,440$.

(d) $7! - 2 \cdot 5! = 4\,800$.

(e) $2 \cdot 5! = 240$.

(f) $6! = 720$.

(g) $5 \cdot 6! = 3\,600$.

(h) $7! - 2 \cdot 6! = 3\,600$.

64. (a) 60.

(b) 40.

(c) 14.

65. (a) $30!$.

(b) $\binom{30}{4}$.

(c) $\binom{10}{3}\binom{15}{7}$.

(d) $15! \cdot 5! \cdot 10!$.

66. (a) $8^5 = 32\,768$.

(b) $8^5 - (8)_5 = 26\,048$.

(c) $3^5 - \binom{3}{1}2^5 + \binom{3}{2}1^5 = 150$.

(d) $2^{10} = 1\,024$.

67. (a) $7^5 = 16\,807$.

(b) $9\,031$.

(c) $4\,380$.

(d) $P(7,5) = 2\,520$.

(e) $1\,800$.

(f) $2\,401$.

68. (a) $P(9,3) = 504$.

(b) $P(8,4) = 1\,680$.

69. (a) $\binom{12}{3} + \binom{12}{5} = 748$.

(b) $\binom{14}{5} - \binom{12}{3} = 1\,782$.

70. (a) $\binom{5}{3}\binom{7}{2} = 210$.

(b) $\binom{12}{5} - \binom{7}{5} = 771$.

(c) $\binom{5}{0}\binom{7}{5} + \binom{5}{1}\binom{7}{4} = 196$.

71. (a) $\binom{16}{9} = 11\,440$.

(b) $2^{16} - 1 = 65\,535$.

72. (a) $\binom{9}{2} = 36$.

(b) $36 - 8 = 28$.

(c) $\binom{9}{3} = 84$.

(d) $\binom{9}{3} - \binom{8}{2} = 56$.

73. (a) $32 - 80x + 80x^2 - 80x^3 + 10x^4 - x^5$.

(b) $64a^6 - 576a^5b + 2160a^4b^2 - 4320a^3b^3 + 4860a^2b^4 - 2916ab^5 + 729b^6$.

(c) $a^6 + 12a^5 + 60a^4 + 160a^3 + 240a^2 + 192a + 64$.

(d) $x^5 - 15x^3 + 90x - \frac{270}{x} + \frac{405}{x^3} - \frac{243}{x^5}$.

(e) $x^{14} + 7x^{11} + 21x^8 + 35x^5 + 35x^2 + \frac{21}{x} + \frac{7}{x^4} + \frac{1}{x^7}$.

74. (a) $\binom{12}{5} = 792$.

(b) $\binom{11}{5}2^5(-1)^6 = 14\,784$.

(c) 0.

(d) $-252a^5b^5$.

(e) 16.

(f) 405.

(g) $64y^6$.

Recursion

77. (a) $a_n = 5a_{n-1}, \quad a_0 = 1 \ (\text{or } a_1 = 5)$.

  (b) $b_n = b_{n-1} + n, \quad b_1 = 1$.

  (c) $c_n = -c_{n-1}, \quad c_0 = 1 \ (\text{or } c_1 = -1)$.

  (d) $\delta_n = \delta_{n-1}, \quad \delta_0 = \sqrt{2} \ (\delta_1 = \sqrt{2})$.

  (e) $e_n = e_{n-1} + (-1)^{n+1}, \quad e_0 = 0$.

  (f) $f_n = \frac{f_{n-1}}{1+f_{n-1}}, \quad f_1 = \frac{1}{2}$.

  (g) $g_n = g_{n-1} + 10^{-n}, \quad g_1 = 0.1 \,(= 10^{-1})$.

78. (a) $a_n = \frac{1}{n+1}$.

  (b) $b_n = 5 \cdot 2^{n-1} - 3$.

  (c) $c_n = n(n+2)$.

  (d) $d_n = \frac{1}{3}\left(2^{n+1} + (-1)^n\right)$.

  (e) $e_n = \frac{1}{4}\left(3^{n+1} - 2n - 3\right)$.

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

  (g) $g_n = 5n!$.

79. (a) $s_n = \left\lfloor \frac{n+1}{2} \right\rfloor = \begin{cases} k & \text{if } n = 2k \\ k+1 & \text{if } n = 2k+1. \end{cases}$

  (b) $t_n = 2^{F_n}$, where F_n is the nth term of the Fibonacci sequence.

80. We are letting P_n be the population (in billions) n years after 1995.

  (a) $P_n = 1.03 \cdot P_{n-1}, \quad P_0 = 7$.

  (b) $P_n = 7(1.03)^n$.

  (c) $P_{15} = 7(1.03)^{15} \approx 10.9$ billions.

81. (a) $s_n = s_{n-1} + s_{n-2} + s_{n-3} + 2^{n-3}$.

  (b) $s_0 = s_1 = s_2 = 0$.

  (c) $s_7 = 47$.

82. (a) $a_n = a_{n-1} + a_{n-2}$.

  (b) $a_0 = 1$, $a_1 = 1$.

  (c) $a_{10} = 89$.

83. (a) $a_n = \frac{1}{1.08} a_{n-1}$.

  (b) $a_{20} = \left(\frac{1}{1.08}\right)^{20} \approx 0.215$.

  (c) $a_{80} = \left(\frac{1}{1.08}\right)^{80} \approx 0.002$.

  (d) $\left(\frac{1}{1.1}\right)^{20} \approx 0.148$.

  (e) $\left(\frac{1}{1.1}\right)^{80} \approx 0.0004$.

84. (a) $a_n = -9 \cdot 2^{n-1} + 4 \cdot 3^{n-1} + n + 4$.

  (b) $b_n = -7 \cdot 2^{n+2} + 7n \cdot 2^{n+1} + n^2 + 8n + 20$.

  (c) $c_n = \frac{1 + (-1)^n}{2^{n+1}}$.

  (d) $d_n = 1 + (-1)^n + \frac{100}{99} \cdot 10^n$.

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

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

  (g) $f_n = (n^2 - n + 2) \cdot 2^{n-1}$.

  (h) $a_n = C \cdot (-3)^n + n^2 + n + \frac{2^{n+1}}{5}$.

85. (a) $y(n) = y(0)(1 + r)^n$.

  (b) $y(n) = y(0)\left(1 + \frac{i}{100}\right)^n$.

  (c) $y(50) = 117\,391$.

  (d) $y(50) = 184\,565$.

86. (a) $y(n) = \left(y(0) + \frac{d}{r}\right)(1 + r)^n - \frac{d}{r}$.

  (b) $y(50) = 1\,281\,299$.

  (c) $y(50) = 1\,853\,336$.

87. (a) The recurrence relation $y(n + 1) = (1 + r)y(n) + d(1 + i)^n$ yields
  $y(n) = y(0)(1 + r)^n + d\frac{(1+r)^n - (1+i)^n}{r-i}$ for $i \neq r$, and
  $y(n) = y(0)(1 + r)^n + nd(1 + r)^{n-1}$ for $i = r$.

(b) $y(50) = 19\,442\,723$.

88. (a) $y(n) = y(0)(1 + r)^n + \frac{d}{r}\left[1 - (1 + r)^n\right]$.

(b) $d = 1\,028.61$.

89. (b)   i. $d > p_0 r$.

   ii. $d = p_0 r$.

   iii. $d < p_0 r$.

90. (a) $s_n = \frac{d}{r}\left[1 - (1 - r)^n\right]$.

(c) $s_n \to \frac{d}{r} = 400$.

Linear Equations and Matrices

91. (a) $k = 10$.

(b) $k \neq 10$.

(c) Infinitely many values.

92. (a) $x_1 = 3$, $x_2 = -2$, $x_3 = 4$.

(b) $x_1 = 2\alpha - 3\beta + 4$, $x_2 = \alpha$, $x_3 = 3 - 4\beta$, $x_4 = \beta$

(c) $(3, -2, 4, -1)$.

93. (a) (i) none ; (ii) $k \neq 2$; (iii) $k = 2$.

(b) (i) $k \neq 4$; (ii) none ; (iii) $k = 4$.

(c) (i) every value : $k \in \mathbb{R}$; (ii) none ; (iii) none.

(d) (i) none ; (ii) $k \neq 11$; (iii) $k = 11$.

94. The system has *either* no solution (when $2a + 3b - c \neq 0$) *or* infinitely many solutions (when $2a + 3b - c = 0$).

95. $3a + b = c$.

97. (a) There are infinitely many choices (for example, $r = 1$, $s = 0$).

(b) $a = 3$, $b = 1$, $c = 8$, $d = -2$.

98. (a) TRUE.

(b) FALSE. (This *equality* is an *identity* if and only if $AB = BA$.)

(c) TRUE.

(d) FALSE.

(e) FALSE. (This *equality* is an *identity* if and only if $AB = BA$.)

(f) TRUE.

(g) FALSE. (This condition is equivalent to $AB = BA$.)

(h) TRUE.

(i) TRUE.

(j) TRUE.

99. (b) $\text{tr}\,(AB - BA) = 0 \neq 2 = \text{tr}\,(I_2)$.

100. (a) TRUE.

(b) FALSE. Give a counterexample.

102. $A^2 = \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix}$, $A^3 = \begin{bmatrix} 14 & 13 \\ 13 & 14 \end{bmatrix}$, $A^4 = \begin{bmatrix} 41 & 40 \\ 40 & 41 \end{bmatrix}$, $A^5 = \begin{bmatrix} 122 & 121 \\ 121 & 122 \end{bmatrix}$.

103. (a) There is no such matrix.

(b) $\begin{bmatrix} 0 & b \\ 1/b & 0 \end{bmatrix}$.

(c) $\begin{bmatrix} 0 & b \\ -1/b & 0 \end{bmatrix}$.

(d) $\begin{bmatrix} -2\alpha & -2\beta \\ \alpha & \beta \end{bmatrix}$.

(e) $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$.

(f) $\begin{bmatrix} \alpha & \beta \\ 0 & \alpha + \beta \end{bmatrix}$.

(g) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

104. (a) $A^{-1} = \begin{bmatrix} 3 & -2 \\ -4 & 3 \end{bmatrix}$, $x = \begin{bmatrix} 3 \\ -2 \end{bmatrix}$.

(b) $A^{-1} = \frac{1}{4}\begin{bmatrix} 7 & -9 \\ -5 & 7 \end{bmatrix}$, $x = \begin{bmatrix} 3/4 \\ 1/4 \end{bmatrix}$.

105. (a) $\begin{bmatrix} -5 & -2 & 5 \\ 2 & 1 & -2 \\ -4 & -3 & 5 \end{bmatrix}.$

(b) $\frac{1}{6}\begin{bmatrix} -21 & 11 & 8 \\ 9 & -5 & -2 \\ -3 & 3 & 0 \end{bmatrix}.$

(c) $\begin{bmatrix} 0 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & -3 & -2 & 1 \end{bmatrix}.$

Determinants

106. (a) Invertible.

(b) Not invertible.

(c) Invertible if and only if $abc \neq 0$.

(d) Not invertible.

(e) Invertible.

107. (a) $\lambda_1 = 1,\ \lambda_2 = 3.$

(b) $\lambda_1 = 3,\ \lambda_2 = 8.$

(c) $\lambda_1 = 1,\ \lambda_2 = 2,\ \lambda_3 = 3.$

(d) $\lambda_1 = -1,\ \lambda_2 = 0,\ \lambda_3 = 2.$

(e) $\lambda_1 = -4,\ \lambda_2 = 0,\ \lambda_3 = 2.$

108. (a) $\alpha \in \mathbb{R}.$

(b) $\alpha \in \mathbb{R} \setminus \{0,1\}.$

109. (a) 8.

(b) 60.

(c) 4.

(d) $-210.$

(e) 120.

(f) 60.

110. (a) 0.

(b) 25.

(c) 30.

(d) 40.

(e) 10.

111. Use properties of the determinants.

112. (a) -6.

(b) -37.

(c) -74.

(d) 39.

(e) 18.

(f) 98.

113. (a) $\det\left(A^T A\right) = 9$.

(b) The number $\det\left(A^T A\right)$ is positive.

115. All statements are TRUE.

116. (a) $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$.

(b) $\left(-\frac{3}{5}, -1, \frac{4}{5}\right)$.

(c) $\left(-\frac{1}{7}, \frac{9}{14}, \frac{2}{7}\right)$.

(d) $\left(\frac{9}{37}, -\frac{7}{37}, -\frac{8}{37}\right)$.

117. (a) $x = 5u - 8v$ and $y = 5v - 3u$.

(b) $x = u\cos\theta + v\sin\theta$ and $y = v\cos\theta - u\sin\theta$.

119. (a) $\frac{1}{10}\begin{bmatrix} 2 & 4 & 2 \\ -5 & 0 & -10 \\ -6 & -2 & -6 \end{bmatrix}$.

(b) $\frac{1}{35}\begin{bmatrix} -15 & 25 & -26 \\ 10 & -5 & 8 \\ 15 & -25 & 19 \end{bmatrix}$.

(c) $\frac{1}{37}\begin{bmatrix} -21 & -1 & -13 \\ 4 & 9 & 6 \\ -6 & 5 & -9 \end{bmatrix}$.

120. *FTT   TFT*.

Vectors, Lines, and Planes

121. (b) $(-5, 7)$.

(c) $(-1, -4)$.

122. $a = 3$, $b = -1$.

123. $\vec{u} + \vec{v} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $\vec{u} - \vec{v} = \begin{bmatrix} 1 \\ -3 \end{bmatrix}$, $3\vec{u} - 2\vec{v} = \begin{bmatrix} 3 \\ -7 \end{bmatrix}$, $\|-2\vec{u}\| = 2\sqrt{2}$, $\|\vec{u} + \vec{v}\| = \sqrt{2}$.

125. (a) $\theta = 135°$.

(b) $\theta = 180°$.

126. (a) $r = 2$.

(b) $k = \frac{8}{5}$.

128. (a) $\cos\theta = -\frac{13\sqrt{10}}{50} \approx -0.82219 \Rightarrow \theta \approx 145.3°$.

(b) $\cos\theta = -\frac{\sqrt{19}}{57} \approx -0.07647 \Rightarrow \theta \approx 94.4°$.

129. $(w_2 + w_3)\vec{i} - w_1\vec{j} - w_1\vec{k}$; $(w_1 + w_2 + w_3)(\vec{j} - \vec{k})$; $(w_1 + w_2 + w_3)(\vec{j} - \vec{k})$; $-2w_1 + w_2 + w_3$; $-2w_1 + w_2 + w_3$.

130. (a) $\begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}$.

(b) $\begin{bmatrix} -2 \\ 17 \\ 7 \end{bmatrix}$.

131. (a) $\angle A \approx 78.65°$, $\angle B \approx 64.29°$, $\angle C \approx 37.06°$.

(b) $\frac{\sqrt{478}}{2}$.

(c) $\frac{3\sqrt{10}}{2}$.

(d) $5\sqrt{6}$.

(e) 1.

133. $\vec{r} = \begin{bmatrix} 2 \\ 1 \\ 8 \end{bmatrix} + t \begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix}$; $\quad x = 2 + 2t,\ y = 1 + 3t,\ z = 8 + 4t$.

135. $x = 2t,\ y = 2 + 3t,\ z = -1 - 7t$.

136. $17x - 6y - 5z = 32$.

137. $x + y - z = 13$.

138. $6x + y + z = 23$.

139. $(-1, 2, -3)$.

140. $49x - 7y - 25z + 61 = 0$.

141. 3.

142. $(1, 1, 1)$.

143. $\vec{r} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}$.

144. $\vec{r} = t \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}$.

145. (a) 3.

Complex Numbers

146. $i,\ -i,\ -i$.

147. (a) $4 + 5i$.

(b) $-7 + 24i$.

(c) $-1 + i$.

(d) 1.

(e) 3.

      (f) 3.

148.   (a) 7, 7, 0, 7.

      (b) $2i$, 0, -2, 2.

      (c) $16 - 30i$, -16, 30, 34.

      (d) $-\frac{7}{41} - \frac{22}{41}i$, $-\frac{7}{41}$, $\frac{22}{41}$, $\frac{1}{41}\sqrt{533}$.

149. HINT : If $z = x+iy$, $z = u+iv \in \mathbb{C}$ then $\frac{z}{w} \in \mathbb{R} \iff z\bar{w} \in \mathbb{R} \iff xv = yu$.

152.   (a) $2(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}) = 2\,e^{i\frac{\pi}{3}}$.

      (b) $\sqrt{2}(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}) = \sqrt{2}\,e^{i\frac{5\pi}{4}}$.

      (c) $5\sqrt{2}(\cos\frac{4\pi}{4} + i\sin\frac{3\pi}{4}) = 5\sqrt{2}\,e^{i\frac{3\pi}{4}}$.

      (d) $\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = e^{i\frac{2\pi}{3}}$.

153. $z = \ln\sqrt{2} + i\left(\frac{\pi}{4} + 2k\pi\right)$, $k \in \mathbb{Z}$.

154. $\cos 1 - i\sin 1$, $\cos(\ln 2) + i\sin(\ln 2)$, $\pm\frac{1}{\sqrt{2}}(1 + i)$.

158. HINT : Evaluate $C + iS$. Use *de Morgan's formula* and **Exercise 191**.

159.   (a) $-\frac{1}{5} \pm i\frac{7}{5}$.

      (b) $2 - 3i$, $1 + i$.

      (c) 1, ω, ω^2, ω^3 and ω^4, where $\omega = e^{i\frac{3\pi}{5}}$.

      (d) $\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$, $-\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}$.

      (e) $2^{\frac{1}{6}}\,e^{i\frac{\pi}{4}}$, $2^{\frac{1}{6}}\,e^{i\frac{11\pi}{12}}$, $2^{\frac{1}{6}}\,e^{i\frac{19\pi}{12}}$.

      (f) $e^{i\frac{(8k\pm3)\pi}{12}}$, $k = 0, 1, 2$.

      (g) $12^{\frac{1}{10}}\,e^{i\frac{(6k-1)\pi}{15}}$ and $12^{\frac{1}{10}}\,e^{i\frac{(6k-2)\pi}{15}}$, $k = 0, 1, 2, 3$.

      (h) 1, 1, 2, $-1 \pm i$.

Appendix B

Revision Problems

1. Define the term *tautology*. Determine whether the following propositions are tautologies.

$$(1) \quad p \wedge (p \to q) \to q; \qquad (2) \quad (p \to q) \wedge q \to p.$$

2. Suppose that p and q are propositions so that $p \vee q \to p$ is FALSE. Find the *truth value* of the following propositions :

$$(1) \quad (p \to q) \to (q \to p); \qquad (2) \quad p \wedge (p \to q) \to q.$$

3. Write down the *truth table* for $p \to q$, and then determine whether the propositions
$$(p \to q) \to r \quad \text{and} \quad p \to (q \to r)$$
are *logicaly equivalent*.

4. Determine whether the propositions
$$(p \wedge q) \to r \quad \text{and} \quad (p \to r) \vee (q \to r)$$

are *logically equivalent.*

5. Define the logical operator $\rightarrow$ and then show that the propositions

$$(p \lor q) \rightarrow r \quad \text{and} \quad (p \rightarrow r) \land (q \rightarrow r)$$

are *logically equivalent*

   (a) using truth tables;

   (b) using logical equivalences.

6. Define the term *tautology*, and then determine whether the proposition

$$p \land q \rightarrow (p \rightarrow q)$$

is a tautology.

7. The proposition "p nor q", denoted by $p \downarrow q$, is the proposition that is TRUE when both p and q are FALSE, and is FALSE otherwise.

   (a) Construct the *truth table* for the logical operator $\downarrow$.

   (b) Show that
$$p \downarrow p \iff \neg p.$$

   (c) Show (by using a truth table or otherwise) that the propositions

$$(p \downarrow p) \downarrow (q \downarrow q) \quad \text{and} \quad p \land q$$

are *logically equivalent.*

8.

(a) Construct the *truth table* for the logical operator $\rightarrow$.

(b) Determine whether the propositions

$$p \wedge q \leftrightarrow q \quad \text{and} \quad q \rightarrow p$$

are *logically equivalent*.

Supp Exam, February 2005

9.

(a) Suppose the variable x represents people, and

$$F(x): x \text{ is friendly}, \quad T(x): x \text{ is tall}, \quad A(x): x \text{ is angry}.$$

Write each of the following statements using the above predicates and any needed quantifiers :

  i. Some people are not angry.
 ii. All tall people are friendly.
iii. No friendly people are angry.

(b) Write each of the following in good English. DO NOT use variables in your answers.

  (1) $A(Bill)$; (2) $\neg \exists x A(x) \wedge T(x)$; (3) $\neg \forall x F(x)$.

Class test, March 2000

10. Consider the predicates :

$$L(x,y); \ x < y, \quad Q(x,y): \ x = y, \quad E(x): \ x \text{ is even}, \quad G(x): \ x > 0,$$

$$\text{and} \quad I(x): \ x \text{ is an integer},$$

where the variables x and y represent real numbers. Write the following statements using the above predicates and any needed quantifiers :

(a) Every integer is even.

(b) If $x < y$, then x is not equal to y.

(c) There is no largest number.

(d) Some real numbers are not positive.

(e) No even integers are odd.

Exam, June 2000

11. Let $B(x)$, $G(x)$, $S(x)$, and $L(x, y)$ be the open sentences "x is a boy", "x is a girl", "x likes soccer", and "x likes y", respectively.

   (a) Use quantifiers and these predicates to express

      i. "Every boy likes some girl".
      ii. "All boys like all girls who like soccer".

   (b) In plain English negate the sentences (i) and (ii).

   (c) Use quantifiers and predicates to express the negated sentences. Simplify each expression so that no quantifier or implication remains negated.

12. Explain the terms *converse* and *contrapositive* of a conditional $p \to q$. Consider the proposition "Alice will win the game only if she plays by the rules."

   (a) Restate this proposition in good English in *three* different equivalent ways.

   (b) State the *converse* of this proposition.

   (c) State the *contrapositive* of this proposition.

   (d) Suppose that *Alice plays by the rules but loses*. Determine *with justification* whether the original proposition is TRUE or FALSE.

Supp Exam, February 2002

13. Consider the predicate

$$P(x, y) \; : \; x + 2y = xy$$

where the variables x and y represent real numbers. Determine *with justification* the truth values of the following propositions :

(a) $P(1, -1)$;

(b) $\forall x \exists y \, P(x, y)$;

(c) $\forall y \exists x \, P(x, y)$;

(d) $\exists x \exists y \, P(x, y)$;

(e) $\neg \forall x \exists y \, \neg P(x, y)$.

Class test, March 2004

14. Consider the predicate

$$P(x, y) \; : \; x^2 + 4y^2 = 4xy$$

where the variables x and y represent real numbers. Determine *with justification* the truth values of the propositions :

$$(1) \quad \forall x \exists y \, P(x, y) \quad \text{and} \quad (2) \quad \neg \exists y \forall y \, \neg P(x, y).$$

Exam, June 2004

15. Consider the predicate

$$T(x, y) \; : \; x \text{ is taking } y$$

where the variable x represents *students* and the variable y represents *courses*. Use quantifiers to express each of the following statements :

(a) No student is taking all courses.

(b) There is a course that no students are taking.

(c) Some students are taking no courses.

(d) Every student is being taken by at least one student.

<div align="right">**Class test, August 2004**</div>

16. Consider the predicate

$$A(x) : x \text{ is aggressive}, \quad S(x) : x \text{ is short}, \quad T(x) : x \text{ is talkative}$$

where the variable x represents *people*. Write the following statements using the above predicate and any needed quantifiers :

(a) Some short people are not talkative.

(b) All talkative people are aggressive.

(c) No aggressive people are short.

<div align="right">**Exam, November 2004**</div>

17. Investigate for *injectivity, surjectivity,* and *bijectivity* the function

$$f : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lfloor x + 2 \rfloor - \lfloor x \rfloor + \frac{x}{2}.$$

<div align="right">**Class test, March 1999**</div>

18. TRUE or FALSE ? Motivate your answers.

(a) If A, B are sets, then $A \setminus B = A \setminus (A \cap B)$.

(b) If A, B, C are sets and $A \cup C = B \cup C$, then $A = B$.

(c) The function $f : \mathbb{Z} \to \mathbb{Z}, \quad f(x) = 2\lfloor \frac{x}{2} \rfloor$ is one-to-one.

(d) The function $g : \mathbb{N} \to \mathbb{N}, \quad g(n) = n!$ is *not* onto.

<div align="right">**Exam, June 1999**</div>

19. Let $A = \{1, 2, 3, 4, 5\}$.

(a) Write *all* the subsets of A which contain the set $\{2, 5\}$.

(b) Write *all* the subsets B of A such that $B \cap \{2, 5\} = \{5\}$.

<div align="right">**Class test, May 2000**</div>

20. Prove that for any sets A and B

$$(A \cap B) \cup (A \cap B^c) = A.$$

<div align="right">**Class test, March 2001**</div>

21. Prove or disprove : If A, B, C are sets, then

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

<div align="right">**Class test, August 2004**</div>

22. Let $A = \mathbb{R} \setminus \{1\}$ and consider the function

$$f : A \to A, \qquad x \mapsto \frac{x+1}{x-1}.$$

(a) Determine $f(-2)$, $f(-1)$, $f(0)$, and $f\left(\frac{1}{3}\right)$.

(b) Investigate the function for *injectivity* and *surjectivity*.

(c) If the function is bijective, find its *inverse*.

(d) Find $f \circ f$ and $f \circ f \circ f$.

<div align="right">**Class test, March 2001**</div>

23. TRUE or FALSE ? Motivate your answers.

(a) If A, B are sets, then $A \setminus (A \setminus B) = A \cap B$.

(b) If A, B are finite sets, then $|A \cup B| = |A| + |B|$.

(c) If A is a finite set, then any function $f : A \to A$ that is one-to-one is also onto.

(d) The function $g : \mathbb{N} \to \mathbb{N}, \quad n \mapsto 2n + 1$ is one-to-one but *not* onto.

<div align="right">**Class test, March 2000**</div>

24. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} x^2 & \text{if } x \geq 0 \\ 2x & \text{if } x < 0. \end{cases}$$

Sketch the graph of f and then investigate the function for *injectivity* and *surjectivity*. If the function is invertible, find its *inverse*.

Class test, March 2000

25. Let $A = \{1, 2, 3, 4\}$ and $B = \{\alpha, \beta\}$.

   (a) Give an example of a function $f : A \to B$ that is a surjection but *not* an injection, and then explain why it meets these conditions.

   (b) State the *domain, codomain,* and *range* of the function you gave in part (a). Is your function *invertible* ?

   (c) Construct two different invertible functions from the set A onto the set (Cartesian product) $B \times B$. How many such functions are there ?

Class test, March 2003

26. TRUE or FALSE ? Justify your answers.

   (a) The number 0 is an element of $\emptyset$.

   (b) $\emptyset = \{\emptyset\}$.

   (c) $\emptyset \in \{\emptyset\}$.

   (d) If A, B, C are sets and $A \setminus C = B \setminus C$, then $A = B$.

   (e) For all sets A and B, if $A \cap B = \emptyset$ then $A \times B = \emptyset$.

   (f) If $f : A \to B$ and $g : B \to C$ are one-to-one, then $g \circ f : A \to C$ is also one-to-one.

   (g) $\{a, b\} = \{b, a\}$.

   (h) $\{a\} \subseteq \{\{a\}\}$.

(i) The power set of $\{\emptyset\}$ is $\{\{\emptyset\}\}$.

(j) The function $g : \{a, b, c\} \to \{1, 2, 3\}, \quad a \mapsto 2, b \mapsto 1, c \mapsto 3$ is *invertible*.

(k) There exists a function $f : \{1, 2, 3\} \to \{N, O, P, E\}$ which is *onto*.

(l) If $A, B, C \in 2^X$, then

$$A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C).$$

27. TRUE or FALSE ? Justify your answers.

(a) $\emptyset \in \{\emptyset\}$ and $\emptyset \subseteq \{\emptyset\}$.

(b) For A, B, C sets, $A \setminus (B \cap B) = (A \setminus B) \cup (A \setminus C)$.

(c) For A, B sets, if $A \setminus B = \emptyset$, then $A = B$.

(d) The function $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}, \quad f(x) = \dfrac{x - 1}{x}$ is *invertible*.

(e) If $f : A \to B$ and $g : B \to C$ are both one-to-one functions, then the composite function $g \circ f : A \to C$ is also one-to-one.

Class test, March 2004

28. TRUE or FALSE ? Justify your answers.

(a) $\emptyset \in \{\emptyset\}$.

(b) For A, B sets, if $A \cup B = A \cap B$, then $A = B$.

(c) The function $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto (x - 1)^3$ is one-to-one but *not* onto.

Exam, June 2004

29. Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}$. Recall the definitions of *the floor function* and *the ceiling function*, and then show that

(a) $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ (or, equivalently, $0 \leq x - \lfloor x \rfloor < 1$).

(b) $\lceil x \rceil - 1 < x \leq \lceil x \rceil$ (or, equivalently, $0 \leq \lceil x \rceil - x < 1$).

(c) $\lceil x \rceil + \lfloor -x \rfloor = 0$.

(d) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$.

(e) $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

30. Consider the function

$$f : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lfloor 1 - x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq 1 - x\}.$$

(a) Determine $f(-1)$, $f(0)$, $f\left(\frac{1}{2}\right)$, and $f(1)$.

(b) Sketch the *graph* of f.

(c) Explain what is meant by saying that a function is *injective* (or one-to-one), *surjective* (or onto). Hence determine *with justification* whether function f is injective or/and surjective.

Class test, August 2004

31. Let $a, b, c, d \in \mathbb{R}$. Prove that

(a) $a^2 + b^2 \geq 2ab$ with equality if and only if $a = b$.

(b) If $a + b + c \geq 0$, then

$$a^3 + b^3 + c^3 \geq 3abc$$

with equality if and only if $a = b = c$ or $a + b + c = 0$.

(c) If $a, b, c, d \geq 0$, then

$$a^4 + b^4 + c^4 + d^4 \geq 4abcd$$

with equality if and only if $a = b = c = d$.

[Hint : (b) Expand the product

$$(a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca).$$

(c) Write

$$\frac{a^4 + b^4 + c^4 + d^4}{4} = \frac{\frac{a^4 + b^4}{2} + \frac{c^4 + d^4}{2}}{2}. \ ]$$

32. Let $a, b, c, a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{R}$. Prove that :

    (a) (**Mean inequalities**)   If $0 < a \le b \le c$, then

    $$a \le \frac{3}{\frac{1}{a} + \frac{1}{b} + \frac{1}{c}} \le \sqrt[3]{abc} \le \frac{a + b + c}{3} \le \sqrt{\frac{a^2 + b^2 + c^2}{3}} \le c$$

    with equality if and only if $a = b = c$.

    (b) (**Cauchy-Schwarz inequality**)

    $$(a_1 b_1 + a_2 b_2 + a_3 b_3)^2 \le (a_1^2 + a_2^2 + a_3^2)(b_1^2 + b_2^2 + b_3^2)$$

    with equality if and only if $a_1 = r b_1$, $a_2 = r b_2$ and $a_3 = r b_3$ ($r \in \mathbb{R}$).

    (c) (**Chebyshev inequality**)   If $a_1 \le a_2 \le a_3$ and $b_1 \le b_2 \le b_3$, then

    $$(a_1 + a_2 + a_3)(b_1 + b_2 + b_3) \le 3(a_1 b_1 + a_2 b_2 + a_3 b_3)$$

    with equality if and only if $a_1 = a_2 = a_3$ and $b_1 = b_2 = b_3$.

33. Let $x, y \in \mathbb{R}$. Recall the definition of *the absolute value function* and then show that

    (a) $|x| \ge 0$; $|x| = 0 \iff x = 0$.

    (b) $|xy| = |x||y|$.

    (c) $|x + y| \le |x| + |y|$.

    (d) $\big| |x| - |y| \big| \le |x - y|$.

34. Let $a, b, c \in \mathbb{R}$ such that $1 \le a$ and $b \le c$. Prove that

    $$(1 + a)(b + c) \le 2(b + ac)$$

    with equality if and only if $a = 1$ or $b = c$.

Class test, March 2004

35. Let $\alpha, \beta \in S_5$ be given by

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{bmatrix} \quad \text{and} \quad \beta = (1, 2, 4)(3, 5).$$

  (a) Write the permutation α in *cycle form*.

  (b) Calculate

$$\alpha\beta, \quad \beta\alpha, \quad \alpha^2, \quad \beta^{-1}, \quad \text{and} \quad \beta^{-1}\alpha^{-1}.$$

  (c) Determine the *signature* of

$$\alpha, \quad \alpha^2, \quad \text{and} \quad (\alpha\beta)^{-1}.$$

Class test, May 2001

36. Write all permutations on three elements in *cycle form*, and then find *all* permutations $\alpha \in S_3$ such that $\alpha^2 = (1, 2, 3)$.

Class test, May 2001

37. Define the term *permutation on n elements* and then explain what is meant by the *cycle notation*. Consider the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{bmatrix}$.

  (a) Write α, α^2, and α^{-1} in cycle form.

  (b) Determine the permutation σ so that $\alpha\sigma = \alpha^{-1}$.

Class test, March 2003

38.

  (a) Define the term *permutation on n elements* and then explain what is meant by the *cycle notation*.

  (b) Consider the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{bmatrix}$.

    i. Write α, α^2, and α^{-1} in cycle form.

ii. Determine the permutation π so that $\alpha\pi = \alpha^{-1}$.

Class test, March 2004

39. Consider the permutations (on five elements)

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{bmatrix}.$$

Write each of the permutations

$$\alpha, \beta, \alpha\beta, \alpha^2, \quad \text{and} \quad \beta^{-1}$$

in *cycle form*.

Exam, June 2004

40. Calculate the sum

$$S_n = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)}$$

for $n = 1, 2, 3, 4,$ and 5. Guess a general formula for S_n, and then prove by *mathematical induction* this formula.

Class test, March 1999

41. Calculate the sum

$$S_n = \frac{2}{3} + \frac{2}{3^2} + \frac{2}{3^3} + \cdots + \frac{2}{3^n}$$

for $n = 1, 2, 3,$ and 4. Guess a general formula for S_n, and then prove this formula by *mathematical induction*.

Exam, June 1999

42. For which natural numbers n is $n! > 2^n$? Prove your answer using *mathematical induction*.

Class test, March 2000

43. Calculate the sum

$$S_n = \frac{1}{n^2} + \frac{3}{n^2} + \frac{5}{n^2} + \cdots + \frac{2n-1}{n^2}$$

for $n = 1, 2, 3,$ and 4. Guess a general formula for S_n, and then prove this formula by mathematical induction.

Exam, June 2000

44.

(a) Write the sum

$$S = \frac{1}{3} - \frac{2}{5} + \frac{3}{7} - \frac{4}{9} \cdots + \frac{99}{199}$$

in *sigma notation*; that is in the form $\displaystyle\sum_{i=i_0}^{N} a_i$.

(b) Find

$$T = \sum_{i=1}^{199} (2i + 1).$$

Class test, May 2001

45. Use *mathematical induction* to prove that

$$n(n+1)(n+2) \quad \text{is divisible by } 6$$

for every positive integer n.

Class test, May 2001

46. Calculate the sum

$$S_n = \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1) \cdot (2n+1)}$$

for $n = 1, 2, 3, 4$ and 5. Guess a general formula for S_n, and then prove this formula by mathematical induction.

Class test, May 2001

47. Prove by *mathematical induction* that

$$5^n - 1 \vdots 4$$

for any natural number n.

Class test, March 2003

48. Prove by *mathematical induction* that

$$3^{2n-1} + 4^{2n-1} \vdots 7$$

for any positive integer number n.

49. Consider the sum

$$S_n = 4 \cdot 7 + 7 \cdot 10 + 10 \cdot 13 + 13 \cdot 16 + \cdots \quad \text{to } n \text{ terms.}$$

(a) What is the nth term of S_n ?

(b) Calculate the sum.

(c) Use *mathematical induction* to verify your result.

Class test, March 2003

50. Prove by *mathematical induction* that

$$1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} = 2\left(1 - \frac{1}{2^{n+1}}\right)$$

for all natural numbers n.

Exam, June 2003

51. Let $a, b \in \mathbb{R}$.

(a) Prove that
$$\frac{a+b}{2} \leq \sqrt{\frac{a^2 + b^2}{2}}$$
with equality if and only if $a = b$.

(b) Use *mathematical induction* to prove that

$$\left(\frac{a+b}{2}\right)^n \le \frac{a^n + b^n}{2}$$

for all natural numbers n.

Exam, June 2003

52.

(a) Explain the notation $n!$ (read : "n factorial"), and then compare the numbers 3^6 and $6!$.

(b) Prove by *mathematical induction* that

$$3^n < n! \quad \text{for all integers } n \ge 7.$$

Class test, May 2004

53. Explain the notation $a \vdots b$ (read : "a is divisible by b"), and then prove by *mathematical induction* that

$$n^3 - n \vdots 6 \quad \text{for all integers } n \ge 1.$$

Exam, June 2004

54. Consider the sum

$$S_n = 3 \cdot 5 + 5 \cdot 7 + 7 \cdot 9 + 9 \cdot 11 + \cdots \quad \text{to } n \text{ terms.}$$

(a) What is the nth term of S_n ?

(b) Calculate the sum. (HINT : You may use the sums $\displaystyle\sum_{k=1}^{n} k$ and $\displaystyle\sum_{k=1}^{n} k^2$.)

(c) Use *mathematical induction* to verify your result.

Class test, May 2004

55.

(a) Explain the notation $\displaystyle\sum_{i=p}^{q} a_i$, and then calculate (the sum)

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

(HINT: You may use the formula $\displaystyle\sum_{i=1}^{n} i = \frac{n(n + 1)}{2}$.)

(b) Use *mathematical induction* to verify your result.

Exam, June 2004

56. Consider the sum

$$S_n = 4 + 7 + 10 + 13 + \cdots \quad \text{to } n \text{ terms.}$$

(a) What is the nth term of S_n ?

(b) Calculate the sum. (HINT : You may use the sum $\displaystyle\sum_{i=1}^{n} i$.)

(c) Use *mathematical induction* to verify your result.

Class test, October 2004

57. Prove by *mathematical induction* that

$$3^{2n+1} + 4^{2n+1} \quad \text{is divisible by } 7$$

for all natural numbers n.

Class test, October 2004

58. Consider the sum

$$S_n = \sum_{k=1}^{n}(3k + 2).$$

(a) Calculate the sum. (HINT : You may use the formula $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.)

(b) Use *mathematical induction* to verify your result.

Exam, November 2004

59. Using only the digits $1, 2, 3, 4, 5, 6,$ and $7,$ how many five-digit numbers can be formed that satisfy the following conditions ?

(a) no additional conditions ;

(b) at least one 7 ;

(c) no repeated digits ;

(d) at least one 1 and at least one 7.

Class test, May 1999

60. How many solutions are there to the equation

$$x + y + z = 100$$

if x, y, z are natural numbers ?

Class test, May 1999

61. Consider a group of 12 people consisting of 7 men and 5 women. How many 5-person teams can be chosen

(a) that contain 3 men and 2 women ?

(b) that contain at least one man ?

(c) that contain at most one man ?

(d) if a certain pair of people insist on been selected together or not at all ?

(e) if a certain pair of people refuse to be selected together ?

62. How many positive integers not exceeding $1\,000$ are *not* divisible by either 8 or 12 ?

63.

   (a) How many functions are there from a set with 3 elements to a set with 8 elements ?

   (b) How many one-to-one functions are there from a set with 3 elements to a set with 8 elements ?

   (c) How many onto functions are there from a set with 3 elements to a set with 8 elements ?

   (d) What is the coefficient of $x^3 y^8$ in $(x + y)^{11}$ and $(2x + 3y)^{11}$?

64. How many ways are there to assign six jobs to four employees so that every employee is assigned at least one job ?

65.

   (a) Evaluate $\binom{4}{2}$ by listing all *sets* of size 2 whose elements belong to the set $\{a, b, c, d\}$.

   (b) Evaluate $\left(\binom{2}{4}\right)$ by listing all *multisets* of size 4 whose elements belong to the set $\{0, 1\}$.

   (c) List all 2-*permutations with repetition* of the set $\{0, 1, a, b\}$.

66. Determine the number of bit strings of length 10 that have

   (a) exactly three 0s.

(b) the same number of 0s and 1s.

(c) at least seven 1s.

67.

(a) Consider the set $S = \{0, 1, a, b\}$. List *all*

- 2-permutations
- 3-combinations
- 2-permutations with repetition
- 3-combinations with repetition.

of the set S.

(b) A person giving a party wants to set out 10 assorted cans of soft drink for his guests. He shops at a store that sells 5 different types of soft drinks. Use *multisets* to count how many selections of 10 soft drinks he can make.

68. Explain what is meant by a *bit string*, and then determine the number of bit strings of length eight that

(a) have exactly three 0s;

(b) start and end with an 1;

(c) have at least six 1s.

69.

(a) How many integers from 1 to 1 000 are *divisible* by 3 ?

(b) How many integers from 1 to 1 000 are *divisible* by 3 *and* 7 ?

(c) How many integers from 1 to $1\,000$ are *divisible* by 3 *or* 7 ?

(d) How many three-digit integers (i.e. integers from 100 through 999) are *divisible* by 6 *and* 9 ?

Class test, October 2004

70. How many different committees of *four* can be selected from a group of *twelve* people if

(a) a certain pair of people insist on serving together or not at all ?

(b) a certain pair of people refuse to serve together ?

Class test, October 2004

71. How many different committees of *six* can be selected from a group of *four* men and *four* women

(a) that consist of three men and three women ?

(b) that consist of *at least* one woman ?

(c) that consist of *at most* one man ?

Supp Exam, February 2005

72. Find :

(a) the coefficient of $x^5 y^6$ in the expansion of $(2x - y)^{11}$.

(b) the middle term in the expansion of $(1 - a)^{14}$.

(c) the largest coefficient in the expansion of $(x + 2)^7$.

(d) $\binom{20}{1} + \binom{20}{2} + \binom{20}{3} + \cdots + \binom{20}{19}$.

Class test, May 1999

73. TRUE or FALSE ?

(a) The coefficient of $x^2 y^9$ in the expansion of $(x + y)^{11}$ is 55.

(b) The *middle term* in the expansion of $\left(a - \frac{1}{a}\right)^{12}$ is -264.

(c) The largest coefficient in the expansion of $\left(x + \frac{1}{x}\right)^{7}$ is 35.

<div align="right">**Exam, June 2001**</div>

74. Write down the *binomial formula*, and then use this formula to

    (a) expand $(x - y)^5$;

    (b) find the *middle term* in the expansion of $(2 - a)^{10}$;

    (c) calculate the sum
    $$\binom{50}{0} + \binom{50}{1} + \binom{50}{2} + \cdots + \binom{50}{50}.$$

<div align="right">**Exam, June 2004**</div>

75. Describe the sequence $(a_n)_{n \geq 0}$: $0, 1, 0, 1, 0, 1, \ldots$ recursively (include initial conditions) and then find an explicit formula for the sequence.

<div align="right">**Class test, May 1999**</div>

76. Consider the sequence (of decimal fractions)
    $$a_1 = 0.1, \quad a_2 = 0.11, \quad a_3 = 0.111, \quad a_4 = 0.1111, \quad \ldots$$

    (a) Observe that
    $$a_1 = \frac{1}{10}; \quad a_2 = \frac{1}{10} + \frac{1}{100}; \quad a_3 = \frac{1}{10} + \frac{1}{100} + \frac{1}{1000}.$$
    Hence express a_n as a sum (of n terms).

    (b) Show that
    $$a_n = \frac{1}{9}\left(1 - \frac{1}{10^n}\right).$$

    (c) Describe the sequence $(a_n)_{n \geq 1}$ *recursively*. (Include initial conditions.)

<div align="right">**Class test, October 2004**</div>

77. Describe the sequence

$$1, \ 11, \ 111, \ 1111, \ 11111, \ \cdots$$

recursively. (Include initial conditions.)

78. Solve the following *recurrence relation* :

$$a_n = a_{n-2} + n; \quad a_0 = 1, \ a_1 = 2.$$

79. Let d_n denote the number of people infected by a disease and suppose that *the change in the number infected in any period is proportional to the change in the number infected in the previous period.* Show that there exists some constant k such that

$$d_{n+2} - d_{n+1} = k(d_{n+1} - d_n).$$

Obtain an expression for d_n (in terms of d_0 and d_1) for $k = 2$.

80.

   (a) Find a *recurrence relation* of the number of ways to climb n stairs if stairs can be climbed two or three at a time.

   (b) What are the initial conditions ?

   (c) How many ways are there to climb eight stairs ?

81. Find the solution of the *recurrence relation*

$$a_n = \frac{1}{2}a_{n-2}; \quad a_0 = a_1 = 1$$

and then determine a_{20}.

82. Solve the *recurrence relation* :

$$a_n = a_{n-2} + n; \quad a_0 = 1, a_1 = \frac{7}{4}.$$

Exam, June 2000

83. Solve the following *recurrence relation* :

$$F_n = F_{n-1} + F_{n-2}; \quad F_0 = 1, F_1 = 0.$$

Exam, June 2001

84.

   (a) Find a *recurrence relation* for the number of bit strings of length
       n that contain three consecutive 0s.

   (b) What are the initial conditions ?

   (c) How many bit strings of length seven contain three consecutive 0 ?

Exam, June 2001

85. Solve the following *recurrence relation* :

$$a_n = 2a_{n-1} - a_{n-2} + 2^n; \quad a_0 = 4, a_1 = 9.$$

86.

   (a) Find a *recurrence relation* for the number of bit strings of length
       n that do *not* contain the pattern 11.

   (b) What are the initial conditions ?

   (c) How many bit strings of length eight do not contain the pattern 11
       ?

Exam, June 2003

87. Let R_n denote the maximum number of regions into which n straight lines can cut a plane.

    (a) Find the values of R_0, R_1, R_2, and R_3.

    (b) Show that R_n satisfies the *recurrence relation*

    $$R_n = R_{n-1} + n.$$

    Give reasons for your answer.

    (c) Solve this recurrence relation.

88. Solve the *recurrence relation*

    $$a_n = -2a_{n-1} - a_{n-2} + n; \quad a_0 = \frac{1}{4} \text{ and } a_1 = \frac{1}{2}.$$

    (HINT : Try a particular solution of the form $An + B$.)

    Exam, June 2004

89. Solve the *recurrence relation*

    $$a_n = a_{n-1} + 10^{-n}, \quad a_1 = 10^{-1}.$$

    (HINT : Try for a particular solution of the form $K \cdot 10^{-n}$.)

    Class test, October 2004

90. Use *Gaussian elimination* to solve the linear system :

    $$\begin{aligned} x - 2y + 3z &= 7 \\ 2x - 3y - z &= 6 \\ x - 3y + 10z &= 15 \end{aligned}$$

    and then give a geometric interpretation.

    Exam, June 1999

91. Use *Gaussian elimination* to solve the linear system :

$$x + 5y = 12$$
$$3x - 7y = 14$$
$$2x - 4y = 10$$

and then give a geometric interpretation.

Exam, June 2000

92. Use *Gaussian elimination* to solve the following linear system :

$$2x + 2y + z = 3$$
$$x + y + 3z = -1$$
$$3x + 3y + 4z = 2.$$

Exam, November 2001

93. Explain what is meant by *linear system* and then use *Gaussian elimination* to solve the linear system :

$$3x + y + z = 0$$
$$x - 2y + 3z = 7$$
$$2x + y - z = -1$$
$$-x - 4y + 5z = 11.$$

Class test, May 2003

94. Use *Gaussian elimination* to solve the following linear system :

$$x + y + z = 2$$
$$2x + 3y + z = -1$$
$$3x + y + 2z = 7$$
$$x - 2y + z = 8.$$

Exam, June 2003

95. Use *Gaussian elimination* to solve the linear system

$$
\begin{aligned}
2x - y + 3z &= 0 \\
x + 4y - z &= 1 \\
x + 13y - 6z &= 3.
\end{aligned}
$$

Class test, May 2004

96. Consider the linear system

$$
\begin{aligned}
x - 2y + 3z &= 0 \\
3x + y - z &= 1 \\
x + 5y - 7z &= k.
\end{aligned}
$$

Determine for what values of the parameter $k \in \mathbb{R}$ the given system is *consistent*. If so, solve the system (by using *Gaussian elimination*).

Exam, June 2004

97. Consider the linear system

$$
\begin{aligned}
x - y + 4z &= -2 \\
2x - y - 5z &= 0 \\
x - 2y + 7z &= k.
\end{aligned}
$$

(a) Determine for what values of the parameter $k \in \mathbb{R}$ the given system has *at least* one solution.

(b) Solve the system for those values of k determined in (a).

Supp Exam, February 2005

98. Find the inverse of the following matrix :

$$
A = \begin{bmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix}.
$$

Use A^{-1} to solve the equation $Ax = \begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix}$.

Exam, June 1999

99. Evaluate the determinant

$$\begin{vmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \\ 2 & 3 & 0 & 1 \\ 1 & 2 & 3 & 0 \end{vmatrix}.$$

Exam, June 1999

100. Consider the matrix

$$A(x) = \begin{bmatrix} 0 & 1 & x \\ 1 & x & x \\ x & x & x \end{bmatrix}.$$

   (a) Find all values of $x \in \mathbb{R}$ such that $A(x)$ is *invertible*.

   (b) Compute the *inverse* of the matrix $A(2)$.

Class test, May 2000

101. Given the matrix $B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{bmatrix}$, find all matrices A such that

$$BA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

   How many solutions A does this problem have ?

Exam, June 2000

102. Find $\lambda \in \mathbb{R}$ such that the matrix

$$A = \lambda \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

is *not* invertible (i.e. $\det(A) = 0$).

<div align="right">**Exam, June 2000**</div>

103. Let

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{bmatrix}.$$

(a) Find the *inverse* A^{-1}.

(b) Show that your answer in (a) is correct without repeating the same calculation.

(c) Use A^{-1} to solve the linear system :

$$\begin{aligned} x + 2y + 3z &= 0 \\ 4y + 5z &= -3 \\ 6z &= 6. \end{aligned}$$

<div align="right">**Class test, August 2001**</div>

104. Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix} \quad \text{and} \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Find all values $\lambda \in \mathbb{R}$ such that the matrix $A - \lambda I_3$ is *not* invertible.

<div align="right">**Class test, August 2001**</div>

105. Evaluate the determinant :

$$\begin{vmatrix} 0 & -1 & 7 & 8 \\ 1 & 0 & -1 & 9 \\ 2 & 3 & 0 & -1 \\ 4 & 5 & 6 & 0 \end{vmatrix}.$$

<div align="right">**Class test, August 2001**</div>

106. Consider the matrices

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & -4 & -4 \end{bmatrix} \quad \text{and} \quad E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

   (a) Calculate A^2, $2E - A$, $\det(A)$, and $\det(2E - A)$.

   (b) Is matrix A *invertible* ? Explain.

   (c) Is matrix $2E - A$ *invertible* ? Explain.

   (d) Find the *inverse* matrix $(2E - A)^{-1}$.

Exam, November 2001

107. Give the definition of the *determinant* of an $n \times n$ matrix and then evaluate the determinants

$$\begin{vmatrix} a & b & c \\ b & c & a \\ c & a & b \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{vmatrix}.$$

Class test, May 2003

108. Consider the matrices

$$A = \begin{bmatrix} 0 & 1 & 6 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}, \quad \text{and} \quad C = \begin{bmatrix} 1 & 1 & 2 \end{bmatrix}.$$

   (a) Compute the matrices A^2, A^3, CB, and $A + BC$.

   (b) Find the *inverse* $(A + BC)^{-1}$.

   (c) Show that your answer in (b) is correct without repeating the same calculation.

(d) Let
$$E(t) := I + tA + \frac{t^2}{2}A^2 \qquad (t \in \mathbb{R})$$
where I is the identity matrix. Determine (by direct computation) whether the following equality holds for every $t, s \in \mathbb{R}$
$$E(t + s) = E(t)E(s).$$

Class test, May 2003

109. Show (by direct computation) that
$$\begin{vmatrix} x & y & z & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{vmatrix} = x + y + z + 1.$$
Give a geometric interpretation.

Exam, June 2003

110. Consider the matrices
$$A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad \text{and} \quad C = \begin{bmatrix} -17 & -1 \end{bmatrix}.$$

(a) Find $A^2, A + BC$, and CB.

(b) Explain the notation A^T (read : "A transpose"), and then compute the matrix $AA^T - A^T A$.

(c) Is matrix A *invertible* ? If so, find its inverse A^{-1}.

Class test, May 2004

111. Use *Gaussian elimination* and *Laplace expansion* to evaluate – in two different ways – the determinant
$$\begin{vmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 2 & 4 & 0 & -1 \\ 3 & 5 & 6 & 0 \end{vmatrix}.$$

112. Explain what is meant by saying that two (square) matrices *commute*, and then find all 2×2 matrices X which commute with $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$.

113. Use *Gaussian elimination* and *Laplace expansion* to evaluate – in two different ways – the determinant

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 2 & 0 & 5 & 0 \\ 3 & 7 & 8 & 9 \\ 4 & 0 & 10 & 6 \end{vmatrix}.$$

114.

(a) Find the *inverse* of the matrix

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & 2 \\ 3 & 0 & 1 \end{bmatrix}.$$

(b) Use the matrix A^{-1} to solve (for X) the equation

$$AX = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}.$$

(The unknown X is a 3×1 matrix.)

(c) Use *Cramer's rule* to solve the linear system

$$\begin{aligned} x + 2y &= 3 \\ 3y + 2z &= 1 \\ 3x + z &= 2. \end{aligned}$$

115. Consider the matrices

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

   (a) Calculate

$$I + A^2, \quad (I + A)^2, \quad I + A^{-1} \quad \text{and} \quad (I + A)^{-1}.$$

   (b) Determine the *inverse* of the matrix

$$\begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

116. Consider the matrices

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

   Calculate

   (a) $A^{-1} + B^{-1}$.

   (b) $(A + B)^{-1}$.

   (c) $AB + BA$.

   (d) $A^2 + B^2$.

   (e) $(A + B)^2$.

117. Calculate the determinant

$$\begin{vmatrix} 0 & -1 & 2 & 3 \\ 1 & 0 & -4 & 0 \\ -2 & 4 & 0 & -5 \\ -3 & 0 & 5 & 0 \end{vmatrix}.$$

Class test, November 2004

118. Evaluate the determinant

$$\begin{vmatrix} 0 & -1 & \alpha & 2 \\ 1 & 0 & -1 & 0 \\ -\alpha & 1 & 0 & -1 \\ -2 & 0 & 1 & 0 \end{vmatrix}.$$

Supp Exam, February 2005

119. Let $a, b \in \mathbb{R}$ such that $a + b \neq 0$. Use *Cramer's rule* to solve for x, y, and z (in terms of a and b)

$$\begin{aligned} ax + by &= 1 \\ ay + bz &= 1 \\ az + bx &= 1. \end{aligned}$$

Exam, November 2001

120. Let $u, v \in \mathbb{R} \setminus \{1\}$ such that $u \neq v$. Use *Cramer's rule* to solve for x, y, and z (in terms of u and v)

$$\begin{aligned} x + uy + vz &= 1 \\ y + uz + vx &= -1 \\ z + ux + vy &= 0. \end{aligned}$$

Supp Exam, February 2002

121. Use *Cramer's rule* to solve for $x, y,$ and z (in terms of $u, v,$ and w)

$$\begin{aligned} -x + y + z &= u \\ x - y + z &= v \\ x + y - z &= w. \end{aligned}$$

Class test, May 2003

122. Let $\theta \in \mathbb{R}$. Use *Cramer's rule* to solve for $x, y,$ and z (in terms of $u, v,$ and w)

$$\begin{aligned} x &= u \\ (\cos\theta)y - (\sin\theta)z &= v \\ (\sin\theta) + (\cos\theta)z &= w. \end{aligned}$$

Exam, June 2004

123. Let $u, v, w \in \mathbb{R}$ such that $uvw \neq -1$. Use *Cramer's rule* to solve for $x, y,$ and z (in terms of $u, v,$ and w)

$$\begin{aligned} x + uy &= 1 \\ y + vz &= 0 \\ z + wx &= 0. \end{aligned}$$

Exam, November 2004

124. Let $a, b, c \in \mathbb{R}$ such that $abc \neq -1$. Use *Cramer's rule* to solve for $x, y,$ and z (in terms of $a, b,$ and c)

$$\begin{aligned} x + by &= c \\ y + cz &= a \\ z + ax &= b. \end{aligned}$$

Supp Exam, February 2005

125. TRUE or FALSE ?

(a) The matrix $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}$ is *invertible*.

(b) The vectors $\begin{bmatrix} 4 \\ -6 \\ -10 \end{bmatrix}$ and $\begin{bmatrix} -6 \\ 9 \\ 15 \end{bmatrix}$ are *collinear*.

(c) The equations

$$\vec{r} = \begin{bmatrix} 7 \\ 2 \\ -3 \end{bmatrix} + t \begin{bmatrix} 3 \\ 1 \\ -1 \end{bmatrix} \quad \text{and} \quad \frac{x-1}{-6} = \frac{y}{-2} = \frac{z+1}{2}$$

represent the *same* line.

Class test, May 2003

126. Consider the vectors

$$\vec{u} = \begin{bmatrix} 1 \\ -1 \\ 2 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} -6 \\ 0 \\ 3 \end{bmatrix}.$$

(a) Use the *dot product* to find the angle between $\vec{u}$ and $\vec{v}$.

(b) Use the *cross product* to find a vector $\vec{w}$ orthogonal to both $\vec{u}$ and $\vec{v}$ and such that $\|\vec{w}\| = 3$.

Exam, June 1999

127. TRUE or FALSE ?

(a) The points $A = (1, 2, -1)$, $B = (4, 2, 0)$, $C = (-2, -2, -2)$ are *collinear*.

(b) The lines $x = 1 + 2t, y = 2t, z = 1 - t$ and $\frac{x+1}{2} = \frac{y+2}{2} = \frac{z}{1}$ are *parallel*.

(c) The distance from the point $(1, -1, 1)$ to the plane $x + y + z = 3$ is $\frac{\sqrt{3}}{3}$.

<div align="right">**Exam, June 1999**</div>

128. Consider the vectors

$$\vec{u} = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 2 \\ 0 \\ -1 \end{bmatrix}.$$

  (a) Use the *dot product* to find the angle between $\vec{u}$ and $\vec{v}$.

  (b) Compute the *area* of the triangle determined by $\vec{u}$ and $\vec{v}$.

  (c) Find all values of $k \in \mathbb{R}$ such that the vectors $k\vec{u} + (1 - k)\vec{v}$ and $\begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix}$ are *collinear*.

<div align="right">**Exam, June 2000**</div>

129. Consider the vectors

$$\vec{u} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \quad \text{and} \quad \vec{v} = \begin{bmatrix} 2 \\ -1 \end{bmatrix}.$$

  (a) Calculate

$$\vec{v} - 2\vec{u}, \quad (\vec{v} + \vec{u}) \bullet (\vec{v} - \vec{u}), \quad \text{and} \quad \|\vec{u}\| + \|\vec{v}\| - \|\vec{u} + \vec{v}\|.$$

  (b) Find the *angle* between $\vec{u}$ and $\vec{v}$.

<div align="right">**Class test, October 2001**</div>

130. TRUE or FALSE ? Justify your answers.

  (a) The points $A(1, 1)$, $B(-5, 4)$ and $C(7, -2)$ are *collinear*.

(b) The vectors $\vec{u} = \begin{bmatrix} 1 \\ \alpha \\ -1 \end{bmatrix}$ and $\vec{v} = \begin{bmatrix} 3 \\ 1 \\ \alpha \end{bmatrix}$ are *orthogonal* for some value of α.

(c) Given the points $P(2,1)$, $Q(3,4)$ and $R(1,3)$, the *area* of the parallelogram $\square\,OPQR$ is 5.

Exam, November 2004

131. Consider the planes

$$(\alpha)\quad x - 2y - z = 0 \quad\text{and}\quad (\beta)\quad 2x - y + 3z = 5.$$

(a) Find *parametric equations* of the line $\mathcal{L}$ of intersection of these planes.

(b) Write *symmetric equations* for the line through the point $P(1,1,-2)$ and parallel to the line $\mathcal{L}$.

(c) Find the equation of the plane through the point $P(1,1,-2)$ and perpendicular to the line $\mathcal{L}$.

Class test, October 2001

132. Consider the points

$$A(2,0,0), \quad B(1,1,0), \quad\text{and}\quad C(0,0,3).$$

(a) Find (the components of) the vectors $\overrightarrow{AB}$ and $\overrightarrow{AC}$.

(b) Determine the *angle* (in degrees) between the vectors $\overrightarrow{AB}$ and $\overrightarrow{AC}$.

(c) Compute the *area* of the triangle $\triangle\,ABC$.

Class test, October 2001

133. Consider the points

$$A(-1,0), \quad B(3,0), \quad\text{and}\quad C(0,2).$$

(a) Find (the coordinates of) the point D such that the quadrilateral $\square\,ABDC$ is a *parallelogram*.

(b) Find (the components of) the vectors $\overrightarrow{AB}$, $\overrightarrow{BC}$, and $\overrightarrow{AC}$.

(c) Compute and compare

$$(\overrightarrow{AB} + \overrightarrow{BC})\bullet \overrightarrow{AC} \quad \text{and} \quad \|\,\overrightarrow{AC}\,\|^2 .$$

Explain.

(d) Determine the *angle* (in degrees) between the vectors $\overrightarrow{BC}$ and $\overrightarrow{AD}$.

Exam, November 2001

134. Consider the points

$$A(-2,0), \quad B(1,0), \quad \text{and} \quad C(-1,3).$$

(a) Find (the coordinates of) the point M such that

$$\frac{1}{2}\left(\overrightarrow{AB} + \overrightarrow{AC}\right) = \overrightarrow{AM} .$$

(b) Find (the components of) the vectors $\overrightarrow{AB}$, $\overrightarrow{BC}$, and $\overrightarrow{AC}$.

(c) Compute

$$(\overrightarrow{AB} + \overrightarrow{BC}) + \overrightarrow{CA}$$

and then explain the result obtained.

(d) Determine the *angle* (in degrees) between the vectors $\overrightarrow{AB}$ and $\overrightarrow{CA}$.

Supp Exam, February 2002

135. Consider the point $P(1,0,2)$ and the vectors

$$\vec{u} = \vec{i} - \vec{j} \quad \text{and} \quad \vec{v} = 3\vec{i} + \vec{k}.$$

(a) Determine the *angle* (in degrees) between the vectors $\vec{u}$ and $\vec{v}$.

(b) Write *parametric equations* for the line $\mathcal{L}$ through P with direction $\vec{u}$.

(c) Write the equation of the plane π through P with normal direction $\vec{v}$.

(d) Find the *distance* from the origin to the line $\mathcal{L}$.

Class test, May 2003

136. Consider the points

$$A(-1, 0), \quad B(3, 0), \quad \text{and} \quad C(0, 2).$$

(a) Find (the coordinates of) the point D such that the quadrilateral $\square\, ABDC$ is a *parallelogram*.

(b) Find (the components of) the vectors $\overrightarrow{AB}$, $\overrightarrow{AC} - \overrightarrow{AB}$, $\overrightarrow{BC}$, and $\overrightarrow{AD}$.

(c) Determine the *angle* (in degrees) between the vectors $\overrightarrow{BC}$ and $\overrightarrow{AD}$.

Supp Exam, February 2002

137. Consider the point $P(1, -1, 1)$, the line $\mathcal{L}$ with equations

$$\frac{x-1}{1} = \frac{y-2}{1} = \frac{z}{-2}$$

and the plane π with equation

$$x + y + z - 3 = 0.$$

(a) Write *parametric equations* for the line $\mathcal{L}$.

(b) Find *equations* for

   i. the plane through P and parallel to π;

   ii. the plane through P and the line $\mathcal{L}$.

(c) Determine the *angle* between these two planes.

(d) Compute the *distance* from the point P to

     i. the line $\mathcal{L}$;

    ii. the plane π.

<div align="right">**Exam, June 2003**</div>

138. TRUE or FALSE ? Justify your answers.

    (a) The points $P(-1, 2, 3), Q(0, 1, 3)$, and $R(-4, 5, 3)$ are *collinear*.

    (b) The *angle* between the vectors $\vec{u} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$ and $\vec{v} = \begin{bmatrix} -4 \\ -2 \end{bmatrix}$ is $180°$.

    (c) Given the points $A(0, 2), B(-1, 0)$, and $C(3, -1)$, the *area* of the triangle $\triangle ABC$ is 9.

<div align="right">**Exam, June 2004**</div>

139. Consider the points $A(1, -1, 0)$ and $B(2, 0, 3)$, and the plane π with equation

$$x + y - 2z + 8 = 0.$$

    (a) Write *parametric equations* for the line $\mathcal{L}$ determined by the points A and B.

    (b) Find the point P of intersection of the line $\mathcal{L}$ with the given plane π.

    (c) Determine the (orhogonal) projection B' of the point B onto the plane π. (HINT : The point B' is the intersection of a certain line through B with the given plane.)

    (d) Write *symmetric equations* for the line $\mathcal{L}'$ determined by the points P and B'.

<div align="right">**Exam, June 2004**</div>

140. Consider the points $A(1, 1, -3)$ and $B(1, -1, 5)$, and the plane π with equation

$$y - 4z + 4 = 0.$$

(a) Write

- *parametric equations*

- *symmetric equations*

for the line $\mathcal{L}$ determined by the points A and B.

(b) Find the unique point L of intersection of line $\mathcal{L}$ with plane π.

(c) Calculate the *distance* between L and the midpoint M of the segment $\overline{AB}$.

(d) Determine whether the point $P(4, 0, 1)$ lies on the plane π.

(e) Determine the distance from P to the line $\mathcal{L}$. (HINT : You may use the formula

$$\delta = \frac{\| \overrightarrow{AP} \times \overrightarrow{AB} \|}{\| \overrightarrow{AB} \|}$$

for the distance from point P to line $\overleftrightarrow{AB}$.)

Exam, November 2004

141.

(a) If $z = 2 + i$ and $w = 1 + 3i$, find :

  i. $3z + \bar{w}$;

  ii. $(1 + i)z + w^2$;

  iii. $\arg(z \cdot w)$;

  iv. $|z - 2w|$;

  v. $\mathrm{Re}\left[(z - 1)^{10} + (\bar{z} - 1)^{10}\right]$;

  vi. $\mathrm{Im}\left(\frac{w + \bar{w}}{2i}\right)$.

(b) Solve the equation (for $z \in \mathbb{C}$)

$$z^6 = 1$$

and represent the roots as points in the complex plane.

142. Let $w = \sqrt{3} + i$.

    (a) Compute $w^2, \bar{w}, w^{-1}$, and $|w|$.

    (b) Write w in *polar* (and exponential) form.

    (c) Solve the equation (for $z \in \mathbb{C}$)

    $$z^3 = w$$

    and represent the roots as points in the complex plane.

143. Let $w = -1 - i$.

    (a) Compute $w^2, \bar{w}, w^{-1}$, and $|w|$.

    (b) Write w in *polar* (and exponential) form.

    (c) Solve the equation (for $z \in \mathbb{C}$)

    $$z^3 = -1$$

    and represent the roots as points in the complex plane.

144. Let $w = \sqrt{3} - i$.

    (a) Compute $w^2, \bar{w}$, and w^{-1}.

    (b) Write w in *exponential form* and then compute

    $$w^6 + \bar{w}^6.$$

    (c) Solve the equation (for $z \in \mathbb{C}$)

    $$z^6 - 2\sqrt{3}z^3 + 4 = 0.$$

145. Considert the complex number $w = \sqrt{3} - i$.

    (a) Compute $\bar{w}, |w|$, and w^{-1}.

    (b) Write w in *polar* form.

    (c) Evaluate the expression

$$E = w^{18} + \bar{w}^{18}.$$

    (HINT : You may use De Moivre's formula.)

146. Solve the equation (for $z \in \mathbb{C}$)

$$z^4 - i = 0$$

and represent the roots as points in the complex plane. (HINT : Write the roots in *exponential* form.)

147.

    (a) Write $\left(\frac{1+i\sqrt{3}}{1-i\sqrt{3}}\right)^{1999}$ in the form $a + ib$.

    (b) Show how $\sin\theta$ can be written in terms of the complex exponential function and use this to obtain $\sin^4\theta$ in terms of cosines of multiples of θ.

    (c) Find all solutions of
$$z^5 + 1 = 0$$
    in the form $a + ib$ and show them on a diagram.

148. Show that

$$\sin 5\theta = 5\cos^4\theta \cdot \sin\theta - 10\cos^2\theta \cdot \sin^3\theta + \sin^5\theta.$$

149.

    (a) Let $w = 3 - i$. Plot w, $-w$, $\bar{w}$ and $-\bar{w}$ in the complex plane.

        i. What shape is outlined ?

        ii. What is $|w|$?

    (b) Sketch (in the complex plane) the sets of complex numbers z satisfying, respectively, the conditions :

        i. $|z + i| = 1$.

        ii. $|z - i| = |z|$.

Supp Exam, February 2005

150. Given that $-2 + 3i$ is a *root* of the equation

$$z^4 + 4z^3 + 9z^2 - 16z - 52 = 0$$

find *all* the other roots of this equation.

Bibliography

[Br97]   O. BRETSCHER – *Linear Algebra with Applications*, Prentice-Hall, 1997.

[CR96]   R. COURANT AND H. ROBBINS – *What is Mathematics ? An Elementary Approach to Ideas and Methods* (Second Edition), Oxford University Press, 1996.

[EP88]   C.H. EDWARDS, JR. AND D.E. PENNEY – *Elementary Linear Algebra*, Prentice-Hall, 1988.

[Ep95]   S.S. EPP – *Discrete Mathematics* (Second Edition), Brooks/Cole, 1995.

[Ko91]   B. KOLMAN – *Elementary Linear Algebra*, Prentice-Hall, 1991.

[La86]   S. LANG – *Introduction to Linear Algebra*, Springer-Verlag, 1986.

[Ro95]   K.H. ROSEN – *Discrete Mathematics and its Applications* (Third Edition), McGraw-Hill, 1995.

[Sc00]   E.R. SCHEINERMAN – *Mathematics. A Discrete Introduction*, Brooks/Cole, 2000.