MATH1061

DISCRETE MATHEMATICS

Contents

About the workbook

The MATH1061 course will closely follow the set textbook (see the Course Profile of Study Guide for details of the current textbook), and this is reflected in the workbook. Each chapter (except the last chapter) of the workbook corresponds to a chapter of the textbook and is organized into a chapter overview, chapter learning objectives and sections corresponding to the relevant sections of the textbook. Each section consists of:

1. a list of definitions of important terms and concepts;
2. a collection of examples for you to work through;
3. a list of special points which you should be aware of;
4. a checklist of skills you should acquire in that section.

The solutions to the definitions and examples described in this workbook are provided on the Web, but you should only look at those once you have filled in the definitions and attempted the examples yourself.

The chapters in the workbook are numbered to correspond to the chapters in the textbook, so the chapter numbering of the workbook might seem a bit odd to you. We shall be studying chapters 1 to 5, then chapter 11 (graph theory), chapter 10 (relations), chapter 7 (functions), the last chapter (groups and fields) then chapter 6 and 8. We shall not be studying chapter 9 of the textbook. Hence the numbering of the chapters in the workbook will be: 1, 2, 3, 4, 5, 11, 10, 7, Last chapter, 6, 8.

How to use the workbook

This course is designed for you to work in two ways, both with lectures and also in a more flexible mode. For people unable to attend lectures, you will be provided with an outline detailing the weeks when the various sections should be completed. Thus you work at your own pace to a certain extent, but it is crucial that you keep up to date with lectures. This puts a lot of responsibility on you to ensure that you cover the work at the right pace. Your lecturer will provide an outline with dates that tell you when you should have completed each chapter of the workbook. **It is important that you keep up to date.** It is your responsibility to check the web pages frequently for any changes and further information about the subject, such as the content of the mid-semester examation, dates and so forth.

For those attending lectures (the majority of you), if you purchase a hard copy of this workbook it is a good idea to bring it with you to every lecture, since the lectures will closely follow the workbook.

For each section you need to read the relevant parts of the textbook (details of relevant page numbers are given in the Study Guide) fill in the definition section of the workbook and work through the examples in the workbook. Once you have done that, you should go to that section on the MATH1061 Web pages and check your answers. If you find you are having trouble with any particular example in the workbook, first look at the hint on the MATH1061 Web page, then try the example again before you look at the solution. Once you have completed the definitions and examples for a section of the workbook, read over the Special Points and Checklist. If you aren't certain that you can do everything listed in the Checklist, go back over the relevant examples before proceeding. At the end of each section of the workbook, you should refer back to the Study Guide where there is a list of extra problems from the textbook. You should work through these problems and check your answers against the solutions at the back of the textbook. Sometimes there are many extra problems, so use your own judgement. If you feel you need the extra practice, do all of them; if you are feeling confident in your skills, just do the harder ones.

When you have reached the end of a chapter of the workbook, reread the list of Chapter Learning Objectives (at the start of each chapter) and make sure that you have achieved all those objectives before moving on to the next chapter.

General Comments

You should always bring your workbook to lectures, tutorial and any other contact hour. It is your responsibility to work through the definitions and examples in the workbook, but some of the examples will be discussed in your lectures, so you must bring your workbook to these sessions.

By filling in all the definitions and examples in the workbook, by the end of the course your workbook can act as a complete revision guide, containing relevant definitions and examples as well special points and a checklist of acquired skills.

If you are working through this course without lectures, your lecturer is still there to help. Whenever you have any questions about the course material or how the course is run, please email or call your lecturer or post your question to the course discussion group.

Chapter One

Logic

In the first chapter covered in this subject, you will be introduced to formal Logic. The ability to think logically and to determine whether or not an argument is valid is a vital skill. Consider the following excerpt from *Alice in Wonderland*, by Lewis Carroll:

> *"Do you mean that you think you can find out the answer to it?" said the March Hare.*
>
> *"Exactly so," said Alice.*
>
> *"Then you should say what you mean," the March Hare went on.*
>
> *"I do," Alice hastily replied; "at least–at least I mean what I say–that's the same thing, you know."*
>
> *"Not the same thing a bit!" said the Hatter. "Why, you might just as well say that 'I see what I eat' is the same thing as 'I eat what I see'!"*

In order to win arguments and debates it is extremely important that you can determine whether the given arguments are valid, that is, correct or "legal". In this chapter you will learn how to rewrite a propositional argument in an abstract form and use truth tables to determine the validity of the argument.

Logic is also very important in areas of computer science. The design of digital logic circuits depends directly on the abstract logical connectives which you will find in this chapter. The last section of this chapter discusses the applications of logic to computer science.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- translate English sentences into symbolic statement form;
- translate statement forms into English sentences;
- use the symbols $\sim$, $\vee$, $\wedge$, $\rightarrow$ and $\longleftrightarrow$ to create statements;
- determine the truth values of a given statement form and present this in a truth table;

- negate and rewrite a given statement form;
- determine whether or not two statement forms are logically equivalent;
- determine whether or not a statement form is a tautology or a contradiction;
- determine whether or not a given propositional argument is valid;
- construct a digital logic circuit for a boolean expression and find a boolean expression for a given digital logic circuit;
- determine whether or not two digital logic circuits are equivalent.

Section 1.1

Simple and Compund Statements

In this section you will be introduced to truth tables and three logical connectives: *not*, *or*, *and*. Pay particular attention to:

- truth tables for the logical connectives $\sim$, $\vee$, $\wedge$;
- determining whether two statement forms are logically equivalent.

De Morgan's Laws are useful for the negation of statements and you should remember them. Note the list of logically equivalent statement forms. These tautlolgies are useful for simplifying and rewriting complex statement forms; however do *not* try to memorize it. Just remember that it exists and refer back to it when necessary.

Exercise 1.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. A **statement** or **proposition** is ______________________________

   ____

2. If p is a statement variable, the **negation** of p is ________________

   It has the ________ truth value from p: if p is true, then $\sim p$ is ______

   if p is false, then $\sim p$ is ________

3. If p and q are statement variables, the **conjunction** of p and q is ______

   which is read "________________"

   $p \wedge q$ is true when ______________________________________

   $p \wedge q$ is false when _____________________________________

4. If p and q are statement variables, the **disjunction** of p and q is ______

   which is read "________________"

   $p \vee q$ is true when ______________________________________

   $p \vee q$ is false when _____________________________________

5. A **statement form** or **propositional form** is ____________________

    ____

    ____

6. A **truth table** is ____________________

    ____

    ____

7. Fill in the following truth tables:

p	$\sim p$

p	q	$p \wedge q$

p	q	$p \vee q$

8. Two statement forms are called **logically equivalent** if ____________________

    ____

    ____

9. De Morgan's Laws:

    The statement $\sim(p \wedge q)$ is logically equivalent to the statement ____________

    The statement $\sim(p \vee q)$ is logically equivalent to the statement ____________

10. A **tautology** is ____________________

    ____

11. A **contradiction** is ____________________

    ____

Exercise 1.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Write the following statements in symbolic form.

a) Jayne likes mathematics but does not like chemistry.

Let p be “Jayne likes mathematics” and let q be “Jayne likes chemistry”.

b) Jayne likes neither mathematics nor chemistry but does like biology.

Let p and q be as in part a), and let r be “Jayne likes biology”.

c) Either Sam will come to the party and Max will not, or Sam won’t come to the party and Max will enjoy himself at the party.

Let p be “Sam will come to the party”, let q be “Max will come to the party”, and let r be “Max will enjoy himself at the party”.

2. If p is the statement "it is raining" and q is the statement "it is hot", translate the following into English sentences.

a) $p \wedge \sim q$

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

3. Construct a truth table to determine the truth values for $(p \vee q) \wedge \sim p$.

There are two statement variables so the truth table will have ______ rows.

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

4. Construct a truth table to determine the truth values for $(p \vee q) \wedge \sim (p \vee r)$.

There are three statement variables so the truth table will have ________ rows.

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

5. Are the statement forms $p \wedge \sim q$ and $(p \vee q) \wedge \sim q$ logically equivalent?

There are two statement variables so the truth table will have ________ rows.

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

6. Is the statement form $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$ a tautology, a contradiction, or neither?

There are two statement variables so the truth table will have __________ rows.

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

Special Points

- The truth table for a statement form which has n statement variables will have 2^n rows.
- In other textbooks you might encounter some alternate notation; $\neg p$ is equivalent to $\sim p$.

Checklist

Ensure that you understand:

- how to use the logical connectives $\sim$, $\vee$ and $\wedge$ to create statement forms;
- how to use a truth table to determine the truth values for a statement form;
- how to determine whether or not two statement forms are logically equivalent.

Section 1.2

Conditional Statements

In this section you will be introduced to the logical connectives *if—then* (or *implies*) and *if and only if.* Pay particular attention to:

- truth tables for the logical connectives $\rightarrow$, $\longleftrightarrow$;
- replacing $\rightarrow$ and $\longleftrightarrow$ by a combination of $\sim$, $\vee$, $\wedge$;
- the contrapositive of a conditional statement.

Exercise 1.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. If p and q are statement variables, the symbolic form of **if** p **then** q is ______________. This may also be read "________________________."

   Here p is called the ______________and q is called the ______________

   "If p then q" is false when ______________________________________

   and it is true ____

2. "If p then q" is logically equivalent to ____________________________

3. The **contrapositive** of $p \rightarrow q$ is ________________________________

4. Given statement variables p and q, the **biconditional** of p and q is ______________. This is read "________________________________."

   It is true when ____

   It is false when ____

5. Fill in the following truth tables:

p	q	$p \rightarrow q$

p	q	$p \longleftrightarrow q$

6. The order of operations for the five logical connectives is ______________

____

Exercise 1.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Translate the following statements into symbolic form.

a) (i) If I am worried, I will not sleep. (ii) I will not sleep if I am worried.

Let p be “I will not sleep” and let q be “I am worried”.

b) If I am worried, then I will both work hard and not sleep.

Let p and q be as in part a) and let r be “I will work hard”.

2. Construct a truth table to determine the truth values for $p \to (q \wedge \sim p)$.

There are two statement variables so the truth table will have __________ rows.

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

3. Rewrite the following sentence in "if–then" form. *Either you do not study or you pass the test.*

4. Write the contrapositive of the following sentence. *If you do not study, then you will fail the test.*

5. Rewrite the statements “I say what I mean” and “I mean what I say” in if–then form. Use a truth table to show that the two statements are not logically equivalent.

Let p be “I say it” and let q be “I mean it”.

6. Use a truth table to show that $p \longleftrightarrow q$ is logically equivalent to $(p \to q) \wedge (q \to p)$.

There are two statement variables so the truth table will have ________ rows.

p	q				

7. Use the result of question 6 to complete the following sentence.

p if and only if q is the same as ______________________________

____

Special Points

- Many students forget that when p is false, $p \to q$ is true. Remember that there is only one way for a conditional statement to be false, and that is when the hypothesis is true and the conclusion is false.

Checklist

Ensure that you understand:

- how to use the logical connectives $\to$, and $\longleftrightarrow$ to create statement forms;
- that the contrapositive of an if–then statement is equivalent to the statement;
- how to rewrite statements which use $\to$ and $\longleftrightarrow$ in terms of $\sim$, $\vee$ and $\wedge$.

Section 1.3

Valid and Invalid Arguments

In this section you will learn how to determine whether or not a simple argument is valid.

Exercise 1.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. An **argument** is ____

   ____

   ____

   An argument can be presented symbolically as ____________________

2. An argument is **valid** if ____

   ____

   ____

Exercise 1.3.2: Examples

Complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Represent the following arguments in symbolic form and determine whether or not they are valid.

a) If wages are raised, buying increases. If there is a depression, wages are not raised. Therefore, either there is not a depression, or wages are not raised.

Let w represent "wages are raised", b represent "buying increases", and d represent "there is a depression".

b) If Bill is a cheater, then Bill sits in the back row. Bill sits in the back row. Therefore Bill is a cheater.

Let c represent "Bill is a cheater" and s represent "Bill sits in the back row".

c) If the cat fiddled or the cow jumped over the moon, then the little dog laughed. If the little dog laughed, then the dish ran away with the spoon. But the dish did not run away with the spoon. Therefore the cat did not fiddle.

Let c represent “the cat fiddled”, j represent “the cow jumped over the moon”, d represent “the little dog laughed”, and r represent “the dish ran away with the spoon”.

Special Points

- If you want to avoid the use of a truth table to determine the validity of an argument, remember that you need to look for truth values which make all the premises true and the conclusion false. If you can find such truth values, the argument is invalid; if you cannot find such values, the argument is valid. You should definitely avoid the use of a truth table if you have four or more propositions.
- In choosing letters to represent the propositions of an argument, try to choose letters which will help you remember the propositions.

Checklist

Ensure that you understand:

- how to represent an argument symbolically in the form $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$;
- how to use a truth table to determine whether or not an argument is valid;
- how to determine whether or not an argument is valid by identifying a set of truth values which make the premises true but the conclusion false.

Section 1.4

Application: Digital Logic Circuits

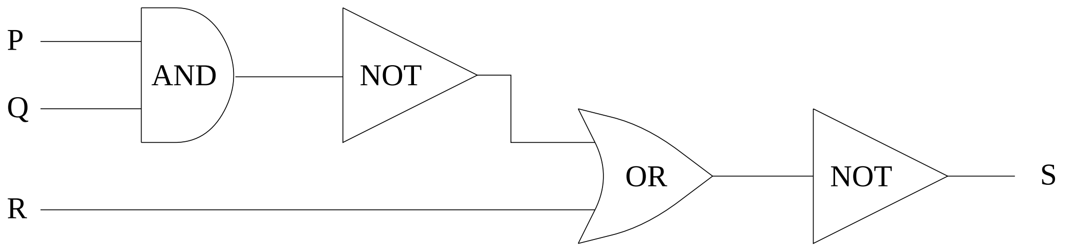
In this section you will discover the analogy between the operations of switching devices and the operations of logical connectives. Pay particular attention to:

- computing the input/output table for a circuit;
- finding a Boolean expression which represents a circuit.

Exercise 1.4.1: Examples

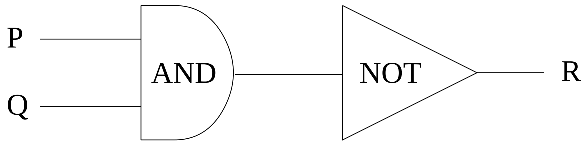
Complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Indicate the output of the circuit below when the input signals are $P = 1$, $Q = 0$ and $R = 0$.



Output: S =

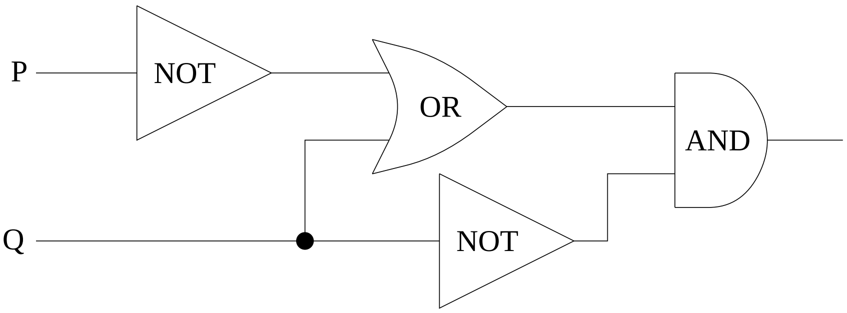
2. Construct the input/output table for the following circuit:



There are two inputs so our table will have __________ rows.

P	Q	R

3. Find a Boolean Expression for the circuit below and determine which combination of inputs this circuit recognizes.



Checklist

Ensure that you understand:

- how to compute the input/output table for a circuit;
- how to find a Boolean expression which represents a circuit.

Have you achieved the Chapter 1 Learning Objectives listed on pages 1 and 2?

Chapter Two

Quantified Statements

In this chapter you will extend your knowledge of symbolic representation of statements to include quantified statements, that is, statements which include quantities such as “every”, “each”, “some”. Many arguments involve quantifiers and it is important to be able to determine the validity of such arguments. In this chapter we shall learn how to translate English statements involving quantifiers into symbolic form and determine their validity.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- translate English sentences involving quantifiers into symbolic statement form;
- translate symbolic statement forms involving $\forall$ and $\exists$ into English sentences;
- determine whether a given statement involving quantifiers is true or false;
- negate statements which involve quantifiers.

Section 2.1

Quantified Statements I

In this section you will learn how to represent quantified statements symbolically. Quantified statements are statements which involve quantities such as “all”, “some” and “every”. Pay particular attention to:

- rewriting English sentences in symbolic form using the quantifiers $\forall$ and $\exists$;
- determining whether a statement using $\forall$ or $\exists$ is true or false;
- negating quantified statements.

Exercise 2.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. A **predicate** is ______________________________

   ____

2. The **domain** of a predicate variable is ______________________________

   ____

3. The symbol $\mathbb{R}$ represents the set of ______________________________

   An example of an element of $\mathbb{R}$ is ______________________________

4. The symbol $\mathbb{Z}$ represents the set of ______________________________

   An example of an element of $\mathbb{Z}$ is ______________________________

5. The symbol $\mathbb{Q}$ represents the set of ______________________________

   An example of an element of $\mathbb{Q}$ is ______________________________

6. The symbol $\forall$ denotes

   The statement "$\forall x \in D, S(x)$" is true, if and only if,

   and is false if, and only if,

7. The symbol $\exists$ denotes

   The statement "$\exists x \in D$ such that $S(x)$" is true, if and only if,

   and is false if, and only if,

8. The negation of "$\forall x \in D, S(x)$" is

9. The negation of "$\exists x \in D$ such that $S(x)$" is

10. The negation of "$\forall x \in D,$ if $P(x)$ then $S(x)$" is

Exercise 2.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Let $P(x)$ be the predicate "10 is a factor of x", and let $S(x)$ be the predicate "5 is a factor of x". Suppose the domain of x is $\{1, 2, \ldots, 99\}$. Determine the truth sets for $P(x)$ and $S(x)$ and indicate the relationship between $P(x)$ and $S(x)$ using some of the symbols $\forall$, $\exists$, $\rightarrow$ and $\longleftrightarrow$.

2. Determine whether the following statements are true or false. Here in a) and b) $\mathbb{R}$ represents the real numbers, and in c) and d) let A be the set $\{1, 2, 3\}$.

a) $\forall x \in \mathbb{R}, x^2 = 2$

b) $\exists x \in \mathbb{R}$ such that $x^2 = 2$

c) $\forall x \in A, x^2 < 10$

d) $\exists x \in A$ such that $x > 4$

3. Translate the following statements into informal English sentences.

a) $\forall$ squares s, s is a rectangle.

b) $\exists x \in \mathbb{R}$ such that $x \in \mathbb{Q}$ (the set of Rational numbers).

4. Negate the following statements and state which of the statements (the original or the negation) is true.

a) $\forall x \in \mathbb{Z}, x$ is even.

b) $\exists y \in \mathbb{R}$ such that $y^2 < 0$.

5. Write the statement “if an integer has a factor of 4, then it also has a factor of 2” in symbolic form. Then write the negation of this statement.

Let $F(x)$ be the predicate “4 is a factor of x” and let $T(x)$ be the predicate “2 is a factor of x”.

Special Points

- The book refers to the set of nonnegative integers $\{0, 1, 2, \ldots\}$ as the natural numbers, $\mathbb{N}$. Other books may refer to the set of positive integers $\{1, 2, \ldots\}$ as the natural numbers. We shall be following the textbook.
- Try to avoid negating quantified statements by simply inserting the word “not” or “do not”, because the resulting statement may be ambiguous.

Checklist

Ensure that you understand:

- how to use the symbols $\forall$ and $\exists$ to write a quantified statement;
- how to prove the truth or falsity of quantified statements;
- how to negate quantified statements.

Section 2.2

Quantified Statements II

In this section you will learn how to write and interpret statements which involve more than one quantifier. Pay particular attention to:

- translating statements involving more than one quantifier from English to symbolic form and from symbolic form to English;

- negating statements which involve more than one quantifier.

Exercise 2.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. The **negation** of $\forall x, \exists y$ such that $P(x, y)$ is ____________________
   ____

2. The **negation** of $\exists x$ such that $\forall y$, $P(x, y)$ is ____________________
   ____

Exercise 2.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Translate the following statements into English sentences.

a) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ such that $x^2 = y^2$.

b) $\exists$ a person p such that $\forall$ languages l, p speaks l.

2. Translate the following statements into symbolic form.

a) There is a child with no siblings.

b) Every integer is divisible by at least one prime number.

3. Negate the following statement: $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}, xy = 0$. Then determine which statement is true, the original or the negation.

Special Points

- Remember that $\forall$ negates to $\exists$ and $\exists$ negates to $\forall$.
- When you are writing quantified statements in mathematical form it is customary to use the words *such that* following the symbol $\exists$. Thus a statement starting $\forall x \in D$ will be followed directly by another quantifier or by the predicate, but a statement starting $\exists x \in D$ will be followed by the words *such that* and then another quantifier or the predicate.

Checklist

Ensure that you understand:

- how to translate statements involving multiple quantifiers from English sentences into symbolic form, and from symbolic form into English sentences.
- how to negate statements which involve multiple quantifiers.

Have you achieved the Chapter 2 Learning Objectives listed on page 20?

Chapter Three

Number Theory

In this chapter you will be introduced to some basic concepts in number theory and four methods of proving or disproving mathematical statements. This chapter is fundamental to this course and we hope that you will spend a significant amount of time on it.

Number theory has been a branch of mathematics since the Greek era but it now has exciting new applications in the fields of coding theory and cryptography. The barcodes used on products you buy in the grocery store and the music on your CDs are just two of the many applications of number theory.

The concept of a mathematical proof is very important. If you are going to base any decisions on a mathematical argument, you must be able to convince other people (as well as yourself) that your argument is correct.

You may have heard about a proof of a number theory theorem in the news in recent years. More than 350 years ago, Pierre de Fermat claimed that it is impossible to find positive integers x, y and z with $x^n + y^n = z^n$ if n is an integer greater than or equal to 3. In 1993 an outline of a proof of this claim was given; however mathematicians found an error with one step of the proof. That error has now been resolved and Fermat's theorem has been proved. Proving theorems can be a lengthy process, but also a very rewarding one.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- classify numbers according to which number system they belong to (natural, integer, rational, irrational, real);
- use the properties of the integers to prove properties of the other number systems;
- use various methods of proof to prove mathematical statements:
    1. direct proof,
    2. proof by contradiction,
    3. proof by contraposition;
- disprove a false mathematical statement by finding a counterexample;

- write a mathematical proof in a clear, concise manner;
- use the definitions of even, odd, prime and composite integers, divisibility, floor and ceiling in mathematical proofs;
- apply the Unique Factorization Theorem and the Quotient-Remainder Theorem;
- apply the Euclidean Algorithm to find the greatest common divisor of two integers;
- determine whether or not a solution exists for a linear Diophantine equation and find such a solution;
- find the general solution for a linear Diophantine equation.

Section 3.0

Formal Definitions of Number Systems

Exercise 3.0.1: Examples

1. Beside each step of the following proof, state which definitions and properties of the integers have been used.

Prove that for all integers m, n, p and r, if $m < n$ and $p < r$, then $m+p < n+r$.

Proof Suppose that m, n, p and r are integers and $m < n$ and $p < r$.

Since $m < n$ and $p < r$,

$n + (-m)$ is positive and $r + (-p)$ is positive by ____________

$(n + (-m)) + (r + (-p))$ is positive by ____________

$[(n + (-m)) + r] + (-p)$ is positive by ____________

$[n + ((-m) + r)] + (-p)$ is positive by ____________

$[n + (r + (-m))] + (-p)$ is positive by ____________

$[(n + r) + (-m)] + (-p)$ is positive by ____________

$(n + r) + ((-m) + (-p))$ is positive by ____________

$(n + r) + (-(m + p))$ is positive by ____________

Hence $m + p < n + r$ by ____________

Checklist

Ensure that you understand

- how to use the properties of integers to justify the manipulation of equations and inequalities which you normally take for granted.

Section 3.1

Odds and Evens, Proofs and Counterexamples

In this section you will focus on the basic structure of simple mathematical proofs and also learn how to disprove a mathematical statement using a counterexample. To illustrate the proof techniques, we shall use the properties of even and odd integers and of prime and composite integers. Pay particular attention to:

- the Method of Direct Proof;
- Common Mistakes people make when writing proofs;
- the Method of Disproof by Counterexample.

Exercise 3.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. An integer n is **even** if, and only if, ______________________________

2. An integer n is **odd** if, and only if, ______________________________

3. An integer n is **prime** if, and only if, ______________________________

   ____

4. An integer $n > 1$ is **composite** if, and only if, ______________________

   ____

5. *Method of Direct Proof*

   To show that "$\forall x \in D$, if $P(x)$ then $Q(x)$" is **true**:

   1. Suppose that for a particular but arbitrarily chosen element of D, $P(x)$ is ____

   2. Show that $Q(x)$ is ____

6. To show that "$\forall x \in D$, if $P(x)$ then $Q(x)$" is **false**, find a value of $x \in D$ for which $P(x)$ is ________________ and $Q(x)$ is ________________

Exercise 3.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Prove that there exists an integer which can be written as a product of primes.

Since this is an existential statement, we only need to find one example of an integer which can be written as a product of primes.

Proof

2. Prove that for all $x \in \{0, 1, 2, 3, 4, 5\}$, $x^2 + x + 41$ is a prime number.

Since this a statement about a specified set of values for x, we can use the method of exhaustion.

Proof

3. Prove that for all integers a, b, c and m, if $a - b = rm$ and $b - c = sm$, then $a - c = tm$ for some integers r, s and t.

Proof Suppose that $a - b = rm$ and $b - c = sm$ for some integers r and s.

Therefore, $a - c = tm$ for some integer t.

4. Prove that for all integers a, b, c and m, if $a = d + rm$ and $b = d + sm$, then $a + c = b + c + tm$ where $d, r, s, t \in \mathbb{Z}$.

Proof Suppose that $a = d + rm$ and $b = d + sm$ for some integers d, r, s.

Therefore, $a + c = b + c + tm$ for some integer t.

5. On page 121 of your textbook, in the section on *Begging the question*, an incorrect proof is given of the fact that the product of any two odd integers is odd. Fill in the steps below to correctly prove that the product of any two odd integers is odd.

Proof Suppose m and n are odd integers. By definition of odd, $m = 2a + 1$ and $n = 2b + 1$ for some integers a and b. Then

$$\begin{aligned} m \cdot n &= (2a + 1)(2b + 1) \\ &= \end{aligned}$$

6. Disprove the following statement. If n is an even integer then

$$1 + 2 + 3 + \ldots + (n - 1) = kn$$

for some integer k. (Note that this statement is true for odd integers).

To disprove this statement, we need only find ONE value of n (an even integer) for which the statement does not hold.

Special Points

- To show that a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" is true, you must show that it is true for *all* values in the domain; but to show such a statement is false, it is enough to find *one* example for which it is false.

Checklist

Ensure that you understand:

- the method of direct proof

    1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$".
    2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true.
    3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

- the method of disproof by counterexample

    1. Express the statement to be disproved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$".
    2. Find a value of x in D for which $P(x)$ is true and $Q(x)$ is false.

- how to format a proof

    1. Write the theorem to be proved.
    2. Clearly mark the beginning of your proof with the word **Proof**.
    3. Make your proof self-contained.
    4. Write proofs in complete English sentences.

- the common mistakes that are often made in proofs and how to avoid them

    1. Arguing from examples.
    2. Using the same letter to mean two different things.
    3. Jumping to a conclusion.
    4. Begging the question (assuming the thing you are trying to prove).
    5. Misusing the word 'if'.

Section 3.2

Rational numbers, Proofs and Counterexamples

In this section, we continue our discussion of proof techniques through the study of the rational numbers, that is, quotients of integers.

Exercise 3.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. A real number r is **rational** if, and only if, ______________________________

   ____

2. A real number that is not rational is ______________________________

Exercise 3.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Determine the truth values of the following statements (remember your logical connectives from Chapter 1).

a) (0 is rational) $\wedge$ (0.377777... is rational).

b) ($\sqrt{7}$ is rational) $\vee$ ($\sqrt{25}$ is rational).

c) $\forall x \in \mathbb{R}$, if $3 \le x \le 4$ then x is rational.

In Section 3.0 we discussed the properties of the integers. You may wish to refer back to that section and use the properties of the integers to prove the following properties of the rationals.

2. Prove that the product of two rational numbers is a rational number.

Proof Suppose r and s are rational numbers. Then by definition of rational, $r =$ and $s =$

3. Prove that every rational number r has an additive inverse.

We need to show that for every rational number r, there exists another rational number s such that $r + s = 0 = s + r$.

Proof Suppose that r is a rational number. Hence $r = a/b$ for some integers a and b, where $b \neq 0$.

Not all integers have a multiplicative inverse; in other words if a is an integer, we may not be able to find another integer a' such that $a \cdot a' = 1 = a' \cdot a$. However, the non-zero rational numbers do have multiplicative inverses.

4. Prove that every non-zero rational number has a multiplicative inverse.

We need to show that if r is a rational number and $r \neq 0$, then there exists another rational number r' such that $r \cdot r' = 1 = r' \cdot r$.

Proof Suppose that r is a non-zero rational number; hence $r = a/b$ for some integers a and b, where $a \neq$ and $b \neq$

Checklist

Ensure that you understand:

- how to classify the real numbers as rational or irrational;
- how to use the properties of integers to prove properties of the rational numbers.

Section 3.3

Divisibility, Proofs and Counterexamples

In this section we discover exactly what it means when one integer *divides* another integer. You will also be introduced to one of the most important theorems in number theory, the *Unique Factorization Theorem.* Pay particular attention to:

- the definition of divisibility;
- the Unique Factorization Theorem.

Exercise 3.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. If n and d are integers and $d \neq 0$, then n is **divisible by** d if, and only if,

   ____

2. The notation ______________ is used to represent the statement "d divides n".

3. d **does not divide** n (denoted ______________) if, and only if, _______

   ____

4. An alternative definition to the definition of a prime number given in Section 3.1 is that an integer $n > 1$ is **prime** if, and only if, __________

   ____

5. The **Unique Factorization Theorem** states that: given any integer $n > 1$, ________________________________

   ____

   ____

   ____

Exercise 3.3.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. a) Does $4 \mid 72$? Explain.

b) Is 24 a multiple of 48? Explain.

c) Does $0 \mid 5$? Explain.

d) Is -3 a factor of 9? Explain.

2. Suppose a and b are negative integers and $a \mid b$. Prove that $b \leq a$.

Proof Suppose that a and b are negative integers and $a \mid b$.

3. a) Does $6 \mid 2a(3b+3), \forall a, b \in \mathbb{Z}$? Explain.

b) Is $2a(4b+1)$ a multiple of 4, $\forall a, b \in \mathbb{Z}$? Explain.

4. Find the unique factorization of the following integers.

a) 5440

b) 43560

5. Suppose that k, a and b are integers. If $k \mid a$ and $k \mid b$, prove that $k \mid (a+b)$.

Proof Suppose that k, a and b are integers such that $k \mid a$ and $k \mid b$.

Checklist

Ensure that you understand:

- how to use the definition of divisibility in proofs;
- the Unique Factorization Theorem.

Section 3.4

Quotient-Remainder Theorem, Proofs and Counterexamples

In this section we encounter another important theorem in number theory: the Quotient-Remainder Theorem. You will also see how sometimes it may be easier to prove a statement by splitting the statement into cases. Pay particular attention to:

- the Quotient-Remainder Theorem.

Exercise 3.4.1: Definitions

Fill in the blanks to complete the following sentences.

1. The Quotient-Remainder Theorem states that given any _______________
   ____
   ____

2. Given a non-negative integer n and a positive integer d such that $n = dq + r$, where $0 \leq r < d$,
   n **div** $d =$ _______________ and n **mod** $d =$ _______________

3. If n is divisible by d then n mod $d =$ __________

4. For non-negative integers a and b, and a positive integer d, if a mod $d = r$ and b mod $d = r$, that is, a and b leave the same remainder upon division by d, then we say that "a is congruent to b modulo d" and write $a \equiv b \pmod{d}$. Note that this is the same as saying $a - b = kd$ for some integer k or equivalently $d \mid (a - b)$.

Exercise 3.4.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Given the following values for n and d, find integers q and r such that $n = d \cdot q + r$ and $0 \leq r < d$.

a) $n = 102$ and $d = 11$.

b) $n = -4$ and $d = 5$.

2. Given an amount of money A between 5 cents and 95 cents, the following steps can be used to determine one possible combination of 50 cent (f), 20 cent (t), 10 cent (n) and 5 cent (v) pieces which equal A.

Round the given amount of money to the nearest multiple of five (since we do not have one cent coins). Then evaluate the steps in the order listed.

$$\begin{aligned} f &= A \text{ div } 50 \\ B &= A \text{ mod } 50 \\ t &= B \text{ div } 20 \\ C &= B \text{ mod } 20 \\ n &= C \text{ div } 10 \\ D &= C \text{ mod } 10 \\ v &= D \text{ div } 5 \end{aligned}$$

Use the steps above to find a set of coins which will be equivalent to 95 cents.

Here $A = 95$, so

$$\begin{aligned} f &= 95 \text{ div } 50 = 1. \\ B &= \\ t &= \\ C &= \\ n &= \\ D &= \\ v &= \end{aligned}$$

3. If a and b are integers such that $a = 4x + 1$ and $b = 4y + 1$ for some $x, y \in \mathbb{Z}$, then prove that the product ab is of the the form $4m + 1$, for some integer m.

Proof Suppose $a = 4x + 1$ and $b = 4y + 1$ for some integers x and y.

4. Determine whether each of the following statements is true or false.

i) $2 \equiv 7 \pmod 5$ ii) $112 \equiv 12 \pmod 9$ iii) $11^2 \equiv 7 \pmod 3$

5. For positive integers u, v, w, x and d, if $u \equiv v \pmod{d}$ and $w \equiv x \pmod{d}$, prove the following two statements.

a) $u + w \equiv v + x \pmod{d}$

b) $uw \equiv vx \pmod{d}$

Special Points

- The notation $x \bmod y$ will be used extensively in this course, and in this course the concept of "mod" is more important than the concept of "div".

Checklist

Ensure that you understand:

- how to find the unique integers q and r such that $n = d \cdot q + r$ with $0 \leq r < d$, for any integer n and positive integer d;
- the meaning of the notation $a \equiv b \pmod{d}$.

Section 3.5

Floor and Ceiling, Proofs and Counterexamples

In this section we gain some more experience in the use of proof techniques by looking at the floor and ceiling of real numbers . The concepts of floor and ceiling are useful in the analysis of computer algorithms.

Exercise 3.5.1: Definitions

Fill in the blanks to complete the following sentences.

1. Given any $x \in \mathbb{R}$, the **floor of** x, denoted $\lfloor x \rfloor$, is ________________________

   ____

2. Given any $x \in \mathbb{R}$, the **ceiling of** x, denoted $\lceil x \rceil$, is ________________________

   ____

Exercise 3.5.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Compute the values of $\lfloor -3.5 \rfloor$, $\lceil 4 \rceil$ and $\lceil \frac{26}{5} \rceil$.

2. Suppose you were working in a job where you were only paid for full hours of work. If you worked for 441 minutes, how many hours of work would you be paid for?

3. Is the following statement true or false? Support your answer by either proving the statement or giving a counterexample.

$$\lfloor x \cdot y \rfloor = \lfloor x \rfloor \cdot \lfloor y \rfloor$$

4. Suppose that n is an even integer. Prove that $\left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{n}{2} \right\rfloor$.

Proof Since n is an even integer, $n = 2k$ for some integer k.

5. Suppose that n is an odd integer. Prove that $\left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{n}{2} \right\rfloor + 1$.

Proof Since n is an odd integer, $n = 2k + 1$ for some integer k.

Checklist

Ensure that you understand:

- how to find the floor and ceiling of any real number.

Section 3.6

Contradiction and Contraposition

In this section we are introduced to two powerful methods of proof: contradiction and contraposition. They are very useful alternatives to the method of direct proof introduced earlier in this chapter. Pay particular attention to:

- the steps of the method of proof by contradiction;
- the steps of the method of proof by contraposition.

Exercise 3.6.1: Definitions

Fill in the blanks to complete the following sentences.

1. *Method of Proof by Contradiction*

   1. Assume that the statement to be proved is ______________________

   Recall that the negation of $\forall x \in D$, if $P(x)$ then $Q(x)$ is ____________

   ____

   2. Show that this assumption leads logically to a __________________

   3. Conclude that the original statement is ______________________

2. *Method of Proof by Contraposition*

   1. Write the statement in the form $\forall x \in D$, if $P(x)$ then $Q(x)$.

   2. Rewrite this statement in the contrapositive form: ______________

   ____

   3. Use the Method of Direct Proof (See Exercise 3.1.1) to prove the __________________________ statement.

Exercise 3.6.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further

questions, please email your lecturer or post your question to the discussion group.

1. Prove the following statement by contradiction. For all integers n and all prime numbers p, if n^2 is divisible by p, then n is divisible by p.

To prove this statement by contradiction we shall assume the negation of the statement and show that this leads to a contradiction.
Proof Suppose that there exists a prime p and an integer n such that n^2 is divisible by p but n is not divisible by p.

2. Prove the following statement by contraposition. For all integers n, if n^2 is odd, then n is odd.

To prove this statement by contraposition we will suppose that n is not odd and show that this implies that n^2 is not odd.
Proof Suppose that n is not odd (so n is even).

3. Prove the following statement using your favourite proof technique. The product of any nonzero rational number and any irrational number is irrational.

Proof

Checklist

Ensure that you understand:

- the method of proof by contradiction:

  1. Suppose the statement to be proved is false.
  2. Show that this supposition leads logically to a contradiction.
  3. Conclude that the statement to be proved is true.

- the method of proof by contraposition:

  1. Express the statement to be proved in the form: $\forall x$ in D, if $P(x)$ then $Q(x)$.
  2. Rewrite this statement in the contrapositive form: $\forall x$ in D, if $\sim Q(x)$ then $\sim P(x)$.
  3. Prove the contrapositive by a direct proof. Suppose that x is a particular but arbitrarily chosen element of D such that $Q(x)$ is false. Show that $P(x)$ is false.

- the various methods of proof and disproof introduced so far:

  1. Direct proof.
  2. Disproof by counterexample.
  3. Proof by contradiction.
  4. Proof by contraposition.

Section 3.7

Two Classical Theorems(Extension Material)

This section presents proofs of two famous theorems and will provide you with two more good examples of the method of proof by contradiction. Pay particular attention to:

- the fact that $\sqrt{2}$ is irrational;
- the fact that there are infinitely many primes.

Exercise 3.7.1: Examples

Complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Prove or disprove the following statements.

a) $\sqrt{25}$ is irrational.

b) $1 + \sqrt{8}$ is irrational.

2. We have established the fact that the set of prime numbers is infinite but the actual process of determining whether or not a large number is a prime number is very time-consuming. Use the Web to find the largest known prime number. You might like to investigate other facts about prime numbers at `http://www.utm.edu/research/primes`.

The largest known prime number is

Checklist

Ensure that you understand:

- the proofs of the main theorem given in this section. You will not have to reproduce the proofs, but you should understand them.

Section 3.8

The Euclidean Algorithm

In this section we shall be introduced to the important Euclidean Algorithm.

Exercise 3.8.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let a and b be integers that are not both zero. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the integer d satisfying the following two properties:

   1. ____

   ____

   2. ____

   ____

Exercise 3.8.2: Examples

Complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Use the Euclidean Algorithm to calculate the gcd of the following pairs of integers.

a) 186, 403

b) 90, 37

c) 36, 102

d) 114, 19

Checklist

Ensure that you understand:

- how to apply the Euclidean Algorithm to find the greatest common divisor of two integers.

Section 3.9

Linear Diophantine Equations

The textbook does not cover Linear Diophantine equations but they are an important application of the Euclidean algorithm so we shall include them in this chapter of the workbook. Pay particular attention to:

- Theorem 3.9.1 (page 9 of the Reader).

Use the information in the reading to complete the following exercises.

Exercise 3.9.1: Definitions

Fill in the blanks to complete the following sentences.

1. State Theorem 3.9.1 from the Reader.

   ____

   ____

   ____

Exercise 3.9.2: Examples

Complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

For each of the following Linear Diophantine equations, determine whether or not a solution exists. If a solution does exist, find one such solution.

1. Find, if they exist, integers x and y which satisfy $91x + 221y = 676$.

2. Find, if they exist, integers m and n which satisfy $105m + 56n = -14$.

3. Find, if they exist, integers x and y which satisfy $115x + 35y = 11$.

Checklist

Ensure that you understand:

- how to determine whether or not a linear Diophantine equation has a solution;
- how to use the Euclidean algorithm to find a particular solution to a linear Diophantine equation.

Section 3.10

General Solution to a Linear Diophantine Equation (Extension Material)

When we are looking for a solution to a linear Diophantine equation, we are often interested in a solution which satisfies certain conditions. For instance, we might require that the solution involve positive integers. The solution found by the method in Section 3.9 usually involves one positive integer and one negative integer. In this section we discover how to find all solutions to a linear Diophantine equation. Pay particular attention to:

- Theorem 3.10.1 (page 14 of the Reader).

Use the information in the reading to complete the following exercises.

Exercise 3.10.1: Definitions

Fill in the blanks to complete the following sentences.

1. State Theorem 3.10.1 from the Reader.

   ____

   ____

   ____

   ____

Exercise 3.10.2: Examples

Complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

In the previous section you found one solution to each of the following linear Diophantine equations. For each equation, use the solution you found in the previous section to find the general solution. Then list all solutions which involve only positive integers.

1. Find a formula for all integers x and y, given that x and y satisfy the linear Diophantine equation $91x + 221y = 676$. List all the solutions which involve positive values for x and y.

2. Find a formula for all integers m and n, given that m and n satisfy the linear Diophantine equation $105m + 56n = -14$. List all the solutions which involve positive values for m and n.

Checklist

Ensure that you understand:

- how to apply Theorem 3.10.1 to find the general solution to a linear Diophantine equation;
- how to find solutions to a linear Diophantine equation which satisfy certain conditions.

Have you achieved the Chapter 3 Learning Objectives listed on pages 29 and 30?

Chapter Four

Sequences & Mathematical Induction

Regular patterns and repeated processes occur all around us and, in many instances, it is important to understand the mathematics behind them. In this chapter we examine mathematical sequences. We also discover another proof technique, the Principle of Mathematical Induction, which is useful in proving statements about sequences. In addition, we discuss the fundamental Well-Ordering Principle for the Integers.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- recognise and use the standard notation for sequences and the sums of sequences;
- use Mathematical Induction and Strong Mathematical Induction to prove mathematical statements;
- apply the Well-Ordering Principle for the Integers in proofs of mathematical statements.

Section 4.1

Sequences

In this section we are introduced to the notation used to describe the terms in a sequence of numbers and to describe the sum of such a sequence. Pay particular attention to:

- the summation notation.

Exercise 4.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. In a sequence, each individual element is called a ____________________

2. An **explicit** or **general formula** for a sequence is ____________________

   ____

3. In expanded form, $\sum_{k=m}^{n} a_k =$ ____

4. For each positive integer n, $n!$, read as ***n* factorial**, is defined to be

   ____

5. **Zero factorial**, $0!$, is defined to be ____________________

Exercise 4.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Compute the first four terms of the sequence

$$a_i = (-1)^{i+1}\frac{n}{i+3}, \text{ for all integers } i \geq 0.$$

2. Find an explicit formula for a sequence that has the following initial terms: $-1, 4, -27, 256, -3125, \ldots$.

3. Write the following summation in expanded form by writing out the first 5 terms and the final term.

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

4. Express the following using summation notation.

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{n\cdot(n+1)}$$

5. Given that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$, provide a simplified expression for $\sum_{i=1}^{n+1} i^2$.

6. Simplify $\prod_{j=2}^{5} 2^j$.

7. Simplify the following:

a) $\dfrac{10!}{8!2!}$ b) $\dfrac{(n+2)!}{n!}$.

Special Points

- Do not let changes in the index variable confuse you. Remember that the sums of two sequences which look different in summation notation may represent the same sequence.
- The sum of a sequence is often called a series.

Checklist

Ensure that you understand:

- how to compute the terms of a sequence, given an explicit formula for the sequence;
- how to use summation notation;
- the factorial notation, $n!$.

Section 4.2

Mathematical Induction I

In this section we are introduced to the principle of mathematical induction. Mathematical induction is a very useful proof technique that is mainly used to prove statements about sums of sequences and repeated events which can be built up from small initial cases.

Exercise 4.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. **Principle of Mathematical Induction**:

   Let $P(n)$ be a statement that is defined for integers n, and let a be a fixed integer. Suppose that:

   1. $P(a)$ ____
   2. For all integers $k \geq a$, ______________________________________

      ____

   Then the statement $P(n)$ is true for all integers $n \geq a$.

2. A proof of a statement $P(n)$ by mathematical induction involves two steps. In the **basis step**, you prove ______________________________

   ____

   In the **inductive step**, you **suppose** that $P(k)$ is __________ and then you **show** that $P(k+1)$ is __________.

3. The supposition that $P(k)$ is true is called the __________________

Exercise 4.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further

questions, please email your lecturer or post your question to the discussion group.

1. Use the Principle of Mathematical Induction to help you write out a combination of 2 and 5 cent coins which would be equivalent to
a) 13 cents   b) 16 cents   c) 21 cents.

2. Proofs by Mathematical Induction can sometimes be a bit messy and, if possible, it helps to follow a set layout. Read this proof and take note of the setting out. You may like to use this method in your proofs.

Prove that for all integers $n \geq 1$, $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Proof Let $P(n)$ denote the statement "$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$".

$P(1)$ is the statement $1 = \frac{1(1+1)}{2}$. This is true since $1 = \frac{2}{2}$.

$P(k)$ is the statement $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$.

$P(k+1)$ is the statement $1 + 2 + \ldots + (k+1) = \frac{(k+1)(k+2)}{2}$.

Assume that $P(k)$ is true. Now prove that $P(k+1)$ is true.

$$\begin{aligned}
\text{L.H.S. of } P(k+1) &= 1 + 2 + \ldots + (k+1) \\
&= 1 + 2 + \ldots + k + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \text{ since } P(k) \text{ is assumed true} \\
&= \frac{k(k+1)}{2} + \frac{(k+1) \cdot 2}{2} \\
&= \frac{(k+1)(k+2)}{2} \\
&= \text{R.H.S. of } P(k+1)
\end{aligned}$$

Therefore $P(k+1)$ is true.

Hence, for all integers $n \geq 1$, $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

3. Follow the format of the proof given on the previous page to prove the following claims.

a) For all integers $n \geq 1$, $\sum_{i=1}^{n}(2i-1) = n^2$.

Proof

$P(1)$ is the statement

$P(k)$ is the statement

$P(k+1)$ is the statement

b) For all integers $n \geq 1$, $\displaystyle\sum_{j=1}^{n} \frac{1}{j(j+1)} = \frac{n}{n+1}$.

Proof

$P(1)$ is the statement

$P(k)$ is the statement

$P(k+1)$ is the statement

c) For all integers $n \geq 1$, $\displaystyle\sum_{j=1}^{n} 2^{j-1} = 2^n - 1$.

Proof

$P(1)$ is the statement

$P(k)$ is the statement

$P(k+1)$ is the statement

Special Points

- A proof by mathematical induction only proves that a statement is true for all integers greater than or equal to your basis step. If your proof uses a basis step of $P(4)$, then you have only shown that your statement is true for integers $n \geq 4$, not for values such as $n = 1$ or $n = -3$.
- Usually the basis step is either $n = 0$ or $n = 1$, but any integer may be used as a basis step. The value for your basis step will normally be clear to you from the question.

Checklist

Ensure that you understand:

- why the principle of mathematical induction works;
- how to use the principle of mathematical induction to prove a mathematical statement.

Section 4.3

Mathematical Induction II

In the previous section, mathematical induction was used to prove statements about the sums of sequences. In this section we see how mathematical induction may be used to prove statements about divisibility, inequalities and explicit formulae for sequences.

Exercise 4.3.1: Examples

Complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

Use mathematical induction to prove the following statements. To aid the clarity of your proofs, you should follow the format introduced in the previous section. Always state $P(a)$ (where a is the value for your basis step), $P(k)$ and $P(k+1)$ before you begin the body of your proof.

1. Prove that for all integers $n \geq 1$, the product $n(n+1)(n+2)$ is divisible by three.

Proof

$P(1)$ is the statement

$P(k)$ is the statement

$P(k+1)$ is the statement

2. Prove that $n! > 2^n$ for all integers $n \geq 4$.

Notice that here we are only interested in $n \geq 4$ so your basis step should be $P(4)$.

Proof

$P(4)$ is the statement

$P(k)$ is the statement

$P(k+1)$ is the statement

3. A sequence $b_0, b_1, b_2, \ldots$ is defined by letting $b_0 = 7$ and $b_i = b_{i-1} - 4$ for all integers $i \geq 1$. Prove that $b_n = 7 - 4n$ is a general formula for this sequence for all integers $n \geq 0$.

Proof

$P(0)$ is the statement

$P(k)$ is the statement

$P(k+1)$ is the statement

Special Points

- Always check the wording of the question to make sure you have the correct value in your basis step.

Checklist

Ensure that you understand:

- how to use mathematical induction to prove statements about divisibility, inequalities and explicit formulae for sequences.

Section 4.4

Strong Mathematical Induction

In this section we are introduced to Strong Mathematical Induction. The main difference between Strong and regular Mathematical Induction is that in Mathematical Induction you suppose $P(k)$ is true for a single integer value of k and then use that to prove $P(k+1)$ is true, whereas in Strong Mathematical Induction you suppose that $P(i)$ is true for all integer values of i which are greater than or equal to a (your basis step) but less than some integer k, and then use some of those values of i to prove that $P(k)$ is true.

This section also introduces the Well-Ordering Principle for the Integers, a simple but fundamental principle about the integers. Pay particular attention to:

- the proof of Divisibility by a Prime.

You may omit the section on the Binary Representation of Integers.

Exercise 4.4.1: Definitions

Fill in the blanks to complete the following sentences.

1. Principle of Strong Mathematical Induction:

   Let $P(n)$ be a statement that is defined for all positive integers n and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

   1. $P(a), P(a+1), \ldots$ and $P(b)$, ______________________

   2. For any integer $k > b$, if $P(i)$ is true for all integers i with $a \leq i < k$, then ______________________

   ____

   Then the statement $P(n)$ is true for all integers $n \geq a$.

2. State the Well-Ordering Principle for the Integers

   ____

   ____

   ____

Exercise 4.4.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. For each of the following sets, if the set has a least element, state what that least element is. If there is no least element, explain why the well-ordering principle for the integers does not apply.

a) The set of all nonnegative even integers.

b) The set of all negative integers of the form $46 - 7k$, where $k \in \mathbb{Z}$.

2. Suppose that $b_1, b_2, b_3, \ldots$ is a sequence defined as follows: $b_1 = 2$, $b_2 = 4$, $b_r = 5b_{r-1} - 6b_{r-2}$ for all integers $r \geq 3$. Prove (using Strong Mathematical Induction) that $b_n = 2^n$ for all integers $n \geq 1$.

Proof

3. Read and understand the proof of Divisibility of a Prime given below. This proof (by contradiction) which uses the Well-Ordering Principle for the Integers.

Every positive integer greater than one has a prime divisor.

Proof Assume that there is a positive integer greater than one which does not have a prime divisor. Then since the set of positive integers greater than one with no prime divisors is non-empty, the Well-Ordering Principle says that there is a least positive integer n, greater than one, with no prime divisors. Since n has no prime divisors and n divides n, n is not prime. Hence we can write $n = ab$ with $1 < a < n$ and $1 < b < n$. Since $a < n$, a must have a prime divisor, say p (recall that n was the least positive integer with no divisors). But $p \mid a$ and $a \mid n$ so $p \mid n$, contradicting the fact that n has no prime divisors.

Special Points

- It can be shown that the Principles of Mathematical Induction and Strong Mathematical Induction are equivalent. In addition, the Principle of Mathematical Induction is also equivalent to the Well-Ordering Principle (for the natural numbers).

Checklist

Ensure that you understand:

- the difference between Strong Mathematical Induction and regular Mathematical Induction;
- the Well-Ordering Principle for the Integers.

Have you achieved the Chapter 4 Learning Objectives listed on page 64?

Chapter Five

Set Theory

All collections of mathematical objects can be defined in terms of sets, so the language of set theory is an important part of an introductory mathematics course. The language of sets provides a framework which allows mathematicians to work efficiently. This chapter provides the basic definitions and notation of set theory, and establishes properties of sets through proofs and counterexamples.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- use set notation to write mathematical statements;
- use the definitions of subset, proper subset, equal sets, union, intersection, difference, complement and Cartesian product in determining whether an alleged property of a set is true or false;
- determine whether set properties involving the empty set, $\emptyset$, are true or false;
- use the definitions of the empty set, disjoint sets, mutually disjoint sets, partitions of sets, and the power set in determining whether an alleged property of a set is true or false.

Section 5.1

Basic Definitions

In this section we are introduced to the notation used to describe sets and the basic operations which apply to sets. Pay particular attention to:

- the definitions of subset, set equality, union, intersection, difference, complement and Cartesian product.

Exercise 5.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. The notation $a \in S$ means that ____________________________

2. The order of the elements listed in a set is ____________________

   so $\{x_1, x_2, x_3\}$ _____ $\{x_2, x_3, x_1\}$.

3. The **empty set** is the set containing no elements and is denoted by $\emptyset$.

4. For an arbitrary set A, the **cardinality** of the set A is the number of elements in A and is denoted by $n(A)$ or equivalently $|A|$.

5. If A and B are sets, A is called a **subset** of B, written __________, if, and only if, ____

6. Let A and B be sets. A is a **proper subset** of B if, and only if, ______

   ____

7. Given sets A and B, A **equals** B, written ____________ if, and only if, ____

8. Let A and B be subsets of a universal set U.

   The **union** of A and B, denoted ____________, is ____________

____

The **intersection** of A and B, denoted ______________, is ______________

____

The **difference** of B minus A, denoted ______________, is ______________

____

The **complement** of A, denoted ________________, is ________________

____

9. Let n be a positive integer and let $x_1, x_2, \ldots, x_n$ be (not necessarily distinct) elements. The **ordered n-tuple**, denoted $(x_1, x_2, \ldots, x_n)$, consists of ____

   ____

   Therefore, an ordered pair (x, y) is a ______________________________

   Two ordered n-tuples are **equal** if, and only if, ________________________

   ____

10. Given two sets A and B, the **Cartesian product** of A and B, denoted ______________ is ____

    ____

11. Let $A(x)$ represent the predicate "x is an element of A" and let $B(x)$ represent the predicate "x is an element of B". Write the following definitions using the symbolic logic from Chapters 1 and 2.

    $A \subseteq B$: ____

    $A \nsubseteq B$: ____

    $A = B$: ____

    $A \cup B$: ____

    $A \cap B$: ____

$B - A$: ______________________________

Exercise 5.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. a) How many elements does the set $\{3, 3, \{3\}\}$ have? ____________

b) Is $\{1, 1, 2\} = \{1, 2\}$? ____________

c) Is $1 \in \{1\}$? ____________

d) Is $1 \in \{\{1\}\}$? ____________

2. Describe the following sets in words.

a) $\{1, 2, \ldots, 100\}$

b) $\{x \in \mathbb{R} \mid x > 0\}$

c) $\{y \in \mathbb{Z}^+ \mid -3 \leq y \leq 3\}$

3. Suppose $A = \{a, b, c, d\}$, $B = \{a, b, e\}$ and $C = \{a, b, c, d, e\}$. Give reasons for your answers to the following questions.

a) Is $B \subseteq A$?

b) Is $A \subseteq C$?

c) Is A a proper subset of C?

d) Is $B \subseteq B$?

4. Draw a Venn diagram to represent the relationship between the following sets: $A = \{1, 2, 3\}$, $B = \{1, 4\}$, $C = \{2, 3\}$.

5. True or false:
a) $\{4\} \in \{1, \{3\}, 4\}$ ______________

b) $\{4\} \subseteq \{1, \{3\}, 4\}$ ______________

c) $\{3\} \in \{1, \{3\}, 4\}$ ______________

d) $1 \subseteq \{1, \{3\}, 4\}$ ______________

6. Let

$$\begin{aligned} A &= \{x \in \mathbb{Z} \mid x = 4p - 1 \text{ for some } p \in \mathbb{Z}\}, \\ B &= \{y \in \mathbb{Z} \mid y = 4q - 5 \text{ for some } q \in \mathbb{Z}\}. \end{aligned}$$

Prove that $A = B$.

Proof We must show that $A \subseteq B$ and $B \subseteq A$.

7. Let the universal set be $\{1, 2, \ldots, 10\}$ and let $A = \{1, 2, 3, 4\}$, $B = \{2, 4, 6, 8, 10\}$ and $C = \{1, 3, 5, 7, 9\}$.

State:
a) $A \cap B$ ______________________________

b) $B \cup C$ ______________________________

c) $B - A$ ______________________________

d) $A - C$ ______________________________

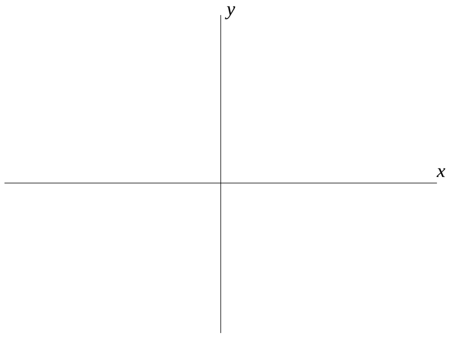
e) B^c ______________________________

f) A^c ______________________________

g) $A^c \cup B$ ______________________________

8. A Cartesian product with which you are probably already familiar is the xy-plane. The points which make up the plane are the elements of the set $\mathbb{R} \times \mathbb{R}$.

a) On the set of axes below, plot the points representing the ordered pairs $(1, 2)$ and $(2, 1)$.



b) Let $A = \{-1, 0, 1\}$ and $B = \{3, 4, 5\}$. Write out the set $A \times B$, and plot the elements of the set on the set of axes above. How many elements are in the set $A \times B$?

Special Points

- Be careful not to confuse the symbols $\in$ and $\subseteq$. The first is used to state that an *element* belongs to a set, the second states a relationship between *two sets.*
- The wording "B set difference A" is often used instead of the "difference of B minus A", and the notation $B \setminus A$ is used instead of $B - A$.
- Many textbooks will use the notation $\overline{A}$ for the complement of A instead of A^c.
- The number of elements in a set is called the *cardinality* of the set as is denoted $n(A)$ or $|A|$.

Checklist

Ensure that you understand:

- the notation used to describe sets;
- the definitions of subset, proper subset, equal sets, union, intersection, difference, complement and Cartesian product.

Section 5.2

Properties of Sets

In this section you are introduced to methods of determining whether alleged set properties are true or false.

Exercise 5.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. Subset Relations: Let sets A, B and C be arbitrary sets.

   1. the Inclusion of Intersection Rule states:

   a) ______________________________and b) ______________________________

   2. The Inclusion in Union Rule states:

   a) ______________________________and b) ______________________________

   3. The Transitive Property of Subsets is:

   if ____________________and ____________________, then ____________________

Note the names are not important, but the actual rules are!

Exercise 5.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Rewrite the subset relation $P \subseteq P \cup Q$ using the logical connectives and quantifiers from Chapters 1 & 2, and use truth tables to validate the relation.

Let $P(x)$ be the predicate "$x \in P$", $Q(x)$ be the predicate "$x \in Q$", and let U be the universal set. Then $P \subseteq P \cup Q$ is equivalent to
$(\forall x \in U)\ P(x) \rightarrow (P(x) \vee Q(x))$.
To prove this is true we can use a truth table:

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

2. Rewrite the set property $(A \cap B)^c = A^c \cup B^c$ using the logical connectives and quantifiers from Chapters 1 and 2. Then use a truth table to prove the property is true.

Let $A(x)$ be the predicate "$x \in A$", $B(x)$ be the predicate "$x \in B$", and let U be the universal set.

3. Determine whether the following statements are true or false.

a) $A \subseteq A \cap B$ ____________________

b) $C \subseteq (A \cap B) \cup C$ ____________________

c) $A \cup B \subseteq A \cap B$ ____________________

d) $A \cap (B \cup A^c) = A \cap B$ ____________________

e) $(A \cup B) - (A \cap B) = A - B$ ____________________

Special Points

- Revise the definitions of the set operations. Let A and B be subsets of a universal set U and suppose x and y are elements of U.

  1. $A \subseteq B$ is equivalent to "$\forall x$, if $(x \in A)$ then $(x \in B)$."
  2. $x \in (A \cup B)$ is equivalent to "$(x \in A)$ or $(x \in B)$."
  3. $x \in (A \cap B)$ is equivalent to "$(x \in A)$ and $(x \in B)$."
  4. $x \in (A - B)$ is equivalent to "$(x \in A)$ and $(x \notin B)$."
  5. $x \in A^c$ is equivalent to "$x \notin A$."
  6. $(x, y) \in (A \times B)$ is equivalent to "$(x \in A)$ and $(y \in B)$."

Checklist

Ensure that you understand:

- how to determine whether an alleged property of a set is true or false.

Section 5.3

The Empty Set, Partitions, and Power Sets

In this section we discuss the empty set, that is, the set with no elements. We will also focus on the partitioning of a set into subsets, and discover what a *power set* of a set is. Pay particular attention to:

- the discussion of the empty set.

Exercise 5.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. The ______________________ is a unique set containing no elements.

   It is denoted by the symbol __________

2. The empty set is a subset of every set. Symbolically: ________________

   Every set is a subset of itself. Symbolically: ________________________

3. Two sets are called **disjoint** if, and only if, ________________________

   ____

   Symbolically: A and B are disjoint $\Leftrightarrow$ ____________________________

4. Sets $A_1, A_2, \ldots, A_n$ are **mutually disjoint** if, and only if, ____________

   ____

   ____

   That is,, for all $i, j = 1, 2, \ldots, n$, $A_i \cap A_j =$ __________ whenever $i \neq j$.

5. A collection of nonempty sets $\{A_1, A_2, \ldots, A_n\}$ is a **partition** of a set A if, and only if, it satisfies the two properties

   1. ____

   2. ____

6. Given a set A, the **power set** of A, denoted $\mathcal{P}(A)$, is ________________

____

Exercise 5.3.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Complete the following proof of the statement: *There is only one set containing no elements.*

Proof Suppose $\emptyset_1$ and $\emptyset_2$ are each sets with ________________elements.
Since $\emptyset_1$ has no elements, it is a subset of ________________________.
That is, ________________

Also since $\emptyset_2$ has no elements ________________.

Thus ________________ by definition of set equality.

2. Determine whether the following statements are true or false.

a) $\emptyset = \{\emptyset\}$ ____________________

b) $A \cup \emptyset = A$ ____________________

c) $A \cap A^c = \emptyset$ ____________________

d) $A \cup A^c = \emptyset$ ____________________

e) $A \cap \emptyset = \emptyset$ ____________________

f) $(A - B) \cap B = \emptyset$ ____________________

g) $\{a, b, c\}$ and $\{d, e\}$ are disjoint sets. ____________________

h) $\{1, 2\}$, $\{5, 7, 9\}$ and $\{3, 4, 5\}$ are mutually disjoint sets. ________________

3. Let

$$\begin{aligned} A_1 &= \{n \in \mathbb{Z} \mid n < 0\} \\ A_2 &= \{n \in \mathbb{Z} \mid n > 0\} \end{aligned}$$

Is $\{A_1, A_2\}$ a partition of $\mathbb{Z}$? If so, explain why; if not, give a partition.

4. If $B = \{1, 2, 3\}$, list the elements of $\mathcal{P}(B)$.

Since B has three elements, the power set of B will have ________ elements.

Special Points

- When asked to list all subsets of a given set A, many students forget that $\emptyset \subseteq A$ and $A \subseteq A$.
- Remember that for all integers $n \geq 0$, if a set X has n elements, then $\mathcal{P}(X)$ has 2^n elements.

Checklist

Ensure that you understand:

- the definitions of the empty set, disjoint sets, mutually disjoint sets, partitions of sets, and the power set.
- how to determine whether set properties involving $\emptyset$ are true or false;

Have you achieved the Chapter 5 Learning Objectives listed on page 84?

Chapter Eleven

Graphs Theory

Graph theory was first studied many years ago, but it has many modern applications. The essence of graph theory first appeared in the year 1736, when the great Swiss mathematician Leonhard Euler used graphs to solve the famous Königsberg bridge problem.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- understand the definitions of graphs, simple graphs, subgraphs, complete graphs, bipartite graphs, paths, circuits, trees and forests;
- distinguish between graphs and digraphs;
- determine whether a graph has a Euler circuit;
- represent a graph by a matrix.

Section 11.1

An Introduction

Graphs are discrete structures consisting of vertices and edges that connect these vertices. There are several different classes of graphs. These differ with respect to the type and number of edges that connect pairs of vertices. The main emphasis of this section is on introducing the terminology used to describe graphs. There are many definitions given in this section and you may need to revise these definitions a few times in order to remember them all.

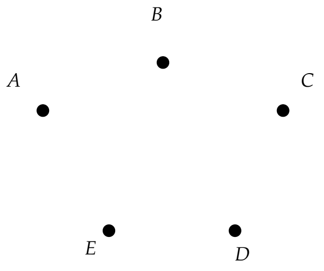
Exercise 11.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. Imagine a medical practitioner working out of six different surgeries. At each surgery there is a computer used to store medical records. To allow patients to freely visit any one of the surgeries the six different computers are to be networked. Analysis shows that the following connections are optimal:

   - connect computer A with computers B and D;
   - connect computer B with computers A, C and E;
   - connect computer C with computers B, D and E;
   - connect computer D with computers A and C;
   - connect computer E with computers B and C;

   In the following diagram, the dots represent the computers. Illustrate the computer connections by drawing straight lines to represent each connection.



A network can be represented by a ______________ . The dots (or nodes in the network) are called ______________________ (plural of ______________) and the line segments joining vertices are called ______________________________.

2. A **graph** G consists of two finite sets:

   - a set $V(G)$ of ______________, and
   - a set $E(G)$ of ___________, where each edge is associated with a set consisting of either one or two vertices called its __________.

   It is assumed that $V(G) \neq \emptyset$. That is, the vertex set $V(G)$ is assumed to be ______________________________________.

   A **loop** is an edge with just ______________________endpoint.

   Parallel edges are two or more distinct edges with the ___________ set of endpoints.

   An edge is said to be **incident** on each of its _______________.

   Two edges are **adjacent** if they are incident on the same __________.

   Two vertices are said to be **adjacent** if they are connected by an ____.

   A vertex that is an endpoint of a loop is said to be _____________.

   An **isolated** vertex, is a vertex which is incident on _____________.

3. Let G be a graph.

   (i) The edge set, $E(G)$, consists of subsets of $V(G)$ of size _________.

   (ii) The vertices $x, y \in V(G)$ are _________________if, and only if, $\{x, y\} \in E(G)$.

   (iii) The edges $\{x, y\}, \{u, v\} \in E(G)$ are adjacent if, and only if, _____ ______________________________________.

(iv) List the edge set for the graph you drew for the computer network.

____

4. A **directed graph**, or **digraph**, consists of two finite sets:

   - a set $V(G)$ of ________________, and

   - a set $E(G)$ of ________________, where each edge is associated with an ordered pair of vertices called its ____________.

   If e is an edge in a directed graph which is associated with the ordered pair (v, w) of vertices, then e is said to be the ________________________ from v to w.

5. A **simple graph** has no ____________________________________ or ________________________.

6. A **complete graph**, denoted K_n, on n vertices, $v_1, v_2, \cdots, v_n$, is a simple graph with an edge connecting every ________________ of vertices.

7. A **bipartite** graph is a simple graph whose vertex set can be partitioned into two disjoint sets $V_1 = \{v_1, v_2, \ldots, v_m\}$ and $V_2 = \{w_1, w_2, \ldots, w_n\}$ such that every edge of the graph has one endpoint in the set V_1 and the other endpoint in the set V_2.

   Use the above definition to complete the following statement. A **complete bipartite graph** on $m + n$ vertices, denoted $K_{m,n}$, is a bipartite graph with vertices $V_1 = \{v_1, v_2, \ldots, v_m\}$ and $V_2 = \{w_1, w_2, \ldots, w_n\}$ in which every vertex in V_1 ____

   ____

   ____

8. A graph H is said to be a **subgraph** of a graph G if, and only if, every vertex in H is also ______________________________, every edge in H is also ______________________________, and every edge in H has the same

   ____

9. Let G be a graph and v a vertex of G. The **degree of** v, denoted $\mathbf{deg}(v)$, equals ____

   ____.

   The **total degree of** G is the ______________________________________.

10. **Theorem** If G is any graph, then the sum of the degrees of all the vertices of G equals ____.

    Equivalently, for any graph G with vertex set $V(G) = \{v_1, v_2, \cdots, v_n\}$, then

$$\begin{aligned} \text{the total degree of } G &= \underline{\hspace{6cm}} \\ &= 2(\underline{\hspace{4.5cm}}) \\ &= 2|E(G)|. \end{aligned}$$

11. **Corollary** The total degree of a graph is _______________.

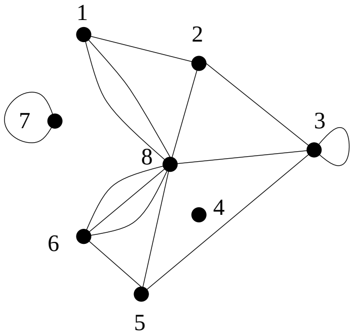
12. **Lemma** In any graph there is an even number of vertices of ________.

    ____

Exercise 11.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. In the following graph determine the sets of: vertices, edges, loops, isolated vertices and parallel edges.



Vertices:

Edges:

Loops:

Isolated vertices:

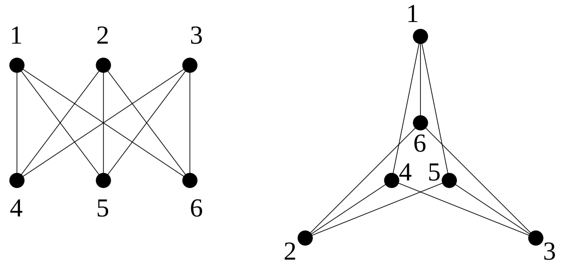
Parallel edges:

2. Consider the graph specified as follows:

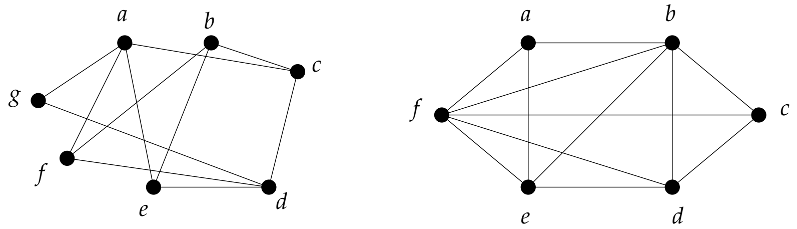
$$\begin{aligned} \text{vertex set} &= \{v_1, v_2, v_3, v_4, v_5, v_6\}, \\ \text{edge set} &= \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_3, v_5\}, \{v_1, v_3\}, \{v_6, v_6\}, \\ &\quad \{v_3, v_6\}\}. \end{aligned}$$

Draw this graph.

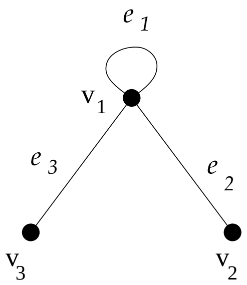
3. List the vertex set and edge set for each of these two graphs and verify that they are two representations of the same graph.



4. For each of the following graphs, determine whether or not the graph is bipartite. Explain your answers.



5. Find all nonempty subgraphs of the following graph.



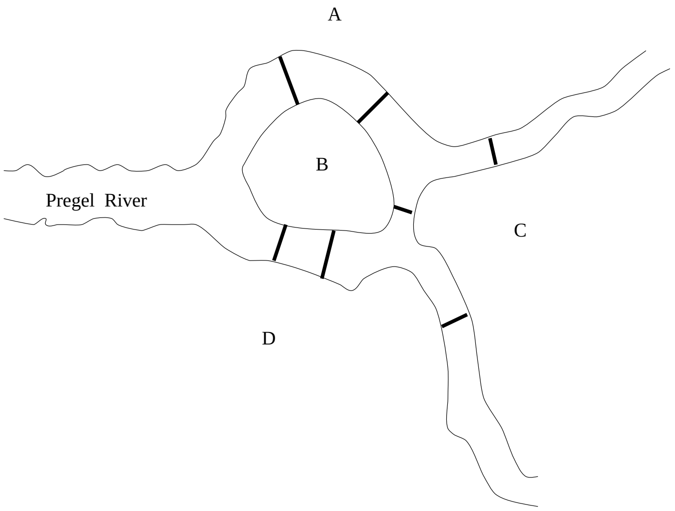
6. Show that the complete graph on seven vertices is a subgraph of the complete graph on ten vertices.

7. Find the total degree of the graph in Question 1. Then apply Theorem 11.1.1 to calculate the number of edges in the graph.

8. Is there a graph with seven vertices of degrees $2, 3, 3, 4, 4, 5$, and 6? Explain your answer.

9. Either draw a graph with ten vertices in which each vertex has degree 3, or show that such a graph cannot exist.

10. **Königsberg bridge problem.** The town of Königsberg in Prussia was built at a point where two branches of the Pregel River met. The town encompassed an island and land adjacent to the river banks. These were connected by seven bridges as shown in the following figure.



Draw a graph which represents the river crossings of Königsberg.

Special Points

- In many graph theory textbooks, the term "multiple edges" is used instead of "parallel edges".

Checklist

Ensure that you understand:

- the definition of a graph, the vertex set of a graph and the edge set of a graph;
- the definition of adjacent edges and adjacent vertices;
- the definition of loops and parallel edges;
- the definition of directed graphs, simple graphs, complete graphs, bipartite graphs and subgraphs;
- the relationship between the sum of the degrees of the vertices of a graph and number of edges of that graph.

Section 11.2

Paths and Circuits

In many applications of graph theory, we are interested in getting from vertex u to vertex v. This could be related to travelling from one city to another or ensuring electricity can get from the generating station to your house. In this section, we investigate paths and circuits in graphs. Pay particular attention to:

- the differences between walks, paths and circuits;
- the proofs of Theorems in this section.

Exercise 11.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let G be a graph and let v and w be vertices in G.

   A **walk from v to w** is ______________________________

   ____

   ____

   ____

   The **trivial walk from v to v** consists of ____________________.

   Hence a trivial walk contains __________ edges and so a loop is __________ a trivial walk.

2. Given a walk $v_0e_1v_1e_2 \dots v_{n-1}e_nv_n$ if there is no ambiguity, then the notation is sometimes simplified to $v_0v_1v_2 \dots v_n$ or to $e_1e_2 \dots e_n$.

3. A **path from v to w** is ______________________________

   ____

   ____

   In a **simple path from v to w** there are __________ repeated vertices.

4. A **closed walk** is a path that ____________ and ____________ at the same vertex

5. A **circuit** is ____________ that does ____________ contain a repeated edge.

   A **simple circuit** is a circuit in which the only repeated vertices are the ____________ and the ____________.

6. Let G be a graph. Two **vertices** v **and** w **of** G **are connected** if, and only if, ________________________________.

   The **graph** G **is connected** if, and only if, given *any* two vertices v and w in G ________________________________.

7. **Lemma** Let G be a graph.

   (a) If G is connected, then any two distinct vertices of G ________ ________________________________.

   (b) If G contains a circuit incident with vertices v and w, and one edge is removed from the circuit, then ____________ ________________________________.

   (c) If G is connected and G contains a circuit, then ____________ ________________________________.

8. Let G be a graph. An **Euler circuit** for G is a circuit that is incident with ____________ vertex of G and uses every edge of G ________________ once.

9. **Theorem** A nonempty graph G has an Euler circuit if, and only if, G is ________________ and every vertex of G has ________. ________________________________.

10. Thus if a nonempty graph G contains a vertex odd degree, then the graph

    ____

    .

11. Let G be a graph and let v and w be two vertices of G. An **Euler path from v to w** is a path ____

    ____

    ____

    ____.

12. **Corollary** Let G be a graph and let v and w be two vertices of G. There is an Euler path from v to w if, and only if, ___________________________

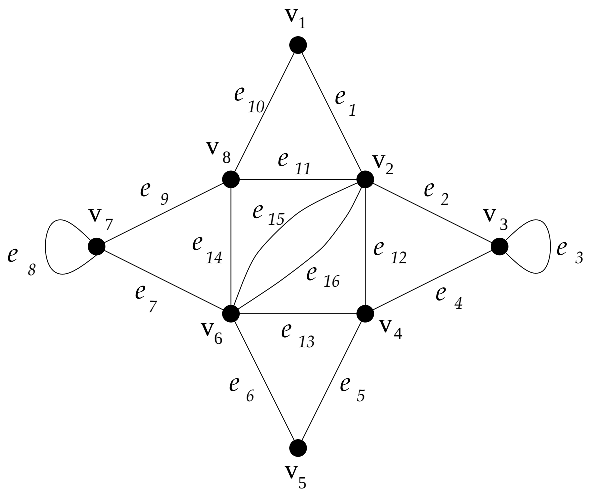
    ____

    ____.

Exercise 11.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Consider the following graph.



Determine which of the following walks are paths, simple paths, circuits, and/or simple circuits.

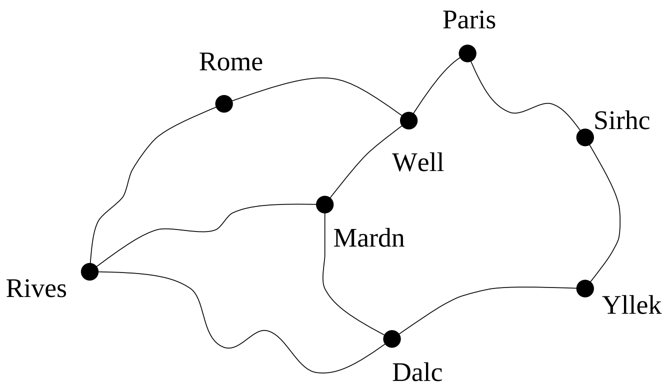
a) $v_3 v_4 v_6 v_8 v_1 v_2 v_3$.

b) $e_1 e_{11} e_{14} e_7 e_8 e_9 e_{10}$.

c) $v_1 e_1 v_2 e_{11} v_8 e_{14} v_6 e_{15} v_2 e_1 v_1$.

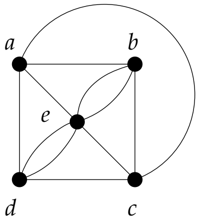
d) $v_1 e_1 v_2 e_2 v_3 e_4 v_4 e_5 v_5 e_6 v_6 e_7 v_7 e_9 v_8$.

2. Consider the following map showing several cities and the roads connecting them. Is it possible for a travelling salesman to find a route which passes through each of the cities exactly once (not necessarily using all the roads) and end up where he started? Is it possible for the travelling salesman to pass through all the cities using all of the roads exactly once? Explain your answers.

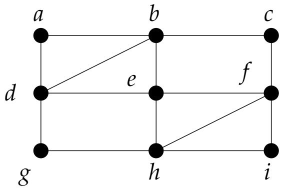


3. **Königsberg bridge problem.** Consider Section 11.1, Question 11. Is it possible to take a walk around Königsberg in such a way as to cross each of the seven bridges exactly once? Explain your answer.

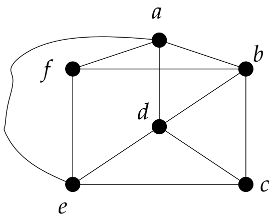
4. Determine whether each of the following graphs has an Euler circuit. For each graph that does have an Euler circuit, write out the circuit. For each graph which does not have an Euler circuit, determine whether the graph has an Euler path, and if it does, write out the Euler path.



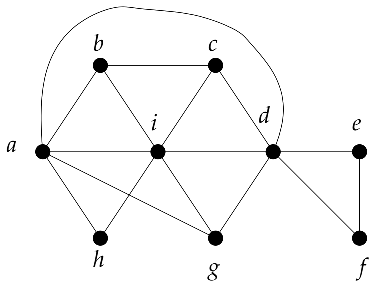
(I)



(II)



(III)



(IV)

Special Points

- Most graph theory textbooks use the term "cycle" for an *undirected* closed walk with no repeated vertices or edges, and the term "circuit" for a *directed* closed walk with no repeated vertices or edges.

Checklist

Ensure that you understand:

- the definition of a walk, a closed walk, a path, a simple path, a circuit and a simple circuit;
- the definition of a connected graph, an Euler circuit and an Euler path;
- the relationship between an Euler circuit in a graph and the parity of the degree of each vertex.

Section 11.3

Matrix Representations of a Graph

There are many useful ways to represent graphs. In this section we shall show how to represent graphs by matrices. We shall only be covering the beginning of this section in the textbook.

Exercise 11.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let G be an (undirected) graph with vertices $v_1, v_2, \cdots, v_n$ in the given order. The **adjacency matrix of** G is the matrix $A = [a_{ij}]$ over the set of nonnegative integers such that

   $a_{ij} =$ ____

   for all $i, j = 1, 2, \cdots, n$.

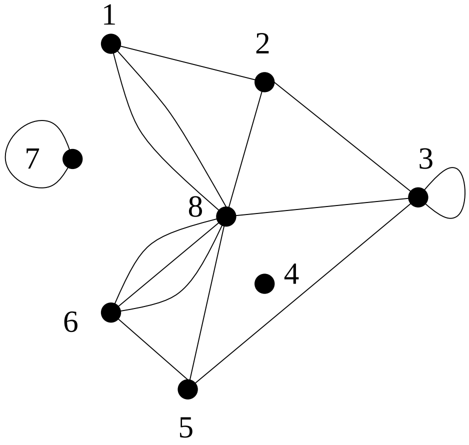
   In other words, the adjacency matrix of G is the matrix $A = [a_{ij}]$ over the set of nonnegative integers such that

$$a_{ij} = \begin{cases} \underline{\hspace{2em}} & \text{if there exist } r \text{ edges connecting } v_i \text{ and } v_j \\ \underline{\hspace{2em}} & \text{otherwise} \end{cases}$$

Exercise 11.3.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

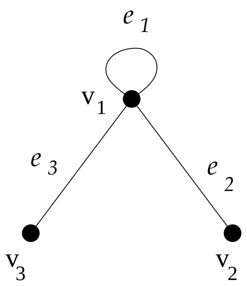
1. Find the adjacency matrix for the following graph.



2. Another useful way of describing a graph is by using an *incidence matrix.* Let G be a graph with vertex set $V(G) = \{v_1, v_2, \ldots, v_r\}$ and edge set $E(G) = \{e_1, e_2, \ldots, e_s\}$. An **incidence matrix** for the graph G is a matrix $N = (n_{i,j})$, of size $r \times s$, with a row corresponding to each vertex of the graph and a column corresponding to each edge of the graph. The entries, $n_{i,j}$, of the incidence matrix for graph G are

$$n_{i,j} = \begin{cases} 2 & \text{if edge } e_j \text{ is a loop on vertex } v_i, \\ 1 & \text{if edge } e_j \text{ is an edge connecting vertex } v_i \text{ to some other vertex,} \\ 0 & \text{otherwise.} \end{cases}$$

Find the incidence matrix for the following graph.



3. Use incidence matrices to prove that for any graph G with vertices $v_1, v_2, \ldots, v_n$ and e edges,

$$\sum_{i=1}^{n} \mathrm{d}eg(v_i) = 2e.$$

Checklist

Ensure that you understand:

- the definitions of adjacency and incidence matrices for a graph.

Section 11.5

Trees

A connected simple graph that contains no simple circuits is called a tree. Trees were used as long ago as 1857, when the English mathematician Arthur Cayley used them to count certain types of chemical compounds. Since that time, trees have been employed to solve problems in a wide variety of disciplines.

Exercise 11.5.1: Definitions

Fill in the blanks to complete the following sentences.

1. A graph is said to be **circuit-free** if, and only if, ____________________

   ____

   A graph is called a **tree** if, and only if, it is ____________________

   ____

   A **trivial tree** is a graph that consists of ____________________.

   A graph is called a **forest** if, and only if, ____________________.

   Hence a forest is a (not necessarily connected) graph which may be thought of as a union of trees.

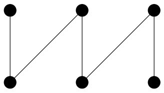
2. **Theorem** Let n be a positive integer and G a tree on n vertices. Then G has ____________________ edges.

3. A finite connected simple graph G with n vertices is tree if, and only if, it has exactly ____________________ edges.

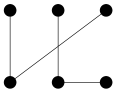
Exercise 11.5.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

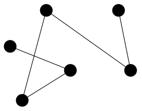
1. Which of the following graphs are trees?



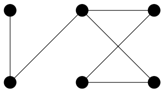
(I)



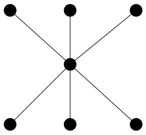
(II)



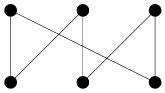
(III)



(IV)



(V)



(VI)

2. Which complete bipartite graphs $K_{m,n}$, where m and n are positive integers, are trees?

3. A tree has precisely five vertices of degree 1 and one vertex of degree 5.

a) Find the degrees of all the vertices in this tree.

b) Draw any two such trees, one with eight vertices and one with six vertices.

Checklist

Ensure that you understand:

- the definition of tree and forest.

Have you achieved the Chapter 11 Learning Objectives listed on page 98?

Chapter Ten

Relations

Every day we deal with items which are related to each other in some way. Examples of this include the relationships between a business and its telephone number, between an employee and his or her salary, and between a person and his or her cousin. In mathematics we also study relationships, including examples such as the relationship between two integers where one integer divides the other, or the relationship between two real numbers when one number is greater than the other. In this chapter we investigate the properties which are used to classify relations on sets.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- work with relations on sets;
- find the inverse of a relation;
- draw directed bipartite graphs (arrow diagrams) for relations;
- draw directed graphs for relations on a set A;
- distinguish between functions and relations;
- determine whether a relation is an equivalence relation;
- find the equivalence classes for an equivalence relation;
- determine whether a relation is a partial order relation;
- determine whether a relation is a total order relation.

Section 10.1

Relations On Sets

In mathematics we are often interested in which elements of a set are related to other elements in the set. Examples of such relationships include: x is greater than y, and x divides y. In this section we formally define a relation on a set and introduce different ways to represent such a relation.

Exercise 10.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let A and B be any two sets. Recall that

$$A \times B = \{(a, b) \mid a \in A \text{ and } \underline{\hspace{3cm}}\}.$$

2. Let A and B be sets. A **(binary) relation** R from the set A to the set B is

____.

Given an ordered pair $(x, y) \in A \times B$, x is related to y by R, if, and only if, ______________________________________

The expression x is related to y by R can be abreviated as ____________

3. **Arrow diagram of a relation.** A relation R from a set A to a set B can be represented by a directed bipartite graph G. The edge set of G is defined as follows, for all $x \in A$ and $y \in B$:

$$\exists \text{ a directed edge from } x \text{ to } y \iff \underline{\hspace{3cm}} \iff \underline{\hspace{3cm}}.$$

4. A function $F : A \to B$ is a relation from the set A to the set B that satisfies the following two properties:

(i) $\forall x \in A$, ______________________________________

____

(ii) $\forall x \in A$ and $\forall y, z \in B$,

____

If F is a function from A to B, we write ____________________

5. Let R be a relation from A to B. The **inverse relation** R^{-1} from B to A is defined as follows:

   ____.

6. A **binary relation on a set** A is ____________________________.

7. If a binary relation R is defined on a set A, then we can represent R using a directed graph G with vertex set A (no longer a bipartite graph). The edge set of G is defined as follows: for all $x, y \in A$,

   $\exists$ a directed edge from x to y $\iff$ __________ $\iff$ __________.

   Note that the directed edges are represented as ordered pairs (x, y) and if the element x is related to itself, then the directed graph G will have a ____________ at the vertex x.

Exercise 10.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Let $A = \{0, 2, 4\}$ and $B = \{1, 2, 3, 4\}$.

a) The Cartesian product $A \times B$ consists of the ordered pairs $(0, 1)$, $(0, 2)$, ___

____

____.

b) Now for $x \in A$ and $y \in B$ (A and B as above) we say that x is related to y, $x\ R\ y$, if, and only if, $x \leq y$.

$0\ R\ 2$ since ________________

$2\ R\ 4$ since ________________

________________ since $2 \leq 3$

________________ since $2 \leq 2$

________________ since $4 > 3$

2. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{0, 2, 4, 6, 8\}$. Suppose ρ is a relation from A to B which is defined as follows. Write down the elements of ρ.

(i) $x \,\rho\, y \iff x \geq y$.

(ii) $x \,\rho\, y \iff x = y$.

(iii) $x \,\rho\, y \iff x - y$ is even.

(iv) $x \,\rho\, y \iff x + y = 7$.

3. Define three different relations from the set of integers $\mathbb{Z}$ to the set of natural numbers $\mathbb{N}$. (There are many, many answers here, so be creative.)

4. Consider the following relations on $\mathbb{Z}$:

(i) $R_1 = \{(a, b) \mid a \leq b\}$;

(ii) $R_2 = \{(a, b) \mid a > b\}$;

(iii) $R_3 = \{(a, b) \mid a = b \text{ or } a = -b\}$;

(iv) $R_4 = \{(a, b) \mid a = b\}$;

(v) $R_5 = \{(a, b) \mid a = b + 1\}$;

(vi) $R_6 = \{(a, b) \mid a + b \leq 3\}$.

Consider each of the following pairs in turn and state to which of the six relations above the pair belongs: $(1, 1)$, $(1, 2)$, $(2, 1)$, $(1, -1)$, and $(2, 2)$.

5. Let $A = \{1, 3, 5\}$ and $B = \{1, 2, 3, 4\}$. Draw a directed bipartite graph to illustrate the relation S from A to B where: $(x, y) \in S \iff x + 1 > y$.

6. Let $A = \{3, 6, 9\}$ and $B = \{2, 4, 6, 8\}$. Let $R = \{(3, 2), (6, 2), (9, 6), (6, 8)\}$ be a relation. Is R a function from A to B? Explain your answer.

7. Let $A = \{x, y, z\}$ and $B = \{1, 4, 7, 10\}$. Suppose that

$$R = \{(x, 4), (x, 10), (z, 1), (y, 7), (y, 1)\}$$

is a relation from A to B. List the elements of R^{-1}.

8. Let $A = \{1, 2, 3, \cdots, 10\}$ and define a binary relation R on A as follows:

$$\forall x, y \in A, \quad x\ R\ y \iff 3 \mid (x - y).$$

a) Write down the elements of R.

b) Write down the elements of R^{-1}. Is $R = R^{-1}$?

Special Points

- A relation from A to B is any subset of the Cartesian product, $A \times B$, of A and B. (This includes the subset $\emptyset$ and the subset $A \times B$, as well as *all* other subsets of $A \times B$!)
- A function from A to B is also a relation from A to B. But beware: not all relations from A to B are necessarily functions!

Checklist

Ensure that you understand:

- the definition of a relation from a set A to a set B;
- the definition of a function;
- the definition of the inverse relation of any relation;
- how to construct the directed bipartite graph for a relation from a set A to a set B;
- how to construct the directed graph for a relation on a set A.

Section 10.2

Reflexivity, Symmetry and Transitivity

There are several properties that are used to classify relations on a set. The properties which we investigate in this section are reflexivity, symmetry and transitivity. We shall see how to identify these properties from the set notation as well as from the directed graph of the relation.

Exercise 10.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let R be a binary relation on a set A.

   (i) R is **reflexive** if, and only if, for all $x \in A$ ______________________

   In terms of the directed graph for the relation R, saying that R is **reflexive** is equivalent to saying that there is a __________ at each vertex of the graph.

   If R is specified as a list of ordered pairs, then R is **reflexive** if, and only if, the ordered pair __________ is an element of R, for all $x \in A$.

   (ii) R is **symmetric** if, and only if, for all $x, y \in A$, _________________

   In terms of the directed graph for the relation R, saying that R is **symmetric** is equivalent to saying that whenever the directed edge (u, v) is in the graph, then the directed edge __________ is also in the graph.

   If R is specified as a list of ordered pairs, then R is **symmetric** if, and only if, whenever $(x, y) \in R$ then the ordered pair __________ also belongs to R.

   (iii) R is **transitive** if, and only if, for all $x, y, z \in A$, _________________

   In terms of the directed graph for the relation R, saying that R is

transitive is equivalent to saying that whenever the directed edges (u, w) and (w, v) are in the graph, then the directed edge __________ is also in the graph.

If R is specified as a list of ordered pairs, then R is **transitive** if, and only if, whenever $(x, y) \in R$ and $(y, z) \in R$ then the ordered pair __________ also belongs to R.

2. Let R be a binary relation on a set A.

   (i) R is **not reflexive**, if, and only if, there exists an element a in A ____.

   (ii) R is **not symmetric**, if, and only if, there exist elements a and b in A ____

   ____.

   (iii) R is **not transitive**, if, and only if, there exist elements a, b and c in A ____

   ____.

3. In the directed graph for a relation, if at least one vertex does not have a loop, then the relation is not ______________ (unless the relation is $\emptyset$).

4. R is the **identity relation on** A if, and only if,

$$\forall x, y \in A, \quad x \; R \; y \iff x = y.$$

   The identity relation is also the ______________ function.

Exercise 10.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Consider the following relations on the set $\{1, 2, 3, 4\}$.

- $R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$
- $R_2 = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$
- $R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$
- $R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$
- $R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$
- $R_6 = \{(1,1), (2,2), (3,3), (4,4)\}$.

For each of the relations R_1, R_2, R_3, R_4, R_5 and R_6, determine if the relation is reflexive, symmetric and/or transitive.

2. Is the "divides" relation R, where $a\ R\ b \iff a \mid b$, on the set of positive integers: i) reflexive? ii) symmetric? iii) transitive?

3. Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and define a relation R on A as follows:

$$\forall x, y \in A, \quad x \, R \, y \iff 3 \mid (x - y).$$

Draw the directed graph of R and use it to check whether R is reflexive, symmetric and/or transitive. (Note that you have already written out the elements of this relation in Section 10.1, Question 8 so use that to draw the graph.)

4. Define a relation σ on $\mathbb{R}$ (the set of all real numbers) as follows: for all $x, y \in \mathbb{R}$,

$$x \, \sigma \, y \iff x > y.$$

a) Is σ reflexive?
b) Is σ symmetric?
c) Is σ transitive?
Justify your answers.

5. Define a relation ρ on $\mathbb{Z}\times(\mathbb{Z}\backslash\{0\})$ as follows: for all $(a,b),(c,d)\in\mathbb{Z}\times(\mathbb{Z}\backslash\{0\})$,

$$(a,b)\ \rho\ (c,d) \quad\Longleftrightarrow\quad \frac{a}{b}=\frac{c}{d}.$$

a) Is ρ reflexive?

b) Is ρ symmetric?

c) Is ρ transitive?

6. Prove that if a relation R is reflexive then R^{-1} is also reflexive.

7. Prove that a relation R is symmetric if and only if $R = R^{-1}$.

8. For the relation R, is the statement "If R is transitive then R^{-1} is transitive" true or false? Justify your answer.

Checklist

Ensure that you understand:

- the definition of reflexive relations, symmetric relations and transitive relations;

Section 10.3

Equivalence Relations and Equivalence Classes

In this section we discover the idea of equivalence relations. The central idea of equivalence relations is that of grouping together things that "look different but are really the same". Pay particular attention to:

- the definition and discussion of equivalence classes;
- examples involving congruence modulo k, for some interger k.

Exercise 10.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. Recall that a **partition of a set** A is a collection of ____________________
____.

2. Given a partition $\{A_1, A_2, \ldots, A_n\}$ of a set A the **binary relation** R **induced by the partition** is defined on A as follows: for all $x, y \in A$, $x\ R\ y$, if, and only if, ____

3. **Theorem:** Given a partition $\{A_1, A_2, \ldots, A_n\}$ of a set A and a binary relation R induced by the partition. Then R is relexive, ________________

4. Let A be a nonempty set and R a binary relation on A. R is an **equivalence relation** if, and only if, ________________________________

5. Let A be a nonempty set and R is an equivalence relation on A. For each element a in A, the ____________________________ of a, denoted $[a]_R$, is the set of elements x in A such that ____________________________. Hence $[a]_R = \{x \in A \mid x\ R\ a\}$.

6. Let A be a nonempty set and R is an equivalence relation on A. The distinct equivalence classes of R form a partition of A. Hence A is equal

to ____

____, and

for any two distince equivalence classes $[a]_R$ and $[b]_R$ ____________

7. Let m and n be integers and let d be a positive integer. Recall the notation ______________ reads "m is congruent to n modulo d" and is equivalent to ______________________________

   Hence,

   $$m \equiv n \pmod{d} \quad \text{if, and only if,} \quad \underline{\hspace{4cm}}.$$

   The relation R where $m\ R\ n$ if, and only if, m is congruent to n modulo d is an equivalence relation for all integers m and n and positive integers d. You will be asked to find the equivalence classes for R later in this section.

Exercise 10.3.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Let $A = \{1, 3, 5, 7, 9, 11, 13\}$ and consider the following partition of A:

$$\{1, 5, 9\}, \quad \{3, 7, 13\}, \quad \{11\}.$$

List the elements of the relation R induced by this partition.

2. Let $A = \{0, 1, 2, 3, 4\}$ and define a relation R on A as follows:

$$\begin{aligned} R \;=\; & \{(0,0), (2,1), (0,3), (1,1), (3,0), (1,4), (4,1), \\ & (2,2), (2,4), (3,3), (4,4), (1,2), (4,2)\}. \end{aligned}$$

a) Draw the directed graph for R.

b) Use the directed graph for R to check whether R is an equivalence relation.

c) If R is an equivalence relation, use the graph to list the partition of the set A which induces the relation R and to list the equivalence classes of R.

3. Which of the relations in Section 10.2, Question 1 are equivalence relations? For each relation which is an equivalence relation, draw the directed graph and then use the graph to list the partition of the set $\{1, 2, 3, 4\}$ and to list the equivalence classes for that relation.

4. Define the relation ρ on the set of integers $\mathbb{Z}$ as follows: for all m and n in $\mathbb{Z}$

$$m \, \rho \, n \iff 7 \mid (m-n).$$

a) Prove that ρ is an equivalence relation.

b) Find the equivalence classes for ρ.

c) Refer to the equivalence classes from part b) to determine which of the following statements are correct? Explain your answers.

(i) $[1] = [-8]$; (ii) $[1] = [8]$; (iii) $[123] = [319]$;
(iv) $[304] = [-10]$; (v) $[-34] = [-6]$.

5. Let

$$\begin{aligned} A_0 &= \{\ldots, -10, -5, 0, 5, 10, 15, 20, 25, \ldots\} \\ A_1 &= \{\ldots, -9, -4, 1, 6, 11, 16, 21, 26, \ldots\} \\ A_2 &= \{\ldots, -8, -3, 2, 7, 12, 17, 22, 27, \ldots\} \\ A_3 &= \{\ldots, -7, -2, 3, 8, 13, 18, 23, 28, \ldots\} \\ A_4 &= \{\ldots, -6, -1, 4, 9, 14, 19, 24, 29, \ldots\}. \end{aligned}$$

a) Prove that A_0, A_1, A_2, A_3, and A_4 partition the set of integers $\mathbb{Z}$.

b) Find the relation σ induced by this partition.

6. Let d be a positive integer. Define the relation ρ on the set of integers $\mathbb{Z}$ as follows: for all m and n in $\mathbb{Z}$

$$m \;\rho\; n \quad \Longleftrightarrow \quad m \equiv n \pmod{d}.$$

(Recall that $m \equiv n \pmod{d}$ if and only if $d \mid (m - n)$.)

a) Prove that ρ is an equivalence relation.

b) List the equivalence classes for ρ.

Special Points

- Let ρ be an equivalence relation on a set A. The equivalence class containing the element a is a subset of A. It contains all the elements of A that are related to a, that is,

$$[a] = \{x \in A \mid a \; \rho \; x\}.$$

- Let R be a relation on $\mathbb{Z}$ such that xRy if, and only if, $x \equiv y \bmod n$, for some positive integer n. Then R partitions $\mathbb{Z}$ into n equivalence classes, $[0], [1], \ldots, [n-1]$. This set of equivalences classes is denoted $\mathbb{Z}_n$, and is often abbreviated to the set $\mathbb{Z}_n = \{0, 1, \ldots, (n-1)\}$.

Checklist

Ensure that you understand:

- the definition of an equivalence relation;
- the definition of an equivalence class for an equivalence relation;
- the relation induced by a partition on a non-empty set A.

Section 10.5

Partial Order Relations

In this section we are introduced to another useful property which a relation may have, that of antisymmetry. A relation which is reflexive, antisymmetric and transitive is called a partial order relation.

Exercise 10.5.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let R be a relation on a set A. R is said to be **antisymmetric** if, and only if,____

   ____.

2. In terms of the directed graph for a relation on a set A, saying that a relation is antisymmetric is the same as saying that whenever there is a directed edge going from vertex a to another distinct vertex b, __________

   ____.

3. Let R be a binary relation defined on a set A. R is said to be **partial order relation** if, and only if, ___________________________

   ____.

4. Let R be a partial order relation on a set A. R is a **total order relation** on A if ____

   ____.

Exercise 10.5.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further

questions, please email your lecturer or post your question to the discussion group.

1. For each of the following relations on the set $A = \{1, 2, 3, 4\}$, decide whether it is antisymmetric. Justify your answers using the directed graph for each relation.

a) $R_1 = \{(1, 1), (2, 2), (2, 3), (2, 4), (4, 4), (3, 3), (3, 4)\}$.

b) $R_2 = \{(1, 2), (2, 3), (3, 4)\}$.

c) $R_3 = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$.

2. Determine whether the relation R on the set of all people is reflexive, antisymmetric, and/or transitive, where for any two people a and b $(a, b) \in R$ if and only if:

a) a is taller than b.

b) a and b were born on the same day.

3. For each of the following relations, determine if the relation is reflexive, symmetric, antisymmetric and/or transitive. Then classify the relation as a partial order relation, an equivalence relation or neither.

a) $(x, y) \in R$ if, and only if, $xy \geq 1$ where x and y are integers.

b) $(x, y) \in R$ if, and only if, x is a multiple of y where x and y are positive integers.

c) $(x, y) \in R$ if, and only if, $x \equiv y \pmod{13}$ where x and y are integers.

4. a) List all the 16 relations on $\{0, 1\}$. Hint: A relation on $\{0, 1\}$ is a subset of

$$\{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

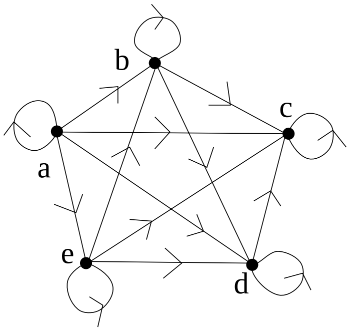
b) Which of the 16 relations on $\{0, 1\}$, which you listed in part a) are partial order relations.

5. Let $A = \{1, 2, 3, 4\}$ and define the relation ρ on the power set of A, $\mathcal{P}(A)$, as follows: for $X, Y \in \mathcal{P}(A)$,

$$X \; \rho \, Y \quad \Longleftrightarrow \quad X \subset Y \;\text{ or }\; X = Y.$$

Show that ρ is a partial order relation.

6. The partial order relation R is described by the following directed graph.



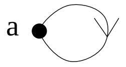
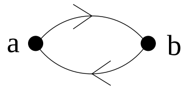
Is R a total order relation on $\{a, b, c, d, e\}$? Justify your answer.

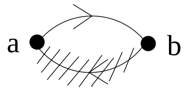
7. a) Is the relation R defined in Question 5 a total order relation on the set $A = \{1, 2, 3, 4\}$?

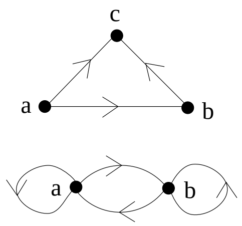
b) What if R were defined in the same way on $\mathcal{P}(B)$ where $B = \{1\}$?

Special Points

- A total order relation on A is also a partial order on A. That is, a total order relation is a partial order relation in which every pair of elements of A is comparable.
- The following table summarizes some of the definitions of the properties of a relation R on a set A:

Property	Description	
	in Logic	in Graphs
Reflexivity	$\forall a \in A, \;\; a \; R \; a.$ $\forall a \in A, \;\; (a, a) \in R.$	
Symmetry	$\forall a, b \in A, \quad$ if $a \; R \; b$ then $b \; R \; a.$ $\forall a, b \in A, \quad$ if $(a, b) \in R$ then $(b, a) \in R.$	

Antisymmetry	$\forall a, b \in A,$
	if $a \; R \; b$ and $b \; R \; a$ then $a = b.$
	$\forall a, b \in A,$
	if $(a, b) \in R$ and $(b, a) \in R$ then $a = b.$
		

Transitivity	$\forall a, b, c \in A,$
	if $a \; R \; b$ and $b \; R \; c$ then $a \; R \; c.$
	$\forall a, b, c \in A,$
	if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R.$
		

Checklist

Ensure that you understand:

- the definition of an antisymmetric relation;
- the definition of partial order and total order relation.

Have you achieved the Chapter 10 Learning Objectives listed on page 123?

Chapter Seven

Functions

Functions are everywhere in mathematics. You have already encountered many functions in this course including truth tables, sequences, mod, div, floor and ceiling. Functions, roughly speaking, give a relationship between two sets of objects. Sometimes functions satisfy special properties and these properties will be discussed in this chapter.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- identify the domain, co-domain and range of a function;
- determine whether a relationship between two sets is a well-defined function;
- describe a function using a formula or arrow diagram;
- determine whether two functions are equal;
- use a transition diagram and a next–state table to describe a finite–state automaton;
- find the language accepted by a finite–state automaton;
- evaluate the eventual–state function for a finite–state automaton;
- determine whether a function is one–to–one or onto;
- find the inverse of a function;
- apply the pigeonhole principle and the generalized pigeonhole principle to solve problems;
- find the composition of two functions using formulae and using arrow diagrams;
- describe a set as finite, infinite, countable or uncountable.

Section 7.1

The Definition of a Functions

Roughly speaking, given two sets of objects, a function is a relationship which associates each element of the first set with *precisely one* element of the second set. In this section we see how to describe a function using a formula or an arrow diagram.

Exercise 7.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. A **function f from a set $\mathcal{X}$ to a set $\mathcal{Y}$** is ____________________

   ____

   ____

   ____

2. The notation $f : \mathcal{X} \to \mathcal{Y}$ is read ____________________

   ____

3. The definition of a fuction $f : \mathcal{X} \to \mathcal{Y}$ states that given an element x in $\mathcal{X}$, there is a unique element y in $\mathcal{Y}$ that is related to x. We write $y = f(x)$, read ____.

   We say x is mapped under f to y or we say f ____________ x to y and write ____________ or $x \to f(x)$.

   We can think of x as the ________ and y as the related ________.

   Equivalently, the **value of** f at x is denoted ________________

   and **the image of** x under f is denoted ________________.

4. The **domain** of the function f is the set ________________ and the **co-domain** of the function f is the set ________________

5. The **range** of a function $f : \mathcal{X} \to \mathcal{Y}$ is set of $y \in \mathcal{Y}$ such that $y = f(x)$ for some $x \in \mathcal{X}$. Symbolically the range of f is:

   ____

6. Given a function $f : \mathcal{X} \to \mathcal{Y}$ and an element $y \in \mathcal{Y}$, the **inverse image of** y is the set of all elements $x \in \mathcal{X}$ such that $f(x) = y$. Symbolically the inverse image of y is:

   ____

7. An arrow diagram for a function has the following two properties:

   1. ____

   2. ____

   ____

8. Suppose f and g are functions from a set $\mathcal{X}$ to a set $\mathcal{Y}$. Then f **equals** g, written $f = g$, if, and only if, ____________________________

9. The special function ι_X from the set X to X is called the __________ and for all $x \in X$, $\iota_X(x) =$ ______________________________

10. Previously we said that a sequence was a list of elements. More formally, a sequence is ____________________________________

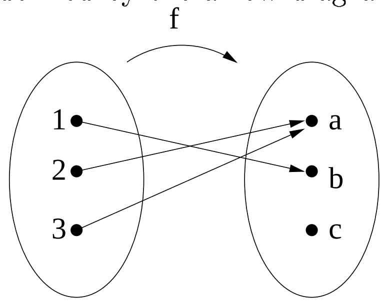
    ____

    ____

Exercise 7.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Let f be the function defined by the arrow diagram below:



a) Write down the domain and co-domain of f. ____________________

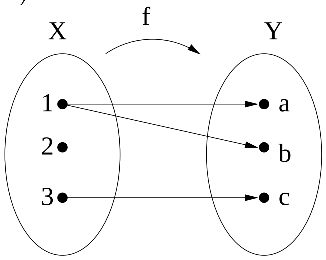
b) Find $f(1)$, $f(2)$ and $f(3)$. ______________________________

c) What is the range of f? ______________________________

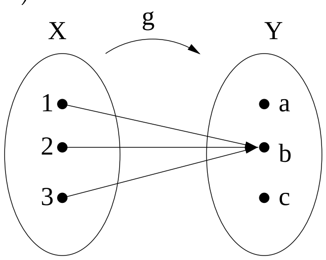
d) Find the inverse images of a, b and c. ____________________

2. Which of the following define functions? Explain your answer.

a)



b)



3.a) Define functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$, where $f(x) = x$ for all $x \in \mathbb{R}$ and $g(x) = \sqrt[3]{x^3}$ for all $x \in \mathbb{R}$. Is $f = g$? Explain your answer.

b) Define functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$, where $f(x) = x$ for all $x \in \mathbb{R}$ and $g(x) = \sqrt{x^2}$ for all $x \in \mathbb{R}$. Is $f = g$? Explain your answer.

4. Write the sequence $-4, 9, -16, 25, \ldots$ as a function.

5. Use the Hamming distance function to calculate $H(1100101, 0010111)$.

6. A **binary operation** on a set X is a special kind of function from $X \times X$ to X. One example of a binary operation is addition on the set $\mathbb{Z}$. Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be the function of addition on the integers.

a) Evaluate $f((3, 2))$.

b) Find an element of $\mathbb{Z} \times \mathbb{Z}$ with an image of -1.

7. Suppose you are told that a function $f : \mathbb{Q} \to \mathbb{Z}$ is to be defined by the formula $f(\frac{m}{n}) = n$ for all integers m and n where $n \neq 0$. Is f well-defined? Justify your answer.

Checklist

Ensure that you understand:

- the definitions of function, domain, co-domain, range, inverse image;
- how to describe a function using a formula, an arrow diagram and a sequence;
- how to determine whether two functions are equal;
- how to determine whether a given function is well-defined.

Section 7.2

One-to-One and Onto, Inverse Functions

In this section we investigate two important properties which functions may satisfy: one–to–one and onto. When a function is both one–to–one and onto, we can define an inverse function which reverses the action of the function. Pay particular attention to:

- how to show a function is one–to–one or onto.

Exercise 7.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let F be a function from a set X to a set Y. F is **one–to–one** (or injective) if, and only if, for all elements x_1 and x_2 in X, ________________

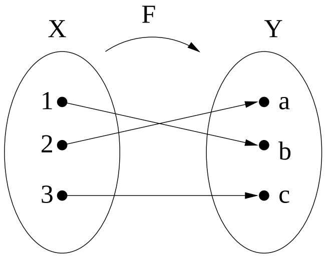
   ____

   The contrapositive statement is: ________________________

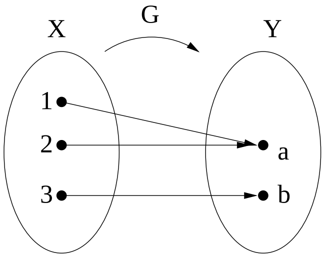
   ____

2. A function $F : X \to Y$ is **not one–to–one** if, and only if, ________________

   ____



F is one-to-one



G is not one-to-one

3. To show that a function $f : X \to Y$ is one–to–one, you usually suppose that ____

   and show that ____

4. To show that a function $f : X \to Y$ is not one–to–one, you usually find

____

5. Let F be a function from a set X to a set Y. F is **onto** (or surjective) if, and only if, $\forall y \in Y$, $\exists x \in X$ such that ____________________

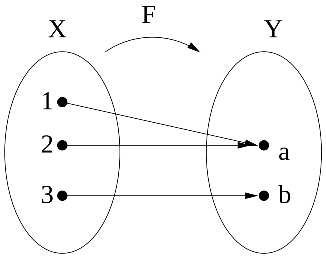
____

That is, for all $y \in Y$ there exists and $x \in X$ such that y is the image of

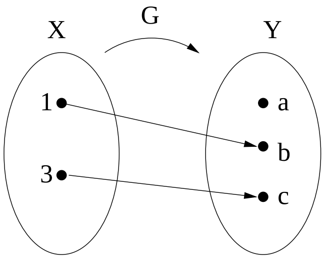
____

6. A function $F : X \to Y$ is **not onto** if, and only if, ____________

____



F is onto



G is not onto

7. To show that a function $f : X \to Y$ is onto, you usually suppose that

____

and show that ______________________________

8. To show that a function $f : X \to Y$ is not onto, you usually find ______

____

9. A **one–to–one correspondence** (or bijection) from a set X to a set Y is ________________________________

____

10. Suppose that the function $F : X \to Y$ is both one–to–one and onto; that is, F is a one–to–one correspondence from X to Y. Then there exists a function $F^{-1} : Y \to X$ such that for any element y in Y,

    $F^{-1}(y) =$ ____

    The function F^{-1} is called the ____________________________ for F.

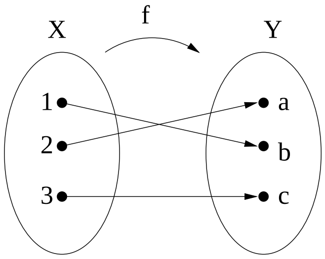
11. Given a function $F : X \to Y$, for which there exists an inverse function $F^{-1} : Y \to X$. Then

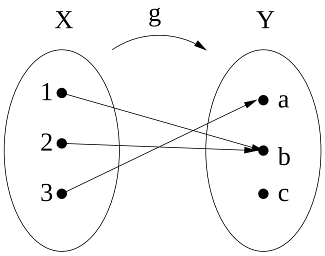
    $F^{-1}(y) = x \quad \leftrightarrow$ ______________________________________

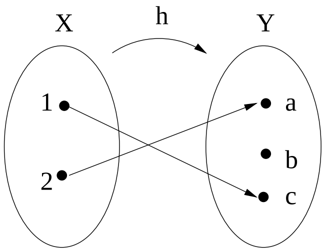
Exercise 7.2.2: Examples

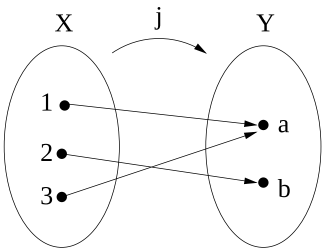
Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Which of the following functions are one-to-one? Which of them are onto?









2. Define the functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ by $f(x) = |x| + 1$ and $g(x) = 2x^3 - 1$, for all $x \in \mathbb{R}$. Are these functions one–to–one? In each case either prove that the function is one–to–one or give a counterexample to show that it is not one–to–one.

3. Searching through long lists is a slow process. One way to speed up the search is to divide the long list into a number of smaller lists. If we have some method of quickly identifying in which of the smaller lists a particular item will appear, then we need only search through the smaller list to find the item.

Suppose we wish to maintain the customer records for a large company and begin by assigning each customer a unique 7–digit account number. This 7–digit number will be used as input to a function H which will determine the sublist to be searched to find the account details. The company has 30,000 customers and we are going to partition the list of accounts into 100 sublists of approximately 300 items each. We define a hash function which maps each 7–digit account number, say n, to an element x in the set $\{0, 1, 2, 3, \ldots, 99\}$, such that

$$H(n) = x, \quad \text{where } n \bmod 100 = x.$$

a) Calculate to which sublists each of the following account numbers would be allocated.
i) 2473871 ii) 3569842 iii) 9085000 iv) 8574642

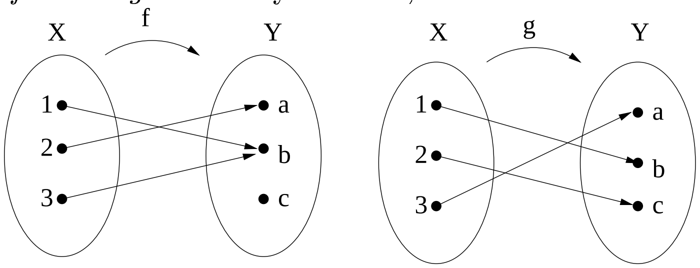
b) Is the function H one–to–one? Explain.

4. Define the functions $F : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$ and $G : \mathbb{Z} \to \mathbb{Z}$ by $F(x) = x^2$ for all $x \in \mathbb{R}$ and $G(x) = x^2$ for all $x \in \mathbb{Z}$. Are these functions onto? In each case either prove that the function is onto or give a counterexample to show that it is not onto.

5. Define the function $F : \mathbb{R} \to \mathbb{R}$ by $F(x) = 2x + 4$ for all $x \in \mathbb{R}$. Show that F is onto.

6. Is the function $f : \mathcal{X} \rightarrow \mathcal{Y}$ a one–to–one correspondence, where $\mathcal{X} = \{0, 1, 2, 3\}$ and $\mathcal{Y} = \{0, 1, 4, 9\}$ and $f(x) = x^2$ for all $x \in \mathcal{X}$? Justify your answer.

7. Given the functions f and g illustrated in the following arrow diagrams, find (if they exist) f^{-1} and g^{-1}. If they do exist, draw their arrow diagram.



8. Find (if it exists) the inverse of the function $g : \mathbb{R} \to \mathbb{R}$ where $g(x) = 2x + 5$ for all $x \in \mathbb{R}$.

Checklist

Ensure that you understand:

- the definitions of one–to–one, onto, one–to–one correspondence, and inverse functions;
- how to determine whether a function is one–to–one or onto;
- how to find the inverse of a function.

Section 7.3

The Pigeonhole Principle

If n pigeons flew into m pigeonholes and $n > m$, then at least one pigeonhole must contain two or more pigeons. This idea seems quite intuitive and it turns out to be extremely useful. Pay particular attention to:

- the applications of the pigeonhole principle and generalized pigeonhole principle.

Exercise 7.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. Recall for a set A, $n(A)$ denotes the number of elements in set A.

2. *Pigeonhole Principle*:

   A function, f, from the set X to the set Y, where $n(X) > n(Y)$, cannot be ________________________________

   ____

   ____

3. *Generalized Pigeonhole Principle*:

   Let k be a positive integer and f a function from a finite set $\mathcal{X}$ to a finite set $\mathcal{Y}$. If $n(\mathcal{X}) > k \cdot n(\mathcal{Y})$, then ________________________

   ____

4. A set is called **finite** if, and only if, it is ________________________

   ____

   ____

   In the first case, the **number of elements** in the set is ____________

   and in the second case it ____________________________

   A set that is not finite is ____________________________

5. *Pigeonhole Principle* For any function f from a finite set X to a finite set Y, if ____

____

6. **Theorem:** Let X and Y be finite sets with the same number of elements and suppose f is a function from X to Y. Then ____________________

____

Exercise 7.3.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. How many students must be in a class to guarantee that at least two students receive the same mark on the final exam which is graded on a scale of 0 to 100, (with no half marks allowed)?

2. There are 680 people on a list. Must there be at least two people on the list with the same first and last initials? Justify your answer.

3. The Prime Minister is packing to go to an important meeting in Asia, but there is a sudden black-out and so he is fumbling around in the dark. He is reaching into his wardrobe to find a tie to wear at the meeting. He has 12 ties, five ties that he likes and seven that he doesn't like. How many ties must he pull out of his wardrobe to be guaranteed of having at least one tie that he likes?

4. Show that in a group of 25 people, at least three must have the same astrological star sign.

5. Assume that in a group of six people, each pair of individuals are either friends or enemies. Show that there are either three mutual friends or three mutual enemies in the group.

Checklist

Ensure that you understand:

- how to apply both the pigeonhole principle and the generalized pigeonhole principle;
- the definitions of finite and infinite.

Section 7.4

Composition of Functions

To calculate the value of $\sqrt{2x+1}$ if you are told that $x = 4$, you would probably first calculate the value of $2(4) + 1$ and then you would find the square root of that result. This is an example of the *composition* of functions. Notice that the result of the first evaluation must be acceptable input to the second evaluation. In this case we would have run into trouble if the evaluation of $2x + 1$ had given us a negative number. In this section we investigate the composition of functions.

Exercise 7.4.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let $f : X \to Y$ and $g : Y \to Z$ be functions with the property that the range of f is a subset of the domain of g. Define a new function $g \circ f : X \to Z$ as follows:

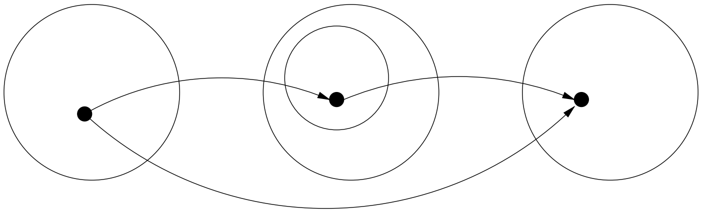
   ____

   The function $g \circ f$ is called the ______________________

   We read $g \circ f$ as "______________________"

   and $g(f(x))$ as "______________________".

   Label the following diagram to illustrate the function $g \circ f$.



2. **Theorem:** Let f be a one–to–one correspondence from a set X to a set Y. Then the inverse function exists and can be denoted by $f^{-1} : Y \to X$. It follows that

$f^{-1} \circ f =$ ____________________ and $f \circ f^{-1} =$ ____________________

Exercise 7.4.2: Examples

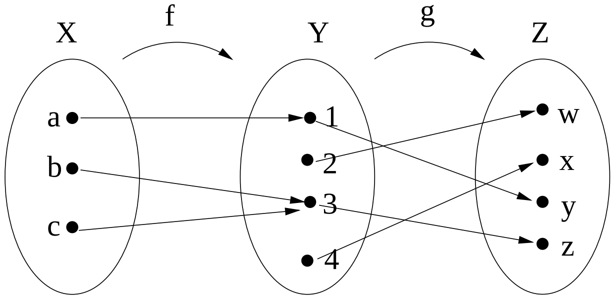
Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^3$ for all $x \in \mathbb{R}$ and let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = 2x - x^2$ for all $x \in \mathbb{R}$.

a) Find $(f \circ g)(x)$ and $(g \circ f)(x)$.

b) Is $g \circ f = f \circ g$?

2. Let $X = \{a, b, c\}$, $Y' = \{1, 2, 3\}$, $Y = \{1, 2, 3, 4\}$ and $Z = \{w, x, y, z\}$. Define the functions $f : X \to Y'$ and $g : Y \to Z$ by the diagram below.



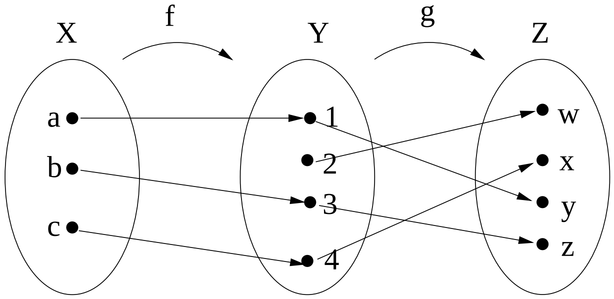
a) Draw the arrow diagram for $g \circ f$.
b) What is the range of $g \circ f$?

3. Suppose that $f : \mathbb{Z} \to \mathbb{Z}$ is a function where $f(x) = x + 1$ for all $x \in \mathbb{Z}$. Let $\iota_{\mathbb{Z}}$ be the identity function.

a) Find $(f \circ \iota_{\mathbb{Z}})(x)$ and $(\iota_{\mathbb{Z}} \circ f)(x)$.

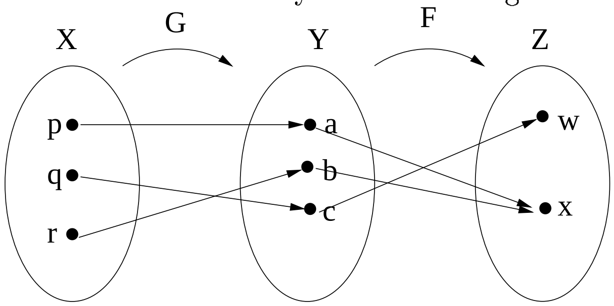
b) If $g : X \to X$ is any function, what can you say about the functions $g \circ \iota_X$ and $\iota_X \circ g$?

4. Let f and g be functions defined by the arrow diagrams below.



a) Draw the arrow diagram representing $g \circ f$.
b) f and g are both one–to–one. Is $g \circ f$ one–to–one?

5. Let F and G be functions defined by the arrow diagrams below.



a) Draw the arrow diagram representing $F \circ G$.
b) F and G are both onto. Is $F \circ G$ onto?

Special Points

- Students often confuse the order of the composition of functions. The composition of f and g is written $g \circ f$. In evaluating this you first find $f(x)$ then $g(f(x))$. And don't forget that in general $f(g(x)) \neq g(f(x))$.

Checklist

Ensure that you understand:

- how to find the composition of two functions using formulae and using arrow diagrams.

Section 7.5

The Cardinality of a Set (Extension Material)

Do all infinite sets have the same size, or are some infinite sets larger than others? Comparing the sizes of infinite sets can be troubling but it has important applications to determining what can and cannot be computed on a computer.

Exercise 7.5.1: Definitions

Fill in the blanks to complete the following sentences.

1. Recall that a **finite** set is ______________________________

   ____

   ____

   An **infinite** set is ______________________________

   ____

2. Let A and B be any sets. Sets A and B are said to have **the same cardinality** if, and only if, ______________________________

   ____

   In other words, ______________________________

   ____

3. A set is said to be **countably infinite** if, and only if, ____________

   ____

   A set is said to be **countable** if, and only if, ________________

   A set that is not countable is said to be ____________________

4. Recall that a function from one finite set to another set of the same size is one–to–one if, and only if, it is onto.

   This result does ______________ hold for infinite sets.

Exercise 7.5.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Show that the set of all odd integers is countable.

2. Show that there is no one–to–one correspondence between a set X and its power set $\mathcal{P}(X)$.

3. Verify that the set $\mathcal{P}(Z^+)$ is uncountable.

Checklist

Ensure that you understand:

- the definitions of finite, infinite, countable, uncountable, cardinality;
- how to show that a set is countable.

Section 12.2

Finite-State Automata

In this section we investigate simple sequential circuits. A sequential circuit is a circuit for which the output depends not only on the input but also on which state the circuit is in before receiving the input. The action of your telephone when you dial a 0 depends on what you have dialled previously. If you have previously dialled 00, you might get the emergency services, but if you have previously dialled 3365, the telephone will be in a waiting state as it expects more digits to be dialled.

Exercise 12.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. A **finite-state automaton** A consists of five objects:

   1. a set I, ____

   2. a set S of ____

   3. a designated state s_0, ________________________________

   4. a designated set of states ____________________________

   5. a next-state function $N : S \times I \to S$ that ____________________

      ____

      ____

      ____

2. A **(state-)transition diagram** is often used to describe the operation of a finite–state automaton. It shows ______________________________

   ____

3. A **next–state table** for an automaton shows __________________

   ____

4. Let A be a finite–state automaton and let I be the input alphabet. Let $\mathcal{I}$ denote the set of strings over the alphabet I, and let $w \in \mathcal{I}$; that is, let w be a string consisting of symbols chosen from the alphabet I. Then w **is accepted by** A if, and only if, ______________________________

____

____

5. Let A be a finite–state automaton with set of states S and input alphabet I. Let $\mathcal{I}$ denote the set of strings over the alphabet I and $N : S \times I \to S$ denote the next–state function. Then the **eventual–state function** $\mathcal{N} : S \times \mathcal{I} \to S$ is defined as follows:

   For any state s and for any input string w, $\mathcal{N}(s, w) =$ ______________

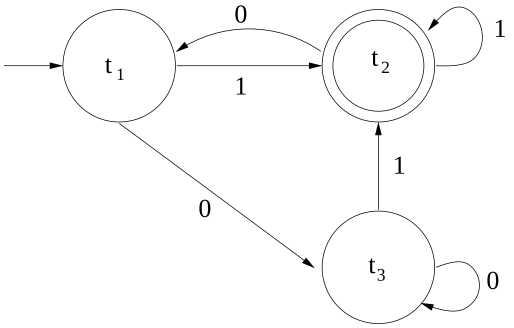
   ____

Exercise 12.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. A vending machine dispenses jaw-breakers that cost 20¢ each. The machine accepts 5¢, 10¢ and 20¢ pieces only and does not give change. As soon as the amount deposited equals or exceeds 20¢, the machine releases a jaw-breaker. The next coin deposited starts (from zero) the process over again.
Draw a transition diagram for this finite–state automaton.

2. Consider the finite–state automaton A defined by the transition diagram below:



a) What are the states of A? ____________________________

b) What are the input symbols of A? ____________________________

c) What is the initial state of A? ____________________________

d) What are the accepting states of A? ____________________________

e) Find $N(t_1, 1)$ and $N(t_3, 0)$. ____________________________

f) Create the annotated next–state table for A.

3. Consider the finite–state automaton A defined by the following next–state table:

		a	b	c	d
→	X	X	Y	Y	X
◎	Y	Y	Y	Y	X

a) What are the states of A? ____________________

b) What are the input symbols of A? ____________________

c) What is the initial state of A? ____________________

d) What are the accepting states of A? ____________________

e) Find $N(X, b)$ and $N(Y, a)$. ____________________

f) Draw the transition diagram for A.

4. Refer back to Question 2.

a) To which states would the automaton go for each of the following strings of input symbols?

i) 01 ________ ii) 0010 ________ iii) 11000 ________ iv) 111 ________

b) Which of the strings from part a) send the automaton to an accepting state?

____

c) What is the language accepted by this automaton?

5. Refer again to Question 2. Find $N^*(t_2, 00100)$.

Checklist

Ensure that you understand:

- the definition of a finite–state automaton and all its components;
- transition diagrams and next–state tables;
- how to find the language accepted by a given automaton;
- how to evaluate the eventual–state function for a given automaton.

Have you achieved the Chapter 7 Learning Objectives listed on page 151?

The Last Chapter

Groups and Fields

In this chapter we investigate algebraic structures which arise when we consider a set and one or two binary operations (such as addition or multiplication) which act on the elements of the set. Groups and fields may seem like very abstract ideas to you at first, but keep in mind that these structures have many important applications in coding theory and cryptography.

Since this chapter is not included in your textbook, a section of reading has been provided to give you the necessary information. Any page numbers referred to in this section are the page numbers in the reading.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- understand the definitions of group, abelian group, subgroup, cyclic group, generator and the order of an element;
- determine whether a given set and binary operation form a group or abelian group;
- determine whether a given group H is a subgroup of a given group G;
- find the order of the elements of a given group;
- understand the definition of a field.

Section G.1

Definitions and Examples of Groups

In this section we introduce the definitions of a *group*. Pay particular attention to:

- the four properties which characterize a group: Closure; Associativity; Identity; Inverse.

Exercise G.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. Recall from Chapter 7 that a **binary operation** is a special kind of function from $X \times X$ to Y.
2. A **group** $(G, *)$ is a set G together with a binary operation $*$ on G, such that:

   1. ____
   ____

   2. ____
   ____

   3. ____
   ____

   4. ____
   ____

3. For any element g belonging to the group $(G, *)$, the n^{th} **power of** g is given by ____ (where $*$ is the binary operation of the group).
4. In a group $(G, *)$ there exists one and only one identity element, e, such that ____

Similarly, for each $g \in G$ there exists one and only one inverse element, g^{-1}, such that ______________________________

5. If the operation of the group $(G, *)$ is ______________, then we say $(G, *)$ is an **abelian** group. That is, it must satisfy all four of the group properties, as well as: ______________________________

Exercise G.1.2: Examples

1. Does the set $\{0, 1\}$ and the binary operation multiplication form a group? Explain.

2. Show that $(\mathbb{Z}_7, \oplus)$, where $\oplus$ denotes addition modulo 7, is a group. You may like to refer back to the Special Points in Chapter 10, Section 10.3 for the definition of $\mathbb{Z}_7$.

3. Verify that $(\mathbb{Z}_6 - \{0\}, \times)$, where $\times$ denotes multiplication modulo 6, is not a group.

4. If p is prime, then every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$. Conversely, if every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$, then p is prime.

Proof (part 1) Suppose p is prime and consider $a \in \mathbb{Z}_p$, $a \neq 0$. Since $0 < a < p$, we know that $\gcd(a,p) = 1$, so we can use the Euclidean Algorithm to find integers x and y such that $ax + py = 1$. Thus $ax = 1 - py$, so $ax \equiv 1(\text{mod} p)$. Thus $[a]^{-1} = [x]$.

Reverse the above argument to complete rest of the proof.

Proof (part 2) Suppose that every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$.

5. Find the multiplicative inverses of each of the non-zero elements of $\mathbb{Z}_7$.

The multiplicative inverse of [2] is [4] because $[2] \times [4] = [8] = [1]$ since we are working modulo 7.

6. Prove that $(\mathbb{Z}_p - \{0\}, \times)$, where p is prime and × denotes multiplication modulo p, is a group.

7. Show that $(\mathbb{Z}, *)$, where $*$ is defined by $a * b = a + b + 2, \quad \forall a, b \in \mathbb{Z}$, is an abelian group.

Special Points

- The four words *Closure*, *Associativity*, *Identity* and *Inverse* can be used as a quick way of remembering the four conditions which a group must satisfy without memorising the exact wording of the definition. Make sure that you understand the meanings of these four words.

Checklist

Ensure that you understand:

- the definitions of a group and an abelian group;
- how to determine whether a given set and binary operation form a group or abelian group.

Section G.2

Elementary Properties of a Group

In this section we delve deeper into the properties of a group. We investigate groups within groups and special types of groups. Note that in the definitions and examples below, the symbol † indicates more challenging exercises and are extension material.

Exercise G.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let G be a group under the binary operation $*$. If a subset H of G is ____

   ____

   then H is said to be a **subgroup** of G. We denote this ______________

2. Let H be a subgroup of G. If H is not equal to the entire group G, then H is said to be a ______________________ of G. If H is not equal to $\{e\}$, we say that H is a ______________________ of G. The subgroup $\{e\}$ is said to be the ______________________ of G.

3. Let G be a group with binary operation $*$ and identity element e. A subset H of G is a subgroup of G if and only if:

   1. ______________________________ (identity);
   2. ______________________________ (inverse);
   3. ______________________________ (closure).

4† Let H be a subset of the group G. Then H is a subgroup of G if and only if ____

5. Let G be a group and a an element of G. Let $\langle a \rangle =$ ______________

   The set $\langle a \rangle$ forms a subgroup and is called the ______________________ of G generated by a. If ____________________ for some $a \in G$, then G is said to be **cyclic** and a is said to be a **generator** of G.

6. A group with a finite number of elements is said to be a ______________ otherwise it is an ________________________. A finite group G containing n elements is said to be of ________________________, written ______________ or ______________.

7. The **order of an element** g in G, written ______________, is defined to be ____ ____. If no such integer exists, then the order of the element is said to be ____________________

8. Let H be a subgroup of a group G and let g be an element of G. If $H = \{g^r \mid r \in \mathbb{Z}\}$, then ____________________

Exercise G.2.2: Examples

1. In each of the following cases, determine whether H is a subgroup of G. Justify your answers.

a) $H = \{0, 2, 4, 6, 8\}$; $G = (\mathbb{Z}_{10}, \oplus)$ (where $\oplus$ denotes addition modulo 10).

b) $H = (\mathbb{Z}_n, \oplus)$ (where $\oplus$ denotes addition modulo n);
$G = (\mathbb{Z}, +)$ (where $+$ denotes addition).

c) $H = \{x \in \mathbb{R} - \{0\} \mid x = 1 \text{ or } x \text{ is irrational }\}$ with the binary operation ×; $G = (\mathbb{R} - \{0\}, \times)$ (where × denotes multiplication in both cases).

2[†]. Let G be an abelian group with identity e. Use definition 4* to show that $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G.

3. Consider $(\mathbb{Z}_8, \oplus)$ where $\oplus$ denotes addition modulo 8. Find the cyclic subgroups generated by the elements [2] and [3]. What are $o(2)$ and $o(3)$? Is either of these elements a generator of $(\mathbb{Z}_8, \oplus)$?

4. A simple way of listing all the elements of a given finite group and their composition under the group operation is by using a **Cayley table**. A Cayley table for a group with n elements $g_1, g_2, \ldots, g_n$ is an $n \times n$ array with a headline and a sideline. The headline and sideline contain the elements of the group written in the same order. The entry in row i and column j of the body of the table is $g_i * g_j$ for all i, j, where $*$ is the binary operation of the group.

Consider the two groups given by the following Cayley tables. Notice that the second group is actually $(\mathbb{Z}_4, \oplus)$ where $\oplus$ denotes addition modulo 4.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

i) What are the orders of these two groups?

ii) What is the order of each element in each group?

iii) Does either group contain any nontrivial subgroups? If so, what are they?

iv) Is either of these groups cyclic? If so, name the generator(s).

Checklist

Ensure that you understand:

- the definitions of subgroup, proper subgroup, nontrivial subgroup and trivial subgroup;
- how to determine whether a given group H is a subgroup of a given group G;
- the definitions of cyclic subgroup, cyclic group and generator of a group;
- how to determine the order of a group and the order of an element;
- how to determine whether two groups are isomorphic.

Section G.3

Definitions and Examples of Fields

In this section we introduce the definitions of a *field.* Pay particular attention to:

- the three properties which characterize a field: Additive group under addition; Non–zero elements from an abelian group under multiplication; Multiplication distributes over addition.

Exercise G.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. A **field** $(F, +, *)$ is a set F together with two binary operation $+$ and $*$ on F, such that:

   1. ____

   ____

   2. ____

   ____

   3. ____

   ____

Exercise G.3.2: Examples

1. Verify that $(\mathbb{Q}, +, \cdot)$ is a field.

2. Verify that $(\mathbb{Z}_p, +, \cdot)$, where p is a prime, is a field.

3. Explain why $(\mathbb{Z}_6, +, \cdot)$ is not a field.

Chapter Six

Counting

Counting is a basic skill which most people acquire at an early age. Children often count the days until Christmas and students often count the number of school days left until the holidays.

> *"... and Christopher Robin knew that it was enchanted, because every time he tried to count the number of trees he could never tell if it was 63 or 64, even if he tied string around each tree as he counted them."*
>
> The Measurement Postulate as interpreted in Winnie-the-Pooh

The aspects of counting explored in this chapter are more involved than the simple counting of days. In this chapter we shall discover how to count the number of ways to perform a multi-step process, the number of ways to arrange a collection of distinct objects, the number of elements in two or three sets when the sets are and are not distinct, and the number of ways to choose a subset of elements from a larger set in which repetition of elements may or may not be allowed. We shall introduc special notation related to counting combinations of elements and make use of this notation in the Binomial Theorem.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- calculate the probability of an event occurring;
- compute the number of elements in a list;
- apply the multiplication rule or addition rule when appropriate;
- calculate the number of permutations and r-permutations of a set of objects;
- apply the Inclusion/Exclusion rule;
- calculate values of $\binom{n}{r}$;
- differentiate between problems for which the order objects are chosen is or is not important, and use appropriate techniques to solve the problems;
- use the $\binom{n}{r}$ notation in algebraic manipulations;
- apply the Binomial Theorem.

Section 6.1

Simple Counting and Probability

In this section you will be introduced to the terminology and notation used for basic probability. We shall also discuss how to determine the number of elements in a list.

Exercise 6.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. A process is said to be **random** if ______________________________

   ____

   ____

2. A **sample space** is ______________________________

   ____

3. An **event** is ______________________________

4. If S is a finite sample space in which all outcomes are equally likely and E is an event in S, then the **probability of** E, denoted __________, is

   ____

5. For any finite set A, $\boldsymbol{n(A)}$ denotes ______________________________

   ____

   An alternate notation for $n(A)$ is ______________________________

6. Let m and n be integers where $m \leq n$. Then there are __________ integers from m to n inclusive.

Exercise 6.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. In the game of *Two Up*, you bet on either heads or tails. Two coins are tossed. You win if both coins show the side you bet on, you lose if both coins show the opposite side you bet on. If the two coins show a combination of heads and tails, nothing happens (your bet stays as it was) and the coins are tossed again.

a) If this was the complete set of rules for Two Up, work out the probability that
i) you win on the first toss.
ii) you win if you are betting on heads (after the coins are tossed as many times as necessary to get either two heads or two tails).

b) There is an additional rule in Two Up. If the coin toss turns up a combination of a head and a tail five times in a row, the house takes all the bets (so all the players lose). What is the probability that five coin tosses in a row show a mix of heads and tails?

2. a) How many integers from 1000 to 10000 inclusive are multiples of four?

b) What is the probability that a randomly chosen integer from 1000 to 10000 inclusive is divisible by four?

3. Suppose you have a list of the integers written consecutively from -52 to 57.
a) How many integers are in the list?

b) Where would you have to split the list (into two sublists) in order to have a sublist containing 61 consecutive integers?

Checklist

Ensure that you understand:

- the definitions of sample space, event and probability;
- how to calculate the number of elements in a list.

Section 6.2

Trees and the Multiplication Rule

In this section, we see how to calculate the number of ways in which we can complete a process which involves many independent steps. We are also introduced to the notation for counting permutations, that is, orderings of distinct objects.

Exercise 6.2.1: Definitions

Fill in the blanks to complete the following sentences.

1. *The Multiplication Rule* Let O be an operation consisting of k steps where:

   - there are n_1 different ways to perform the first step,
   - there are n_2 different ways to perform the second step (regardless of how the first step was performed),

     $\vdots$

   - there are n_k different ways to perform the kth step (regardless of how the preceding steps were performed).

   Then there are ____________________________ different ways to perform the entire operation O.

   A **tree** can be used to represent the set of all possible outcomes of operation O.

2. A **permutation** of a set of objects is arrangement or ________________

   ____

3. **Theorem:** For any integer n with $n \geq 1$, the number of permutations of a set with n elements is ____

4. An ***r* -permutation** of a set of n elements is ____________________

   ____

   The number of r-permutations of a set of n elements is denoted ________

5. **Theorem:** For positive integers n and r, where $1 \leq r \leq n$, the number of r-permutations of a set of n elements is given by the formula

   ____

   or, equivalently, ____

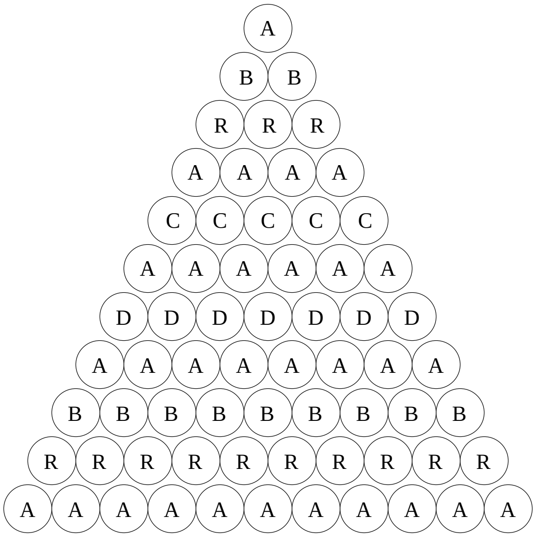
Exercise 6.2.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. How many bit strings (strings of 0s and 1s) of length n are there?

2. How many bit strings (strings of 0s and 1s) of length four do not have two consecutive 1s?

3. Beginning with the letter A at the top of the pyramid and reading down, always passing from a letter to an adjoining letter, in how many ways is it possible to read *ABRACADABRA*?



4. a) Consider the following nested loop:

```
for $i = 1$ to 4
    for $j = 1$ to 3
        for $k = 1$ to 5
            Statements in body of inner loop
            None lead out of the inner loop
        next $k$
    next $j$
next $i$
```

How many times will the inner loop be iterated when the program runs?

b) Consider the following nested loop:

```
for $i = 1$ to n
    for $j = 1$ to n
        for $k = 1$ to n
            Statements in body of inner loop
            None lead out of the inner loop
        next $k$
    next $j$
next $i$
```

How many times will the inner loop be iterated when the program runs?

5. How many four digit numbers, which are not divisible by five, can be created using the digits 4, 5, 6 and 7, without repeating any digits.

6. At the local Chinese take-away, the menu consists of 6 chicken dishes, 7 pork dishes, 9 beef dishes and 5 vegetarian dishes. Your prospective in-laws are coming to dinner tonight and you want to impress them by providing a variety of dishes. You decide to buy 4 dishes from the take-away (one each of chicken, pork, beef and vegetarian). How many possible meal combinations could you serve?

7. In how many ways can a photographer at a wedding arrange six people in a row, including the bride and groom, if:

a) the bride must be next to the groom?

b) the groom's mother is not next to the bride?

c) the bride's mother is to the left of the groom (not necessarily right beside him)?

Checklist

Ensure that you understand:

- how and when to apply the multiplication rule;
- the definitions of permutation and r-permutation.

Section 6.3

Sets and the Addition Rule

In this section we discover how to solve counting problems which involve two or more sets of objects. We shall see how to count the number of elements in the union of two sets, the difference of two sets, and the intersection of two sets. Pay particular attention to:

- the Inclusion/Exclusion Principle.

Exercise 6.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let $A_1, A_2, \ldots, A_k$ be a collection of sets which partition of a finite set A.

   Then (from the definition a partition in Chapter 5)

   $A =$ ______________________________ and for $i, j \in \{1, \ldots, k\}$ and $i \neq j$

   $A_i \cap A_j =$ __________________.

   The Addition Rule states that:

   $n(A) =$ ____

2. Let S be a finite sample space, A an event in S and A^c the complement of A in S. Then

   $1 - P(A^c) =$ ____

3. *The Inclusion/Exclusion Principle*

   If A, B and C are any finite sets, then

   $n(A \cup B) =$ ____

   and $n(A \cup B \cup C) =$ ____

   ____

Exercise 6.3.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Refer back to the Chinese take-away in Section 6.2, Question 6, and recall that there were 6 chicken dishes, 7 pork dishes, 9 beef dishes and 5 vegetarian dishes. Tonight you are on your own and you would like one dish from the take-away. However, after the latest salmonella outbreak, you have decided not to eat chicken for a few weeks. How many ways are there to choose your meal?

2. Suppose that you go to the Chinese take-away for dinner with two friends and you each randomly choose one dish (which could all be the same) and then share the three dishes for your meal.
a) What is the probability that the three of you end up with a meal that does not consist only of chicken dishes?

b) What is the probability that the three of you end up with a meal that has no vegetarian dishes in it?

3. A total of 1232 students have taken a course in Statistics, 879 have taken a course in Calculus and 114 have taken a course in Logic. Furthermore, 103 have taken courses in both Statistics and Calculus, 23 have taken courses in both Statistics and Logic and 14 have taken courses in both Calculus and Logic. If 2092 students have taken at least one course in Statistics, Calculus or Logic, how many students have taken courses in all three maths subjects?

4. Solve the *Chelsea Pensioners* puzzle by Lewis Carroll: If 70% have lost an eye, 75% an ear, 80% an arm and 85% a leg, what percentage at least must have lost all four?

Checklist

Ensure that you understand:

- when it is appropriate to use the addition rule to solve a problem;
- how to use the Inclusion/Exclusion rule.

Section 6.4

Combinations

In this section we investigate the ways to count how many subsets of a given size can be chosen from a set. These problems can become very involved when the subsets have to satisfy certain conditions. It is also important to be able to decide whether or not the order in which elements are selected is important. Pay particular attention to:

- the formula for an r-combination;
- the trap of double counting.

Exercise 6.4.1: Definitions

Fill in the blanks to complete the following sentences.

1. An **ordered selection** of r elements from a set of n elements is an _____

   ____

   An **unordered selection** of r elements from a set of n elements is an __

   ____

2. For nonnegative integers n and r, with $r \leq n$, An ***r*-combination** chosen from a set of n elements is __________________________

   The **number of r-combinations** that can be chosen from a set of n elements is denoted by ______, read "______________________",

   An r-combination is merely a collection of r different elements chosen from a set of n elements.

   Alternate notation to $\binom{n}{r}$ is $C(n,r)$.

3. **Theorem:** Let n and r be nonnegative integers, with $r \leq n$. The number of subsets of size r (or r-combinations) that can be chosen from a set of n elements, $\binom{n}{r}$, is given by the formula

   $\binom{n}{r} = $ ____

   or, equivalently, $\binom{n}{r} = $ ________________________________.

4. Suppose a collection of n objects consists of:

   - n_1 indistinguishable objects of type 1;
   - n_2 indistinguishable objects of type 2;

     $\vdots$

   - n_k indistinguishable objects of type k;

   where $n_1 + n_2 + \ldots + n_k = n$. Then the number of distinct permutations of the collection of n objects is

   $$\binom{n}{n_1} \cdot \binom{n-n_1}{n_2} \cdot \binom{n-n_1-n_2}{n_3} \ldots \binom{n-n_1-n_2-\ldots n_{k-1}}{n_k}$$

   Using the above Theorem it can be shown that

   $$\binom{n}{n_1} \cdot \binom{n-n_1}{n_2} \cdot \binom{n-n_1-n_2}{n_3} \ldots \binom{n-n_1-n_2-\ldots n_{k-1}}{n_k}$$

   $=$ ____

Exercise 6.4.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Calculate (without a calculator) the value of

a) $\binom{9}{3}$ b) $\binom{200}{198}$.

2. There are five questions on your maths assignment but you only have time to complete three of them. How many combinations of questions are there which you could complete?

3. You are playing a word game in which you must make up a sentence using the three words you draw out of a bag containing ten words.

a) How many possible ways are there to choose three words from the bag of ten words?

b) Suppose the game rules change so that you now have to make up a sentence in which the three words appear in the order in which they were chosen. How many possible combinations are there now?

c) What is the relationship between your answers to parts a) and b)?

4. Recall that the Chinese take-away sells six chicken dishes, seven pork dishes, nine beef dishes and five vegetarian dishes.

a) This week they have a promotional deal in which, if you buy the chicken with noodles dish, you get a beef and black bean dish for free. How many ways are there to choose four different main dishes (assuming that if you choose the chicken with noodles, you also take the beef and black bean)?

b) From previous experience, you realize that there are two pork dishes which do not go well together. How can you choose four main dishes which contain at most one of the two pork dishes?

5. In the game of poker each player is dealt five cards from an ordinary deck of cards, and each player is said to have a 5-card hand.

a) How many 5-card poker hands contain four cards of the one denomination?

b) Find the error in the following calculation of the number of 5-card poker hands which contain at least one jack. Once you have found the error, calculate the true number of 5-card poker hands which contain at least one jack.

Consider this in two steps:
Choose one jack from the four jacks.
Choose the other four cards in the hand.
Thus we have $\binom{4}{1}\binom{51}{4} = 999600$ such hands.

6. How many distinct ways are there to arrange the letters of the word *abracadabra*?

Special Points

- Watch out for the common error of counting things twice.

Checklist

Ensure that you understand:

- how to calculate the value of $\binom{n}{r}$;
- how to determine whether or not the order in which objects are chosen matters;
- how to use a case analysis to solve counting problems.

Section 6.5

r-Combinations with Repetition Allowed

In this section we discover how to count the number of r-combinations when repetition of elements is allowed.

Use the information in the reading to complete the following exercises.

Exercise 6.5.1: Definitions

Fill in the blanks to complete the following sentences.

1. The number of r-combinations that can be chosen from a set with n elements when repetition is allowed is ______________________________

Exercise 6.5.2: Examples

Complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. The Chinese take-away shop sells fortune cookies with fortunes relating to Health, Wealth, Happiness and Love. Normally these fortune cookies are kept in four separate jars, but to save space on the counter, they have all been put into one big jar. Assuming that there are at least six fortune cookies of each type in the jar, how many different combinations of the fortune types can you get if you choose six cookies from the jar?

2. How many solutions does the equation $x + y + z = 11$ have, where x, y and z are all non-negative integers?

Special Points

- This table may help you to remember which formula applies to which situation:

	Permutations (order matters)	Combinations (order does not matter)
Repetition is allowed	n^k	$\binom{n+k-1}{k}$
Repetition is not allowed	$P(n,k)$	$\binom{n}{k}$

Checklist

Ensure that you understand:

- when it is appropriate to use the formula for r-combinations with repetition;
- how to solve counting problems involving r-combinations with repetition.

Section 6.6

Useful Formula

In this section we shall explore some useful formulas involving $\binom{n}{r}$ and hopefully become more comfortable with using the $\binom{n}{r}$ notation in algebraic manipulations.

Exercise 6.6.1: Definitions

Fill in the blanks to complete the following sentences.

1. Let n and r be positive integers with $r \leq n$.
   Prove that $\binom{n}{r} = \binom{n}{n-r}$.

2. *Pascal's Formula*:

   Let n and r be positive integers and suppose $r \leq n$.
   Then $\binom{n+1}{r} =$ ______________________________

Exercise 6.6.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Given that $\binom{n}{n-2} = \frac{n(n-1)}{2}$, find an expression for $\binom{x+3}{x+1}$.

2. Use Pascal's formula to compute:

a) $\binom{7}{5} + \binom{7}{6}$

b) $\binom{9}{6} + \binom{9}{5}$

Checklist

Ensure that you understand:

- how to execute algebraic manipulations involving $\binom{n}{r}$.

Section 6.7

The Binomial Theorem

In this section we are presented with a very useful theorem. The Binomial Theorem gives an expression for expanding $(a+b)^n$, avoiding the tiresome process of multiplying $(a+b)$ by itself n times.

Exercise 6.7.1: Definitions

Fill in the blanks to complete the following sentences.

1. The sum of two terms is called a ____________________

2. **The Binomial Theorem:** Given any real numbers a and b and any nonnegative integer n,

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\ &= \underline{\hspace{10cm}}\end{aligned}$$

Exercise 6.7.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Expand the following using the Binomial Theorem.

a) $(x+y)^4$

b) $(2a-3b)^5$

2. Find the coefficient of m^2n^8 in the expansion of $(m+n)^{10}$.

3. Find the coefficient of x^6y^3 in the expansion of $(5x-3y)^9$.

Checklist

Ensure that you understand:

- how to apply the Binomial Theorem to expand expressions of the form $(a+b)^n$;
- how to apply the Binomial Theorem to find the coefficient of a given term in a binomial expansion.

Have you achieved the Chapter 6 Learning Objectives listed on pages 199 and 199?

Chapter Eight

Recursion

A sequence is said to be defined recursively if certain initial values are specified and later terms of the sequence are defined by relating them to a fixed number of earlier terms. In this chapter we shall formally define a recurrence relation, provide some related examples and explore methods for finding an explicit formula for a sequence that is recursively defined.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- compute terms of a recursively defined sequence;
- write a recurrence relation in more than one way;
- solve second-order linear homogeneous recurrence relations with constant coefficients;
- work with $\displaystyle\sum_{i=1}^{n} a_i$ and $\displaystyle\prod_{i=1}^{n} a_i$ and their recursive definitions.

Section 8.1

Recursively Defined Sequences

There are many situations in which the value of an expression changes based on preceding values; for instance the calculation of compound interest or the number of breeding rabbits. In situations such as these it is often helpful to describe the situation in terms of how the value changes from step to step. In this section we formally define a recurrence relation and give a variety of examples that show how to analyze certain kinds of problems in terms of recursion.

Exercise 8.1.1: Definitions

Fill in the blanks to complete the following sentences.

1. A sequence can be defined in a variety of different ways. One informal way is to write ____ that the general pattern will be obvious.

2. A second way to define a sequence is to ______________________________ ____.

3. A third way to define a sequence is to use ______________________________. This requires giving both an equation, called a ______________________________ that relates later terms in the sequence to earlier terms and a specification, called ______________________________ of the values of the first few terms of the sequence.

4. A **recurrence relation** for a sequence $a_0, a_1, a_2, \ldots$ is ____________________ ____ ____ ____

   The **initial conditions** for such a recurrence relation ____________________ ____

Exercise 8.1.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Let $c_0, c_1, c_2, \ldots$ be a sequence that satisfies the following recurrence relation: for all integers $k \geq 2$,

$$\begin{array}{lll} (1) & c_k & = (k-1)c_{k-1} + kc_{k-2} + k \\ (2) & c_0 & = 1 \ \text{ and } \ c_1 = 2. \end{array}$$

Calculate the values of c_2, c_3, and c_4.

2. Let $b_0, b_1, b_2, \ldots$ be a sequence that satisfies the following recurrence relation: for all integers $i \geq 2$,

$$b_i = 5b_{i-1} - 6b_{i-2}.$$

Write expressions for b_{i+1} and for b_{i+2}.

3. Show that the sequence 1, 1, 2, 6, 24, 120, $\ldots, n!, \ldots$ for $n \geq 0$ satisfies the recurrence relation $b_k = k \cdot b_{k-1}$ for all integers $k \geq 1$.

4. Show that the sequence 5, 10, 20, 40,$\ldots, 5 \cdot 2^k, \ldots$ for $k \geq 0$ satisfies the recurrence relation $a_n = 2 \cdot a_{n-1}$ for all integers $n \geq 1$.

5. *Bit strings*

a) Make a list of all bit strings of lengths 0, 1, 2, 3 and 4 that do not contain the bit pattern 10.

b) For each integer $n \geq 0$ let

$$S_n = \left[\begin{array}{l} \text{the number of bit strings of length } n \\ \text{that do not contain the pattern 10} \end{array} \right].$$

Find S_0, S_1, S_2, S_3 and S_4.

c) Find the number of bit strings of length ten that do not contain the pattern 10. (Use a recurrence relation for S_n.)

Checklist

Ensure that you understand:

- the definition of recurrence relation and the meaning of initial conditions;
- how to show that a sequence satisfies a certain recurrence relation;
- how to find a recurrence relation for a given sequence;
- how to write a recurrence relation in more than one way.

Section 8.3

Recurrence Relations

A variety of techniques exist for finding explicit formulas for special classes of recursively defined sequences. The method explained in this section is one that works for Fibonacci and other similarly defined sequences.

Exercise 8.3.1: Definitions

Fill in the blanks to complete the following sentences.

1. A **second-order linear homogeneous recurrence relation with constant coefficients** is ______________________________

   ____

   ____.

2. Use the discussion "Second order linear homegeneous recurrence relations with constant coefficients: The Distinct Roots Case' to fill in the following details.

   Suppose $a_k = -a_{k-1} + 12a_{k-2}$ is a second-order linear homogeneous recurrence relation. Suppose that for some number t with $t \neq 0$, the sequence $1, t, t^2, t^3, \ldots, t^n, \ldots$ satisfies the above relation. So for all integers $k \geq 2$,

   ____

   Since ______________, this equation may be divided by __________ to obtain ______________________. Or, equivalently, ______________________

   The only possible values of t are __________ and __________. Therefore the two sequences will be

   ____

   and ____

3. **Theorem:** Let A and B be real numbers. A recurrence relation of the form ____

   is satisfied by the sequence ________________________________

   where t is a nonzero real number, if, and only if, t satisfies the equation

   ________________________________.

4. The **characteristic equation** of the second-order linear homogeneous recurrence relation with constant coefficients,

$$a_k = A \cdot a_{k-1} + B \cdot a_{k-2}, \text{ for all integers } k \geq 2$$

   is

   ____

5. If $r_0, r_1, r_2, \ldots$ and $s_0, s_1, s_2, \ldots$ are sequences that satisfy the same second-order linear homogeneous recurrence relation with constant coefficients, and if ____

   ____

   ____

   ____

   also satisfies the same recurrence relation.

6. (**Distinct Roots Theorem**) Let A and B be real numbers and suppose a sequence $a_0, a_1, a_2, \ldots$ satisfies a recurrence relation

   ____

   for all integers $k \geq 2$. If the characteristic equation

   ____

   has ________________ r and s, then there exists real numbers C and D such that

   $a_n =$________________________________.

   Further the values a_0 and a_1 can be used to determine __________

   ____.

Exercise 8.3.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Which of the following defines a second-order linear homogeneous recurrence relation with constant coefficients? Answer Yes/No in the space provided.

a) $a_{k+1} = 4a_k - \frac{1}{2}a_{k-1}$ ____________

b) $b_k = -b_{k-1} + 5$ ____________

c) $c_k = a \cdot c_{k-1} + c_{k-2}$ (where a is a constant) ____________

d) $d_k = d_{k-1} \cdot d_{k-2}$ ____________

e) $e_k = 2e_{k-1} + 3e_{k-2} - \sqrt{2}\, e_{k-3}$ ____________

2. Consider the recurrence relation $a_k = 2a_{k-1} + 15a_{k-2}$ for all integers $k \geq 2$. Find all the sequences of the form

$$1, t, t^2, t^3, \ldots, t^n, \ldots$$

which satisfy this recurrence relation.

3. Consider the second-order linear homogeneous recurrence relation:

$$r_k = r_{k-1} + 2r_{k-2}.$$

a) Find the two sequences which satisfy this relation; call these sequences b_k and c_k.

b) Now let $a_n = 3b_n - c_n$ for all $n \geq 0$. Show that for all integers $k \geq 2$, the sequence a_k also satisfies the recurrence relation

$$r_k = r_{k-1} + 2r_{k-2}.$$

4. Find a sequence that satisfies the recurrence relation

$$b_k = 5b_{k-1} - 4b_{k-2}$$

and that also satisfies the initial conditions $b_0 = 2$ and $b_1 = 3$.

5. Find an explicit formula for the sequence $a_0, a_1, a_2, \ldots$ which satisfies the recurrence relation

$$a_k = a_{k-1} + 6a_{k-2}$$

and that also satisfies the initial conditions $a_0 = 13$ and $a_1 = -1$.

Checklist

Ensure that you understand:

- the definition of a second-order linear homogeneous recurrence relation with constant coefficients;
- how to find sequences which satisfy recurrence relations with initial conditions;
- how to find the explicit formula for the recurrence relation

  $$a_k = Aa_{k-1} + Ba_{k-2}$$

  when its characteristic equation has two distinct roots.

Section 8.4

General Recursive Definitions

Sequences of numbers are not the only objects that can be defined recursively. Sets, sums, products, unions, intersections, and functions can also be defined recursively.

Exercise 8.4.1: Definitions

Fill in the blanks to complete the following sentences.

1. There are three main components to needed to define a set of objects recursively. They are:

   I. **Base:** ____.

   II. **Recursion:** ______________________________________

   ____.

   III. **Restriction:** ____________________________________

   ____.

2. Given a positive integer n and a sequence of numbers $a_1, a_2, a_3, \ldots, a_n$, $\sum_{i=1}^{n} a_i$ (**summation from** $i = 1$ **to** n **of the** a_i), is defined recursively as follows:

   ____

   ____

3. Given a positive integer n and a sequence of numbers $a_1, a_2, a_3, \ldots, a_n$, $\prod_{i=1}^{n} a_i$ (**product from** $i = 1$ **to** n **of the** a_i) is defined recursively as follows:

   ____

   ____

Exercise 8.4.2: Examples

Use the definitions above to complete the following problems. If you encounter any difficulties, please refer to the hints on the Web. Once you have finished these problems, please check your solutions on the Web. If you have any further questions, please email your lecturer or post your question to the discussion group.

1. Complete the following program to show how you might compute the product of $a[1], a[2], \ldots, a[n]$.

```
prod := 0
for $k$ := 1 to $n$
            ________________________________
next $k$.
```

2. Prove, using mathematical induction or otherwise, that for any positive integer n, if $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are real numbers then:

$$\prod_{i=1}^{n}(a_i \cdot b_i) = \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} b_i.$$

Checklist

Ensure that you understand:

- the summation and product notation;
- how to think of the summation and product in terms of recursion.

Have you achieved the Chapter 8 Learning Objectives listed on page 227?

Contents

Section 1.3

Valid and Invalid Arguments

Given a collection $p_1, p_2, \ldots, p_n$ of statements (called premises) and another statement q (called the conclusion), an **argument** is the assertion that the conjunction of the premises implies the conclusion. Symbolically this is represented as

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \to q.$$

An argument is **valid** if whenever the premises are all true, the conclusion must also be true. That is, when $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \to q$ is a tautology. An argument is **invalid** if it is possible to have a situation in which all the premises are true but the conclusion is false.

One way to test an argument for validity is:

1. Choose symbols to represent the simple propositions.
2. Identify the premises and conclusion of the argument, and write the argument in symbolic form.
3. Construct a truth table showing the truth values of all the premises and the conclusion.
4. Find the rows (called critical rows) in which all the premises are true.
5. In each critical row, determine whether the conclusion is also true. If the conclusion is true in each critical row, then the argument is valid, but if there is at least one critical row in which the conclusion is false, then the argument in not valid.

Example 1.3.1 Determine whether or not the following argument is valid.
If I am rich, then I am happy. I am not happy. Therefore, I am not rich.

Let r represent the statement "I am rich", and let h represent the statement "I am happy". This argument can be represented symbolically as

$$((r \to h) \wedge \sim h) \to \sim r,$$

with truth values:

r	h	$r \to h$	$\sim h$	$\sim r$
T	T	T	F	F
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

The only row in which both premises are true is the last row. The conclusion is also true in this row, so the argument is valid.

Alternatively we can add two more columns to the truth table and determine whether or not $((r \to h) \wedge \sim h) \to \sim r$ is a tautology.

r	h	$r \to h$	$\sim h$	$\sim r$	$((r \to h) \wedge \sim h)$	$((r \to h) \wedge \sim h) \to \sim r$
T	T	T	F	F	F	T
T	F	F	T	F	F	T
F	T	T	F	T	F	T
F	F	T	T	T	T	T

Example Determine whether or not the following argument is valid. *If New York is a big city, then New York has tall buildings. New York has tall buildings. Therefore New York is a big city.*

Let b represent "New York is a big city" and t represent "New York has tall buildings". Then the argument can be represented symbolically as

$$((b \to t) \wedge t) \to b.$$

b	t	$b \to t$	t	b
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	F	F

There are two rows in which both premises are true, so the critical rows are 1 and 3. In row 3, the conclusion is false. Hence, for these truth values of b and t, the premises are true and the conclusion is false, so this argument is **not** valid.

When arguments contain many propositions, they lead to very large truth tables. In determining the validity of an argument, the important rows of the truth table are the rows in which all the premises are true. You can use this idea to avoid the use of a large truth table. A shorter method of determining the validity of an argument is to determine whether there is any way for it to be invalid. You can do this by looking for truth values which make all the premises true and the conclusion false. If you can find such truth values, the argument is invalid; if you cannot find such truth values, the argument is valid.

Example

Determine whether or not the following argument is valid.
If the races are fixed, or the gambling houses are crooked, then the tourist trade

will decline and the town will suffer. If the tourist trade decreases then the Police will be happy. The Police are never happy. Therefore, the races are not fixed.

Let r represent the statement "the races are fixed", g represent the statement "the gambling houses are crooked", d represent the statement "the tourist trade declines", s represent the statement "the town will suffer", and h represent the statement "the Police will be happy". Then the argument may be presented in symbolic form as

$$[((r \vee g) \to (d \wedge s)) \wedge (d \to h) \wedge (\sim h)] \to \sim r.$$

A truth table for this argument would have $2^5 = 32$ rows, so we shall try to avoid using a truth table. The only way in which the argument could be invalid is if all the premises are true but the conclusion is false.

If the conclusion is false, then $\sim r$ is false so

$$r \text{ is T.}$$

To obtain an invalid argument, the premises must be true and so

$$\begin{aligned} (r \vee g) \to (d \wedge s) &\quad \text{is} \quad \text{T}, & (1)\\ d \to h &\quad \text{is} \quad \text{T}, & (2)\\ \sim h &\quad \text{is} \quad \text{T}. & (3) \end{aligned}$$

By (3), h must be false, which means that by (2) d must also be false. This means that $d \wedge s$ is false, so by (1) $r \vee g$ must also be false. But that means both r and g must be false, so r must be true and false at the same time, which is impossible (because we have already found that r is T). This means that this argument cannot be invalid, so it must be valid.

Section 3.0

Formal Definitions of Number Systems

There are several number systems which you have already encountered in your mathematical careers and with which you are probably quite familiar. Some of the properties of these number systems may seem obvious to you, but in fact they are core ideas which need to be formally proved before the number systems can be used. In this section, we shall formally define the most common number systems and give a list of core properties which are satisfied by the integers. Later in Chapter 3, you will be asked to prove that these properties also hold for the rational numbers. Further discussion on the properties which hold for real numbers can be found in Appendix A of your textbook (pages 695-697).

Number Systems

Natural numbers (denoted $\mathbb{N}$) is the set of numbers $\{0, 1, 2, \ldots\}$. Many textbooks do not include the number 0 in the set of natural numbers, but we will be following the notation of the textbook "Discrete Mathematics with Applications" by Epp.

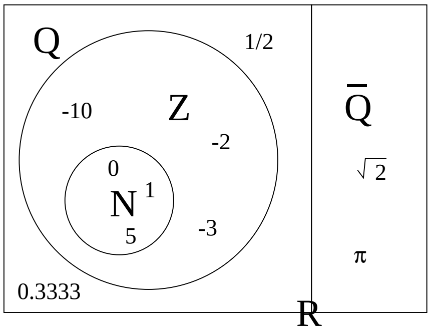
Integers (denoted $\mathbb{Z}$) is the set of numbers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$. The positive integers (denoted $\mathbb{Z}^+$) is the set $\{1, 2, \ldots\}$ and the negative integers (denoted $\mathbb{Z}^-$) is the set $\{-1, -2, -3, \ldots\}$. The positive integers are the natural numbers without 0.

Rational numbers (denoted $\mathbb{Q}$) is the set of numbers which can be expressed in the form m/n where m and n are integers, $n \neq 0$. Rational numbers include the integers, terminating decimals, repeating decimals and fractions.

Real numbers (denoted $\mathbb{R}$) is the set of numbers which include any decimals, infinite or not, recurring or not. Elements of $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ are all real numbers too.

Irrational numbers (denoted $\overline{\mathbb{Q}}$) is the set of real numbers which cannot be expressed in the form m/n where m and n are integers. This set includes numbers such as $\sqrt{2}$ and π.

The relationship between the number systems can be represented pictorially (the entire rectangle below denotes the set of real numbers which is all rational numbers together with all irrational numbers).



Properties of the Integers

We now introduce some properties which are true for the integers. We assume there are two operations which can act on the set of integers and we call these operations addition (denoted by $+$) and multiplication (denoted by $\cdot$). These operations satisfy the following properties:

Closure If a and b are integers, then $a+b$ and $a \cdot b$ are also integers.

Commutativity For all integers a and b,

$$a+b=b+a \text{ and } a\cdot b = b\cdot a.$$

Associativity For all integers a, b and c,

$$(a+b)+c=a+(b+c) \text{ and } (a\cdot b)\cdot c = a\cdot(b\cdot c).$$

Distributivity For all integers a, b and c,

$$a\cdot(b+c)=a\cdot b+a\cdot c \text{ and } (b+c)\cdot a = b\cdot a + c\cdot a.$$

Existence of Identity Elements There exist two distinct integers, denoted 0 and 1, such that for every integer a,

$$0+a=a+0=a \text{ and } 1\cdot a = a\cdot 1 = a.$$

Existence of Additive Inverses For every integer a, there is an integer, denoted $-a$ and called the additive inverse of a, such that

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

All the usual algebraic properties of the integers such as subtraction, cancellation laws for addition and multiplication and multiplication by negative numbers, can be derived from the above axioms.

We can now use the above properties to prove the cancellation law for addition of integers.

Example 3.0.1 Prove that for all integers a, b and c, if $a + b = a + c$, then $b = c$.

Proof Suppose that a, b and c are integers and $a + b = a + c$.

Since

$$\begin{aligned} a + b &= a + c, \\ -a + (a + b) &= -a + (a + c), \\ (-a + a) + b &= (-a + a) + c \text{ (by Associativity)}, \\ 0 + b &= 0 + c \text{ (by Additive Inverse)}, \\ b &= c \text{ (by Additive Identity)}. \end{aligned}$$

Definitions of Inequalities

In order to be able to interpret mathematical statements involving $<$, $>$, $\leq$ and $\geq$ we need to define these symbols. It is easy to say “3 is less than 5” but what does the term “less than” actually mean? We have to impose an ordering on our number system and we do so using the following three observations.

1. For any integers a and b, if a and b are positive, so are $a+b$ and $a \cdot b$. This is simply the closure property for $\mathbb{Z}^+$.

2. For every integer $a \neq 0$, either a is positive or $-a$ is positive but not both.

3. The number 0 is neither positive nor negative.

These observations allow us to define an ordering on the integers so that we can use the descriptions “less than” ($<$) and “greater than” ($>$) to compare two integers.

Given integers a and b,

- $a > 0$ means that a is positive;
- $a < 0$ means that a is negative;
- $a < b$ means $b + (-a)$ is positive;

- $b > a$ means $a < b$;
- $a \leq b$ means $a < b$ or $a = b$;
- $b \geq a$ means $a \leq b$;
- if $a \geq 0$, we say that a is non-negative.

We can now use these definitions to prove some facts about inequalities.

Example 3.0.2 Prove that for all integers a, b and c, if $a < b$ and $b < c$, then $a < c$.

Proof Suppose that a, b and c are integers and $a < b$ and $b < c$.

Since	$a < b$ and $b < c$,	
	$b + (-a)$ is positive and $c + (-b)$ is positive	(by definition of $<$),
	$(c + (-b)) + (b + (-a))$ is positive	(by observation 1),
	$[(c + (-b)) + b] + (-a)$ is positive	(by Associativity),
	$[c + ((-b) + b)] + (-a)$ is positive	(by Associativity),
	$(c + 0) + (-a)$ is positive	(by Additive Inverse),
	$c + (-a)$ is positive	(by Additive Identity).
Therefore	$a < c$	(by definition of $<$).

Section 3.8

The Euclidean Algorithm

Recall from Section 3.4 that the Quotient–Remainder Theorem states that given any integer a and a positive integer d, there exist unique integers q and r such that $a = d \cdot q + r$ and $0 \leq r < d$.

There is a process for finding the integers q and r. If you are given a and d, the integers q and r are given by the equations:

$$\begin{array}{rcl} q & = & \left\lfloor \frac{a}{d} \right\rfloor ; \\ r & = & a - d \cdot q. \end{array}$$

You should now **read pages 173–175** of the textbook which explain the Euclidean Algorithm. Once you have read those pages, continue with the following examples.

Example 3.8.1: Find $\gcd(330, 152)$.

Apply the Euclidean Algorithm to 330 and 152:

$$\begin{array}{rcll} 330 & = & 152 \cdot 2 + 26 & \text{so } \gcd(330, 152) = \gcd(152, 26) \\ 152 & = & 26 \cdot 5 + 22 & \text{so } \gcd(152, 26) = \gcd(26, 22) \\ 26 & = & 22 \cdot 1 + 4 & \text{so } \gcd(26, 22) = \gcd(22, 4) \\ 22 & = & 4 \cdot 5 + 2 & \text{so } \gcd(22, 4) = \gcd(4, 2) \\ 4 & = & 2 \cdot 2 + 0 & \text{so } \gcd(4, 2) = \gcd(2, 0) \end{array}$$

Therefore $\gcd(330, 152) = 2$.

Example 3.8.2: Find $\gcd(1098, 131)$.

Apply the Euclidean Algorithm to 1098 and 131:

$$\begin{array}{rcll} 1098 & = & 131 \cdot 8 + 50 & \text{so } \gcd(1098, 131) = \gcd(131, 50) \\ 131 & = & 50 \cdot 2 + 31 & \text{so } \gcd(131, 50) = \gcd(50, 31) \\ 50 & = & 31 \cdot 1 + 19 & \text{so } \gcd(50, 31) = \gcd(31, 19) \\ 31 & = & 19 \cdot 1 + 12 & \text{so } \gcd(31, 19) = \gcd(19, 12) \\ 19 & = & 12 \cdot 1 + 7 & \text{so } \gcd(19, 12) = \gcd(12, 7) \\ 12 & = & 7 \cdot 1 + 5 & \text{so } \gcd(12, 7) = \gcd(7, 5) \\ 7 & = & 5 \cdot 1 + 2 & \text{so } \gcd(7, 5) = \gcd(5, 2) \\ 5 & = & 2 \cdot 2 + 1 & \text{so } \gcd(5, 2) = \gcd(2, 1) \\ 2 & = & 1 \cdot 2 + 0 & \text{so } \gcd(2, 1) = \gcd(1, 0) \end{array}$$

Therefore $\gcd(1098, 131) = 1$.

In this case it may have been apparent to you that the $\gcd(1098, 131)$ was 1, part way through the algorithm, since you may have realized that 19 and 12 have no common divisors other than 1. If you are only interested in finding the gcd, you may stop the algorithm at any point. Here we did every step of the algorithm since we will be referring back to this example in the next section.

Section 3.9

Linear Diophantine Equations

A Diophantine equation is an equation in one or more unknowns with integer coefficients for which integer solutions are sought. Some examples of linear Diophantine equations are:

$$2x = 6, \qquad 5y + 2z = 11, \qquad 6m + 4n = 3.$$

The word Diophantine refers to the Greek mathematician of the third Century A.D., Diophantus of Alexandria, who made a study of such equations. A linear equation is one in which the unknowns $(x, y, z, m,$ etc.$)$ appear only to the first power. Hence a linear Diophantine equation is an equation with integer coefficients in one or more unknowns, which appear only to the first power, and for which integer solutions are sought.

When confronted by any type of equation, the first problem is to discover whether or not a solution exists. If a solution does exist, we are then faced with the problem of determining how many solutions there are, and how to find one or all of them explicitly.

Consider the simple linear Diophantine equation $ax = b$ where a and b are fixed integers. The equation $2x = 6$ is an example of such an equation. We know that this equation has an integer solution for x if, and only if, $a \mid b$. Furthermore, if a solution exists, it is unique unless $a = b = 0$, in which case every integer is a solution. For example, in the equation $2x = 6$, we know that the unique solution is $x = 3$.

In this section we shall investigate linear Diophantine equations, in two variables, of the form $ax + by = c$, where a, b and c are fixed integers.

Theorem 3.9.1 The linear Diophantine equation $ax+by = c$, where $a, b, c \in \mathbb{Z}$, has a solution if, and only if, $\gcd(a, b) \mid c$.

We shall not prove this theorem here. If you are interested in the proof of Theorem 3.9.1, you can find it in “Discrete Mathematics, Logic and Structures” (2nd edition) by Billington et al. (page 184).

By this theorem, the linear Diophantine equation $5y + 2z = 11$ does have a solution since $\gcd(5, 2) = 1$ and $1 \mid 11$. However, the linear Diophantine equation $6m + 4n = 3$ does not have a solution since $\gcd(6, 4) = 2$ and 2 does not divide 3.

The process of finding a solution to a linear Diophantine equation of the form $ax + by = c$ involves working forwards and backwards through the Euclidean algorithm. We shall illustrate this process with a few examples.

Example 3.9.2 Determine whether or not a solution exists to the linear Diophantine equation $330x + 152y = 6$. If a solution does exist, find one such solution.

We must first use the Euclidean algorithm to find $\gcd(330, 152)$. (This was done in the previous section, but we shall repeat it here so that we can refer back to it.)

$$\begin{aligned}
330 &= 152 \cdot 2 + 26 && (1)\\
152 &= 26 \cdot 5 + 22 && (2)\\
26 &= 22 \cdot 1 + 4 && (3)\\
22 &= 4 \cdot 5 + 2 && (4)\\
4 &= 2 \cdot 2 + 0 && (5)
\end{aligned}$$

Thus $\gcd(330, 152) = 2$, and since $2 \mid 6$, there is a solution to the linear Diophantine equation $330x + 152y = 6$.

To find a solution we first work backwards through the Euclidean algorithm to find a solution to the linear Diophantine equation $330x + 152y = 2 = \gcd(330, 152)$.

Rearranging the second last equation of the Euclidean algorithm, we see that $\gcd(330, 152) = 2 = 22 - 4 \cdot 5$. Now we proceed backwards through the steps of the Euclidean algorithm. For each equation, we isolate the remainder term and substitute the resulting expression for that remainder term.

We start with

$$\begin{aligned}
2 &= 22 - 4 \cdot 5\\
& \text{(now isolate the 4 in the previous equation (3) and substitute)}\\
&= 22 - (26 - 22 \cdot 1) \cdot 5 \text{ (since } 4 = 26 - 22 \cdot 1 \text{ by equation (3))}\\
&= 22 \cdot 6 - 26 \cdot 5\\
& \text{(now isolate the 22 in the previous equation (2) and substitute)}\\
&= (152 - 26 \cdot 5) \cdot 6 - 26 \cdot 5 \text{ (since } 22 = 152 - 26 \cdot 5 \text{ by equation (2))}\\
&= 152 \cdot 6 - 26 \cdot 35\\
& \text{(now isolate the 26 in the previous equation (1) and substitute)}\\
&= 152 \cdot 6 - (330 - 152 \cdot 2) \cdot 35 \text{ (since } 26 = 330 - 152 \cdot 2 \text{ by equation (1))}\\
&= 152 \cdot 76 - 330 \cdot 35
\end{aligned}$$

Notice that we do *not* multiply out the expressions as we go! Now rewrite the equation in the form $330x + 152y = \gcd(330, 152)$:

$$330(-35) + 152(76) = 2.$$

However, we wanted a solution to the equation $330x+152y=6$. To obtain such a solution simply multiply both sides of the equation by 3:

$$330(-105)+152(228)=6.$$

Hence $x=-105$ and $y=228$ is one solution to the equation $330x+152y=6$.

Example 3.9.3 Determine whether or not a solution exists to the linear Diophantine equation $155x+403y=19$. If a solution does exist, find one such solution.

First apply to the Euclidean algorithm to find $\gcd(403,155)$.

$$\begin{aligned}
403 &= 155\cdot 2+93\\
155 &= 93\cdot 1+62\\
93 &= 62\cdot 1+31\\
62 &= 31\cdot 2+0
\end{aligned}$$

Hence $\gcd(403,155)=31$. Since 31 does not divide 19, there is no solution to this linear Diophantine equation.

Example 3.9.4 Determine whether or not a solution exists to the linear Diophantine equation $1098m+131n=4$. If a solution does exist, find one such solution.

In Section 3.8a, the Euclidean Algorithm was used to find $\gcd(1098,131)$. From Example 3.8.2 (Reading Section), we know that $\gcd(1098,131)=1$. Since $1\mid 4$, we know that this linear Diophantine equation does have a solution. We now proceed backwards through the steps of the Euclidean algorithm to find a solution to the equation $1098m+131n=1$. You should refer back to the equations in Example 3.8.2 (Reading Section).

$$\begin{aligned}
1 &= 5-2\cdot 2\\
&\quad \text{(now isolate the 2 in the previous equation and substitute)}\\
&= 5-(7-5\cdot 1)\cdot 2\\
&= 5\cdot 3-7\cdot 2\\
&\quad \text{(now isolate the 5 in the previous equation and substitute)}\\
&= (12-7\cdot 1)\cdot 3-7\cdot 2\\
&= 12\cdot 3-7\cdot 5\\
&\quad \text{(now isolate the 7 in the previous equation and substitute)}\\
&= 12\cdot 3-(19-12\cdot 1)\cdot 5\\
&= 12\cdot 8-19\cdot 5\\
&\quad \text{(now isolate the 12 in the previous equation and substitute)}
\end{aligned}$$

$$
\begin{aligned}
&= (31 - 19 \cdot 1) \cdot 8 - 19 \cdot 5 \\
&= 31 \cdot 8 - 19 \cdot 13 \\
&\quad \text{(now isolate the 19 in the previous equation and substitute)} \\
&= 31 \cdot 8 - (50 - 31 \cdot 1) \cdot 13 \\
&= 31 \cdot 21 - 50 \cdot 13 \\
&\quad \text{(now isolate the 31 in the previous equation and substitute)} \\
&= (131 - 50 \cdot 2) \cdot 21 - 50 \cdot 13 \\
&= 131 \cdot 21 - 50 \cdot 55 \\
&\quad \text{(now isolate the 50 in the previous equation and substitute)} \\
&= 131 \cdot 21 - (1098 - 131 \cdot 8) \cdot 55 \\
&= 131 \cdot 461 - 1098 \cdot 55
\end{aligned}
$$

Rewrite the equation in the form $1098m + 131n = \gcd(1098, 131)$:

$$1098(-55) + 131(461) = 1.$$

However, we were looking for a solution to the equation $1098m + 131n = 4$. To obtain such a solution we simply multiply both sides of the equation by 4:

$$1098(-220) + 131(1844) = 4.$$

Hence $m = -220$ and $n = 1844$ is one solution to the equation $1098m+131n = 4$.

Section 3.10

General Solution to a Linear Diophantine Equation

We are often interested in finding positive integer solutions to linear Diophantine equations, so the one solution we find using the method of the previous section is not always enough.

Consider the equation $330x + 152y = 6$ from Example 3.9.2. We are going to consider the relationship between two solutions to this linear Diophantine equation. The first solution will be $x = x_0$, $y = y_0$ and this will be the solution we found in the previous section. Thus $x_0 = -105$ and $y_0 = 228$. Now let the second solution be $x = u$ and $y = v$. Since both these solutions must satisfy the equation we know that:

$$330x_0 + 152y_0 = 6 \quad \text{and} \quad 330u + 152v = 6.$$

$$\begin{array}{rrcl} \text{Thus} & 330u + 152v & = & 330x_0 + 152y_0, \\ & 330u - 330x_0 & = & 152y_0 - 152v, \\ & 330(u - x_0) & = & 152(y_0 - v). \end{array}$$

Now dividing both sides of the equation by $\gcd(330, 152) = 2$ gives:

$$165(u - x_0) = 76(y_0 - v).$$

Thus $\quad 165 \mid 76(y_0 - v) \quad$ and $\quad 76 \mid 165(u - x_0)$.

Consider the fact that $165 \mid 76(y_0 - v)$. Since $\gcd(165, 76) = 1$, no prime factors of 165 will divide into 76. Therefore all the prime factors of 165 must divide into $(y_0 - v)$ and so 165 must divide into $(y_0 - v)$. By similar reasoning, 76 must divide into $(u - x_0)$. Hence we conclude that

$$165 \mid (y_0 - v) \quad \text{and} \quad 76 \mid (u - x_0).$$

So $\quad y_0 - v = 165s \quad$ and $\quad u - x_0 = 76t \quad$ for some $s, t \in \mathbb{Z}$.

Substituting these values into $165(u - x_0) = 76(y_0 - v)$ we see that

$$165(76t) = 76(165s) \quad \text{and hence } s = t.$$

Thus, the general solution is given by

$$u = x_0 + 76t \quad \text{and} \quad v = y_0 - 165t.$$

Using $x_0 = -105$ and $y_0 = 228$ as the initial solutions, an infinite number of solutions to our equation can be found where:

$$u = -105 + 76t \quad \text{and} \quad v = 228 - 165t \quad \text{where } t \in \mathbb{Z}.$$

Theorem 3.10.1 If x_0 and y_0 are one solution to the linear Diophantine equation $ax + by = c$, where $a, b, c \in \mathbb{Z}$, and $d = \gcd(a, b)$, then the general solution to the linear Diophantine equation $ax + by = c$ is given by

$$\begin{aligned} x &= x_0 + \frac{b}{d} \cdot t \\ \text{and} & \\ y &= y_0 - \frac{a}{d} \cdot t \end{aligned}$$

for $t \in \mathbb{Z}$.

Thus, if there is a solution to a linear Diophantine equation, then there are infinitely many solutions.

We shall now see how Theorem 3.10.1 can be used to solve a problem.

Example 3.10.2
The owner of a small business has \$1740 to spend on upgrading the desks and chairs in her offices. If each new desk costs \$354 and each new chair costs \$258, how many new desks and chairs can she purchase so that she spends exactly \$1740?

If we let x represent the number of desks bought and y represent the number of chairs bought, then this problem is equivalent to finding an integer solution to

$$354x + 258y = 1740$$

in which x and y are both positive.

We must first look for an integer solution to the equation $354x + 258y = 1740$. We shall use the Euclidean algorithm to find $\gcd(354, 258)$.

$$\begin{aligned} 354 &= 258 \cdot 1 + 96 \\ 258 &= 96 \cdot 2 + 66 \\ 96 &= 66 \cdot 1 + 30 \\ 66 &= 30 \cdot 2 + 6 \\ 30 &= 6 \cdot 5 + 0 \end{aligned}$$

Thus $\gcd(354, 258) = 6$, and since $6 \mid 1740$, there is a solution to the linear Diophantine equation $354x + 258y = 1740$.

To find a solution we first work backwards through the Euclidean algorithm to find a solution to the linear Diophantine equation $354x + 258y = 6$.

Now we proceed backwards through the steps of the Euclidean algorithm.

$$\begin{aligned} 6 &= 66 - 30 \cdot 2 \\ &= 66 - (96 - 66 \cdot 1) \cdot 2 \\ &= 66 \cdot 3 - 96 \cdot 2 \\ &= (258 - 96 \cdot 2) \cdot 3 - 96 \cdot 2 \\ &= 258 \cdot 3 - 96 \cdot 8 \\ &= 258 \cdot 3 - (354 - 258 \cdot 1) \cdot 8 \\ &= 258 \cdot 11 - 354 \cdot 8 \end{aligned}$$

Hence $354(-8) + 258(11) = 6$ and, since $1740 = 290 \cdot 6$, we can multiply both sides of the equation by 290 and obtain the equation

$$354(-2320) + 258(3190) = 1740.$$

So one solution to this linear Diophantine equation is $x = -2320$ and $y = 3190$. Unfortunately we cannot purchase a negative number of desks. We can now apply Theorem 3.10.1, with $x_0 = -2320$, $y_0 = 3190$, $a = 354$, $b = 258$ and $d = 6$ to find the all the solutions to this linear Diophantine equation:

$$x = -2320 + \frac{258}{6}t \qquad y = 3190 - \frac{354}{6}t.$$

Thus for any integer t, the values $x = -2320 + 43t$ and $y = 3190 - 59t$ provide an integer solution to the equation $354x + 258y = 1740$.

The business owner wanted a solution in which both x and y are non-negative, so we need to determine whether there is a value of t for which both $x \geq 0$ and $y \geq 0$.

$$\begin{array}{lcl} -2320 + 43t \geq 0 & \text{and} & 3190 - 59t \geq 0 \\ t \geq \dfrac{2320}{43} & & t \leq \dfrac{3190}{59} \\ t \geq 53.9\ldots & & t \leq 54.06\ldots \end{array}$$

A value of $t = 54$ will provide a solution for which both x and y are positive: $x = -2320 + 43 \cdot 54 = 2$ and $y = 3190 - 59 \cdot 54 = 4$. Thus the business owner should buy two desks and four chairs.

Section 6.5

r-Combinations with Repetition Allowed

From previous sections we know that there are $\binom{n}{r}$ ways in which we can choose r elements from a set of n distinct elements. Now we are interested in how many ways we can choose r elements from a set of n elements when we are allowed to repeat elements; that is, each time we choose an element from the set of distinct elements, we replace it before we choose the next element. Thus at each stage, we can choose any one of the n elements, regardless of whether or not that element has been chosen previously. We shall demonstrate how to count these types of r-combinations using an example.

Example 6.5.0 Congratulations, you are on "Who Dares Wins". You have the opportunity to win up to $600. To win your prize, blindfolded, you must select six notes from a money bag which contains $5 notes, $10 notes, $20 notes, $50 notes and $100 notes. You are told that there are at least six notes of each denomination in the bag and you can make as many selections as you like with the proviso that if you remove more than six notes you get nothing. The bag also contains a scorpion, so don't try to feel around for the different sized notes. How many ways are there of selecting the six notes from the bag?

The problem involves counting 6-combinations with repetition allowed from a set of five elements (the possible denominations). Imagine placing five boxes on a table, with the boxes marked $5, $10, $20, $50 and $100. Assuming you have selected six notes, place each note in the appropriate box. Two possibilities are illustrated below.

Selection	$5	$10	$20	$50	$100
Two $5, one $10, three $50	XX	X		XXX	
Four $10, one $50, one $100		XXXX		X	X

Using an X to represent a note and a | to separate the denominations, the first possibility illustrated above looks like XX|X||XXX|, and the second possibility illustrated above looks like |XXXX||X|X. Notice that if one of the boxes is empty, then you may get two bars beside each other. Each possibility can be represented as a string of six crosses and four bars, so the number of ways of selecting the notes is equivalent to the number of ways of arranging six crosses and four bars. This is the number of ways to arrange ten items, in which six are indistinguishable of type A and the four are indistinguishable of type B:

$$\frac{10!}{6!4!} = 210$$

Another way to think of this is that you must select the six positions for the crosses, and then the bars simply fall into place. This corresponds to the number of ways of selecting six objects from a set of ten (choose where the crosses go), which is $\binom{10}{6} = 210$.

Theorem When repetition of elements is allowed, there are $\dbinom{n+r-1}{r}$ r-combinations that can be chosen from a set of n elements.

In the preceding example, we were interested in counting 6-combinations, with repetition allowed, from a set of 5 elements, so $n = 5$ and $r = 6$. Using the theorem we see there are $\dbinom{5+6-1}{6} = \dbinom{10}{6}$ of such 6-combinations.

The Last Chapter

Groups and Fields:

In this chapter we investigate algebraic structures which arise when we consider a set and one or two binary operations (such as addition or multiplication) which acts on the elements of the set. Groups and fields may seem like very abstract ideas to you at first, but keep in mind that these structures have many important applications in coding theory and cryptography.

Since this chapter is not included in your textbook, a section of reading has been provided to give you the necessary information. Any page numbers referred to in this section are the page numbers in the reading.

Chapter Learning Objectives

By the end of this chapter you should be able to:

- understand the definitions of group, abelian group, subgroup, cyclic group, generator, and order of an element;
- determine whether a given set and binary operation form a group or abelian group;
- determine whether a given group H is a subgroup of a given group G;
- find the order of the elements of a given group;
- understand the definition of a field.

Groups and Fields:

Section G.1

Definitions and Examples of Groups

A binary operation is a function from $X \times X$ to Y where, usually, $Y \subseteq X$. In this Section, we take a more detailed look at some of the algebraic structures which arise when we take a single binary operation on a set.

In Section 3.0, we studied the properties of the integers. We noted that the binary operation of addition on the integers satitisfied the properties of closure, associativity, and that there existed an identity element under addition, as well as additive inverses for all integers. The integers under addition provides an example from a wider class of algebraic structures called groups. A *group* is a set together with a binary operation which satisfies these four properties. Formally:

Definition G.1.1 A *group* $(G, *)$ is a set G together with a binary operation $*$ on G, such that:

- for all $g, h \in G$, $g * h \in G$; that is, G is closed under the binary operation $*$;
- for all $g, h, k \in G$, $(g * h) * k = g * (h * k)$; that is, $*$ is associative;
- there exists an element $e \in G$ such that for all $g \in G$, $g * e = g = e * g$; that is, G has an identity e;
- for all $g \in G$, there exists $g^{-1} \in G$, such that $g * g^{-1} = e = g^{-1} * g$; that is, for all $g \in G$ there exists an inverse element $g^{-1} \in G$.

Algebraic structures, such as groups, have been used extensively in coding theory and cryptography.

The notation $(G, *)$ is used to denote the group consisting of the set G together with the binary operation, $*$ on G. However, when we are talking of groups in general or when the binary operation has been clearly defined, we simply denote the group by G. It is also common practice to refer to the binary operation as multiplication and denote it by juxtaposition; that is we write $g_1 g_2$ in place of $g_1 * g_2$.

In the above definition we stated the associative law in relation to the product of three elements. What if we wish to take the product of four elements, or more? In what way do we proceed? It turns out that the associative law, as given, implies that the product of n elements has a unique meaning. That is, all possible products of the n elements, $s_1, s_2, \ldots, s_n$, taken in this order are equal; brackets may be inserted or omitted at will.

For any element $g \in G$, we say that the n^{th} *power* of g is given by $g^n = g*g*\ldots*g$, (with n $g's$) where $*$ is the binary operation of the group. Equivalently, if the binary operation is given in terms of additive notation, then the n^{th} power is given by $ng = g + g + \ldots + g$ (still with n $g's$.

Example G.1.2 Recall that in Chapter 10 we studied the equivalence relation ρ on $\mathbb{Z}$, defined by

$$x\rho y \text{ if, and only if, } x \equiv y (\text{mod } 6).$$

The equivalence classes for this relation are the sets $[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6$. In this way the set of equivalence classes is identified with the set $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. We may define a binary operation $\oplus$ on $\mathbb{Z}_6$ as follows

$$\forall x, y \in \mathbb{Z}_6, \quad x \oplus y = z \text{ if, and only if, } z \in \mathbb{Z} \text{ and } z \equiv x + y (\text{mod } 6).$$

If we consider the set of integers modulo 6, namely $\mathbb{Z}_6 = \{0, 1, \ldots, 5\}$, together with the operation of addition modulo 6, denoted by $\oplus$ then our work in Chapter 10 can be used to verify that:

Closure: For any $z_1, z_2 \in \mathbb{Z}_6$, $z_1 \oplus z_2 \in \mathbb{Z}_6$, and so $\mathbb{Z}_6$ is closed under the binary operation $\oplus$.
Associativity: For any $z_1, z_2, z_3 \in \mathbb{Z}_6$, $(z_1 \oplus z_2) \oplus z_3 = z_1 \oplus (z_2 \oplus z_3)$, so $\oplus$ is associative on $\mathbb{Z}_6$.
Identity: For any $z \in \mathbb{Z}_6$, $0 \oplus z = z = z \oplus 0$, so 0 is the identity element of $\mathbb{Z}_6$.
Inverse: For all $z \in \mathbb{Z}_6$, there exists $z^{-1} \in \mathbb{Z}_6$ such that $z \oplus z^{-1} = 0 = z^{-1} \oplus z$, namely $z^{-1} = 6 - z$; that is, for any element z of $\mathbb{Z}_6$ there exists an inverse element.

Since addition modulo 6, taken on $\mathbb{Z}_6$, is closed, associative, and has an identity and since inverse elements exist, we have proved that $(\mathbb{Z}_6, \oplus)$ is a group.

Example G.1.3 Consider the set B of all binary strings of length n. That is, each string is made up of n digits, each of which is either "0" or "1". Define the following binary operation $*$ on B.

Let a and b be any two strings of B, where $a = a_1a_2\ldots a_n$ and $b = b_1b_2\ldots b_n$, with each a_i and b_i equal to 0 or 1. Let $a * b = c = c_1c_2\ldots c_n$, where

$$c_k = \begin{cases} 1 & \text{if and only if } a_k = b_k, \\ 0 & \text{otherwise.} \end{cases}$$

Closure: It is easy to see that $a * b$ is a binary string of length n, so $a * b \in B$, and thus we have closure.
Associativity: The proof that $*$ is associative is left as an exercise; see Exercise G.1.1.
Identity: The binary string with all digits equal to 1 is the identity.
Inverses: Each string is its own inverse.

Therefore B forms a group under the given binary operation. This group has applications to error–correction in coding theory.

Example G.1.4 Consider the non-zero integers under division: $g = F - \{0\}$ and we ahve the operation $* : G \times G \to \mathbb{Q}$ on G where $g * h = \frac{g}{h}$. But $(G, *)$ is not a group, since closure fails, for example $2 * 3 = \frac{2}{3} \notin G$.

At first, one might be tempted to think that all the "usual sets and operations" form groups. This is not the case, as the following example shows.

Example G.1.5 $\mathbb{Z}$ under multiplication is not a group. We have an identity element, 1. However, 2 (for example) has no identity. Infact, the elements 1 and -1 are the only elements which have inverses, namely themselves.

However, there are some very unusual groups as the next example demonstrates.

Example G.1.6 The group $(D_3, \circ)$ can be visualised in terms of the symmetries of an equilateral triangle. Let us consider an equilateral triangle as shown in Figure G.1.1.

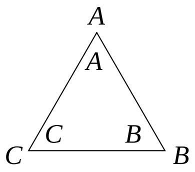


Figure G.1.1

Imagine fixing one copy of an equilateral triangle in the plane, and then covering it by another copy of the triangle which has been moved in some manner. We are interested in the displacement of the vertices. The lettering outside the triangle denotes the original position of the vertices, and the lettering inside the triangle denotes the vertices, after some movement has been carried out.

If we rotate the triangle clockwise through 120° and 240°, we obtain the triangles in Figure G.1.2.

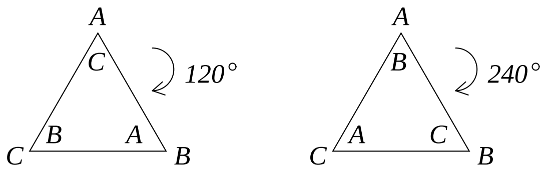


Figure G.1.2

Let us denote these two movements by r_1 and r_2 respectively.

If we drop a perpendicular through vertex A to side CB, and then reflect across this line, we obtain the triangle in Figure G.1.3. We shall denote this movement by m_1.

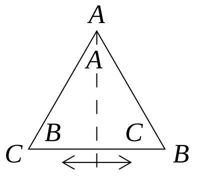


Figure G.1.3

Similarly we can obtain the triangles in Figure G.1.4, and we denote these movements by m_2 and m_3 respectively.

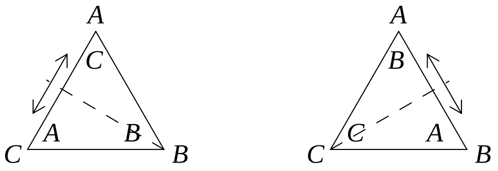


Figure G.1.4

Note that for any of the movements m_1, m_2, m_3, the line we reflect across is fixed in space and does not move.

Then the set $D_3 = \{e, r_1, r_2, m_1, m_2, m_3\}$, where e represents the identity function, (that is, no movement of the original triangle), forms a group under the binary operation "composition of movement". For example, let us consider the composition $(m_1 \circ r_2)$. The resulting triangle is achieved by rotating through 240° and then reflecting across the vertical line which passed through the fixed point A. Figure G.1.5 illustrates this composition.

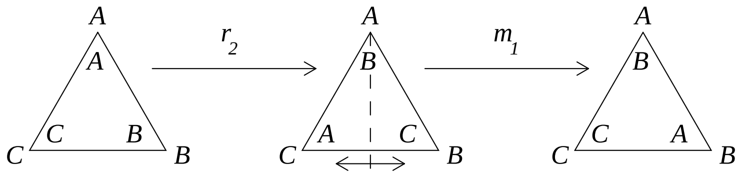


Figure G.1.5

Further examples of groups are $(\mathbb{Z}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$ and $(\mathbb{Z}, *)$ where we define $*$ to be: for $a, b \in \mathbb{Z}$, $a * b = a + b + 2$. For further examples of groups see Exercises G.1 and Section G.2.

The existence of the identity and an inverse for each element is an essential feature of a group.

Proposition G.1.7 In a group $(G, *)$ there exists one and only one identity element, e, such that $g * e = g = e * g$, for all $g \in G$. Similarly, for each $g \in G$ there exists one and only one inverse element, g^{-1}, such that $g*g^{-1} = e = g^{-1}*g$.

Proof (i) Assume that there exist elements e and e' in G such that, for all $g \in G$,

$$g * e = g = e * g \quad (1) \qquad \text{and} \qquad g * e' = g = e' * g \quad (2).$$

Since the statements (1) and (2) are true for all $g \in G$, we substitute $g = e'$ in equation (1) and obtain

$$e' * e = e'.$$

Substituting $g = e$ in equation (2) gives

$$e = e' * e.$$

By comparing the last two equations we get $e = e'$. Hence the identity element is unique.

(ii) Now assume that for every $g \in G$ there exists ${g_1}^{-1}$ such that

$$g * {g_1}^{-1} = e = {g_1}^{-1} * g,$$

and ${g_2}^{-1}$ such that

$$g * {g_2}^{-1} = e = {g_2}^{-1} * g.$$

If we use the fact that G has an identity and $*$ is associative, we can write

$${g_1}^{-1} = {g_1}^{-1} * e = {g_1}^{-1} * (g * {g_2}^{-1}) = ({g_1}^{-1} * g) * {g_2}^{-1} = e * {g_2}^{-1} = {g_2}^{-1}.$$

Thus ${g_1}^{-1} = {g_2}^{-1}$, and the inverse of g is unique.

It follows directly from our definition of a group that the left and right cancellation laws hold.

Proposition G.1.8 If G is a group with a binary operation $*$, then the *left* and *right cancellation laws* hold. That is, for all $g, g_1, g_2 \in G$, if $g * g_1 = g * g_2$, then $g_1 = g_2$, and if $g_1 * g = g_2 * g$, then $g_1 = g_2$.

Proof Assume that $g * g_1 = g * g_2$. Our aim is to remove the g's and leave an equation involving g_1 and g_2. Therefore we multiply on the left by g^{-1}, the inverse of g. (We know this exists since G is a group.) We then have:

$$g^{-1} * (g * g_1) = g^{-1} * (g * g_2).$$

Since * is associative

$$(g^{-1} * g) * g_1 = (g^{-1} * g) * g_2,$$

which implies that

$$e * g_1 = e * g_2.$$

Finally, since e is the identity element, this implies that $g_1 = g_2$, as required.

Similarly the right cancellation law holds. Notice that it is not necessary for the binary operation on a group to be commutative. However, some groups are commutative.

Definition G.1.9 If the operation of the group $(G, *)$ is commutative, then we say $(G, *)$ is an *abelian* group. That is, it must satisfy conditions (1) to (4) of the group properties given in Definition G.1.1, as well as:

(5) for all $g, h \in G$, $g * h = h * g$.

That is, a group is commutative if the order in which the elements are multiplied does not matter.

These groups are termed abelian in honour of the Norwegian mathematician N.H. Abel (1802-1829). Abel made extensive use of the properties of commutative groups in his study of the roots of polynomial equations.

The group $(\mathbb{Z}_6, \oplus)$ is an abelian group, however $(D_3, \circ)$ where the binary operation is composition of movements on the equilateral triangle is not abelian. The fact is clear when one considers the following useful Cayley tables.

Loosely speaking, a **Cayley table** is an $n \times n$ table with a headline and a sideline. The headline and sideline contain the elements of the group in the same order $g_1, g_2, \ldots, g_n$, say. The identity element is usually listed first in the headline and sideline. The body of the table is made up as follows: the entry in row i and column j is $g_i * g_j$ for all i, j.

Example G.1.10 (i) The Cayley table of $(\mathbb{Z}_6, \oplus)$ is as follows.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Note that because $\mathbb{Z}_6$ has six elements, the Cayley table represents the group as a 6×6 array. Since $(\mathbb{Z}_6, \oplus)$ is an abelian group, row i of the Cayley table is the same as column i. The Cayley table makes it easy to find the inverse of a particular element; the inverse of 2 is 4 since row 2, column 4 is where we find the element 0 (the identity). Note that each element of the group occurs precisely once in each row and once in each column.

(ii) The Cayley table of $(D_3, \circ)$ is as follows.

$\circ$	e	r_1	r_2	m_1	m_2	m_3
e	e	r_1	r_2	m_1	m_2	m_3
r_1	r_1	r_2	e	m_3	m_1	m_2
r_2	r_2	e	r_1	m_2	m_3	m_1
m_1	m_3	m_2	m_2	e	r_1	r_2
m_2	m_1	m_2	m_3	r_2	e	r_1
m_3	m_2	m_1	m_1	r_1	r_2	e

Note that $(D_3, \circ)$ is not abelian as the Cayley table is not symmetric about the forward diagonal. That is, for eaxmple $r_1 * m_1 = m_2 \neq m_3 = m_1 * r_1$.

Exercises G.1

1. Prove that the binary operation $*$, defined in Example G.1.3 is associative.

2. Which of the following sets and binary operations form (i) groups, (ii) abelian groups? Justify your answers.

(a) $(\mathbb{Z}, -)$.

(b) $X = \{nz \,|\, z \in \mathbb{Z}\}$ under addition.

(c) $X = \{nz \,|\, z \in \mathbb{Z}\}$ under multiplication.

(d) $\mathbb{Z}_5$ under multiplication modulo 5.

(e) The set of $n \times n$ matrices with integer entries, under matrix addition.

(f) The set of $n \times n$ matrices with integer entries, under matrix multiplication.

3. Does the set $\{2, 4, 6, 8\}$ form a group under the operation multiplication modulo 10?

4. Does the set $\{1, 3, 6, 9, 12\}$ form a group under the operation multiplication modulo 15?

5. Explain why the set of equivalence classes modulo 16 does not form a group under the operation multiplication modulo 16.

6. Let $\mathbb{E}$ be the set of even integers. Show that $(\mathbb{E}, +)$ is a group. Does the set of odd integers form a group under addition?

7* Let $R = \{\frac{p}{q} \mid p = 2n + 1 \text{ and } q = 2m + 1, \text{ for } n, m \in \mathbb{Z}\}$; that is, R is the set of rational numbers which can be written with both the numerator and denominator odd. Prove that R is a group under the usual operation of multiplication. Is the set of rationals which can be written with even numerators and odd denominators a group under multiplication?

8* Which of the following statements are true and which are false? Briefly justify your answers.

(i) Let G be a group and $g, h \in G$. Then: (a) if $g^{-1} = h$, then $h^{-1} = g$; (b) $(g^{-1})^{-1} = g$; (c) $(gh)^{-1} = g^{-1}h^{-1}$; (d) $(gh)^{-1} = h^{-1}g^{-1}$.

(ii) Let G be a group such that for every $g \in G$, $g^2 = e$. Then: (a) $g_1g_2g_2g_1 = e$; (b) $g_1g_2g_1g_2 = e$; (c) $g_1g_2 = g_2g_1$.

9* Consider the following set of functions, each of which maps $T \to T$, for $T = \mathbb{R} - \{0, 1\}$:

$$\begin{array}{lll} f_1(x) = x; & f_2(x) = \frac{1}{1-x}; & f_3(x) = \frac{x-1}{x}; \\ f_4(x) = \frac{1}{x}; & f_5(x) = 1 - x; & f_6(x) = \frac{x}{x-1}. \end{array}$$

Show that these functions form a group under composition. Recall that the composition of two functions $f_i \circ f_j$ is taken to be $f_i(f_j(x))$.

10* Let a binary operation $\circ$ be defined on the rational numbers, $\mathbb{Q}$, by

$$a \circ b = a + b + ab.$$

Is $\mathbb{Q}$ a group under $\circ$?

11. For each of the following Cayley tables, state whether the table defines a group or not. Justify your answers.

$*$	x	y
x	x	y
y	y	y

$*$	x	y
x	x	y
y	y	z

$*$	x	y	z
x	x	y	z
y	y	x	z
z	z	z	x

$*$	x	y	z
x	x	y	z
y	y	z	x
z	z	x	y

*	A	B	C	D
A	A	D	C	B
B	B	A	D	C
C	C	B	A	D
D	D	C	B	A

12. Consider the set of three elements $G = \{a, b, c\}$. Let $(G, \circ)$ be a group based on G, such that

$$a \circ a = c \quad \text{and} \quad a \circ c = b = c \circ a.$$

Write down the Cayley for this group. Write down the identity element, and the inverse of each element. Is this group commutative?

13. Let G be a group and consider the Cayley table of G. Prove that each element of the group occurs precisely once in every row and once in every column of the Cayley table.

14.* Complete the following partial Cayley tables so as to form groups.

(i)

	E	W	X	Y	Z
E	E	W	X	Y	Z
W	W		Y		E
X	X			E	
Y	Y	Z		W	
Z	Z		W		Y

(ii)

	W	X	Y	Z
W			Z	
X				
Y				
Z			X	

16. Calculate the Cayley table for the group given in Exercise G.1.9.

Section G.2

Elementary Properties of a Group

In Example G.1.10 we gave the Cayley table of $(\mathbb{Z}_6, \oplus)$. If we focus our attention on the elements 0, 2, 4, then we have the following Cayley table:

$\oplus$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

We see that the set $\{0, 2, 4\}$ is closed under $\oplus$. Also $\oplus$ is associative, (because it is associative on the whole of $\mathbb{Z}_6$), the identity element is a member of the set and 4 is the inverse of 2, as 2 is the inverse of 4. In other words the set $\{0, 2, 4\}$ forms a group under the operation $\oplus$. We say that the subset $\{0, 2, 4\}$ is a *subgroup* of $\mathbb{Z}_6$.

Definition G.2.1 Let G be a group under the binary operation $*$. If a subset H of G is itself a group under the group operation, $*$, restricted to H, then H is said to be a *subgroup* of G. We use the notation $H \leq G$.

Example G.2.2
(i) We prove that the set $H = \{e, r_1, r_2\}$ is a subgroup of $(D_3, \circ)$.

Closure: Since H has only three elements, it is easy to check all possible combinations:

Associativity: We have $a \circ (b \circ c) = (a \circ b) \circ c$, for all $a, b, c \in D_3$. It automatically follows that $\circ$ is associative on a subset of D_3.

Identity: $e \in H$.

Inverses: The identity is always its own inverse, so we need only check r_1 and r_2. From the Cayley table given in Example G.1.10 (ii), we see that $(r_1 \circ r_2) = e = (r_2 \circ r_1)$. Therefore the inverse of r_1 is r_2 and *vice versa.*

Since the subset $H = \{e, r_1, r_2\}$ of $(D_3, \circ)$ is a group under the group operation $\circ$, H is a subgroup of $(D_3, \circ)$.

(ii) The group $(\mathbb{Q}^+, \cdot)$ is not a subgroup of $(\mathbb{Q}, +)$. The set $\mathbb{Q}^+$ is a subset of $\mathbb{Q}$, but the group operation multiplication, $\cdot$, of $\mathbb{Q}^+$ is not the same as the group operation addition, $+$, of $\mathbb{Q}$.

Let H be a subgroup of a group G. If H is not equal to the entire group G, then H is said to be a *proper subgroup* of G. We say H is a *nontrivial subgroup* if H is not equal to $\{e\}$; the subgroup $\{e\}$ is said to be the *trivial subgroup* of G. All other subgroups are termed *proper nontrivial subgroups.* The set $\{0, 3\}$ is a proper subgroup of $(\mathbb{Z}_6, \oplus)$, as is $\{0, 2, 4\}$. Other examples are $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

Consider a group G. The group operation is associative on G, therefore it must be associative on all subsets of G. Thus when proving that a subset H is a subgroup of G, we need only show that H satisfies the three conditions (1), (3) and (4) of Definition G.1.1. This is proved formally in Lemma G.2.3.

Lemma G.2.3 Let G be a group with binary operation $*$ and identity element e. A subset H of G is a subgroup of G if and only if:

(a) $e \in H$;

(b) for all $x \in H$, $x^{-1} \in H$;

(c) for all $x, y \in H$, $xy \in H$.

Proof Let H be a subgroup of G. By definition, H is a group under the restricted operation (that is, the operation of the group G). Denote the identity of H by e_1. Since $e_1 \in G$ we have $ee_1 = e_1$. But $e_1e_1 = e_1$, so $e = e_1$ and (a1) follows. We now use the uniqueness of the inverses in G to verify (b) and (c) follow by closure.

Conversely, assume H is a subset of G satisfying (a), (b) and (c). We know that $x * (y * z) = (x * y) * z$ for all $x, y, z \in G$ and $H \subseteq G$, so $*$ must be associative on H. Therefore H is a group under the operation $*$. It follows that H is a subgroup of G.

When dealing with subgroups an obvious question to ask is: what is the smallest subgroup which contains a particular element a? The subgroup must be closed and so it must contain all powers of a and their inverses. (Recall that that the n^{th} power of a is given by $a^n = a * a * \ldots * a$, where $*$ is the binary operation of the group; we shall denote $(a^n)^{-1}$ by a^{-n}.) Therefore the smallest subgroup H of G containing element a is $H = \{a^n \mid n \in \mathbb{Z}\}$. The case $H = G$ is of special significance.

Definition G.2.4 Let G be a group and a an element of G. Let $\langle a \rangle = \{a^n \in G \mid n \in \mathbb{Z}\}$. The set $\langle a \rangle$ forms a subgroup and is called the *cyclic subgroup* of G generated by a. If $\langle a \rangle = G$, for some $a \in G$, then G is said to be *cyclic* and a is said to be a *generator* of G.

Example G.2.5 Consider the element 5 in the group $(\mathbb{Z}_6, \oplus)$. Then this group is cyclic with generator 5, for:

$$\begin{aligned}
5^1 &= 5 \\
5^2 &= 5 \oplus 5 = 4 \\
5^3 &= 5 \oplus 5 \oplus 5 = 3 \\
5^4 &= 5 \oplus 5 \oplus 5 \oplus 5 = 2 \\
5^5 &= 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 = 1 \\
5^6 &= 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 = 0.
\end{aligned}$$

A group with a finite number of elements is said to be a *finite group*; otherwise it is an *infinite group*. A finite group G containing n elements is said to be of *order* n, written $|G| = n$ or $o(G) = n$. The *order of an element* g in G, $o(g)$, is defined to be the least positive integer n, if such an integer exists, such that $g^n = e$. If no such integer exists, then the order of the element is said to be *infinite*. If any two distinct powers of g are equal then by using the cancellation law we see that g has finite order. TConversely, if g has infinite order all its powers are distinct.

It should be noted that if $o(G) = n$, then it does *not* follow that the order of each element of G is n. In most cases this will not be so. Consider the element 2 of the group $(\mathbb{Z}_6, \oplus)$ given in Example G.1.2. The order of this group is 6; however $2^3 = 0$, and 0 is the identity of this group, so $o(2) = 3$. It could also be pointed out that $2^6 = 0$ or $2^9 = 0$ but 6 and 9 are not the smallest such integers and so do not give the order of the element 2. Alternatively we may define the order of an element g in terms of the smallest subgroup containing g.

Lemma G.2.6 Let H be a subgroup of a group G and g be an element of G. If $H = \{g^r \mid r \in \mathbb{Z}\}$, then $o(H) = o(g)$.

Proof If g is of infinite order and we consider the set $H = \{g, g^2, \ldots, g^n, \ldots\}$, then the set H has infinite order as well. We need only consider the case where $o(g)$ is finite. The set $\{g, \ldots, g^{o(g)}\}$ is a subset of H, which implies that $o(g) \leq o(H)$. Therefore it suffices to show $o(H) \leq o(g)$. We must show that for any $m \in \mathbb{Z}$, there is an n where $0 \leq n < o(g)$, such that $g^m = g^n$. By the division algorithm, there exist integers a and b such that $m = a \cdot o(g) + b$, where $0 \leq b < o(g)$. Thus

$$g^m = g^{a \cdot o(g) + b} = \left(g^{o(g)}\right)^a g^b = e^a g^b = g^b,$$

where $0 \leq b < o(g)$. Consequently $o(H) \leq o(g)$ and the result follows.

Example G.2.7 Take $(\mathbb{Z}_6, \oplus)$. As noted previously, the order of the element 2 is 3. Alternatively, $\langle 2 \rangle = \{2, 4, 0\}$ is the subgroup generated by element 2. It contains three elements. Therefore the order of element 2 is three.

If you take further studies in group theory you will study formal techniques for distinguishing between different types of groups. However for now it is enough to note that even if two groups have the same order their basic structure may be different. For example, any one of the following reasons is enough to show that $(\mathbb{Z}_6, \oplus)$ and $(D_3, *)$ are essentially different groups.

The group $(\mathbb{Z}_6, \oplus)$ is abelian, but the group $(D_3, \circ)$ is not.

The group $(\mathbb{Z}_6, \oplus)$ is cyclic, but the group $(D_3, \circ)$ is not.

The group $(\mathbb{Z}_6, \oplus)$ has four subgroups, but the group $(D_3, \circ)$ has six subgroups.

The group $(\mathbb{Z}_6, \oplus)$ has two elements of order 6, but $(D_3, \circ)$ has none.

Exercises G.2

1. Consider the set $T = \{1, 2, 3, 4, 5, 6\}$.

Prove that T forms a group under multiplication modulo 7.

(ii) Prove that the subset $S = \{1, 2, 4\}$ is a subgroup of T under multiplication modulo 7.

(iii) Find all other proper subgroups of T.

(iv) Does S contain any proper subgroups?

(v) Write down the orders of T and S.

(vi) Write down the order of each of the elements of T.

(vii) Is T cyclic? If so, find all generators of T.

(viii) Is S cyclic? If so, find all generators of S.

2. Consider the two groups given by the following Cayley tables.

$*$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

$*$	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

(i) What is the order of each of these two groups?

(ii) What is the order of each element in each group?

(iii) Does either group contain any non-trivial subgroups? If so, what are they?

(iv) Are either of these groups cyclic? If so name the generator(s).

3. Let $X = \{x \mid (\exists z \in \mathbb{Z})(x = 3z)\}$. Prove that X is a subgroup of $(\mathbb{Z}, +)$. What is the order of X?

5. Let G be a group and let $g \in G$. If $g = g^{-1}$, what are all the possible values of the order of g?

Section G.3
Definitions and Examples of Finite Fields

In the previous sections we investigated sets with *one* binary operation defined on them; in particular we explored the properties of such systems which satisfired the four requirements of closure, associativity, identity and inverse, and so were groups. When we deal with sets such as the integers, $\mathbb{Z}$, the rationals, $\mathbb{Q}$, or the real numbers, $\mathbb{R}$, we commonly encounter *two* binary operations on these sets, namely addition and multiplication. Therefore before closing this chapter we would like to present the reader with the definition of a field.

Definition G.3.1 A *field* $(F, +, \cdot)$ is a set F together with two binary operations $+$ and $\cdot$ (usually called, respectively, addition and multiplication) satisfying:

- $(F, +)$ is an abelian group;
- $(F - \{0\}, \cdot)$ is an abelian group), where 0 denotes the additive identity;
- for all a, b, c in F, $a \cdot (b + c) = a \cdot b + a \cdot c$; that is the distributive law holds in F.

Examples of fields are $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_p, \oplus, \otimes)$ where p is a prime and $\oplus$ and $\otimes$, repectively, are the operations of addition and mutiplication modulo p. But care must be take, for example, $(\mathbb{Z}_6, \oplus, \otimes)$ is not a field. To see this refer back to Exercise G.1.2 Question 3 where it was shown that not all non-zero elements of $\mathbb{Z}_6$ have multiplicative inverses.

Exercises G.1: Solutions

1. We show that $a * (b * c) = (a * b) * c$ for all binary strings $a, b, c \in B$. So let $a = a_1 a_2 \dots a_n$, $b = b_1 b_2 \dots b_n$ and $c = c_1 c_2 \dots c_n$, where each a_i, b_i, c_i is 0 or 1. Fix an index m and consider the m-th digit for the product on each side of the above equation. We have the following cases:

(a) $a_m = b_m = c_m = 1$. Then $(a * (b * c))_m = 1$ and $((a * b) * c)_m = 1$.

(b) $a_m = b_m = 1$, $c_m = 0$. Then $(a * b)_m = 1$, so $((a * b) * c)_m = 0$; and $(b * c)_m = 0$, so also $(a * (b * c))_m = 0$.

(c) $a_m = 1$, $b_m = c_m = 0$. Then $(a * b)_m = 0$, $(b * c)_m = 1$, so that $((a * b) * c)_m = 1 = (a * (b * c))_m$.

(d) $a_m = 1$, $b_m = 0$, $c_m = 1$. Then $(a * (b * c))_m = 0 = ((a * b) * c)_m$.

(e) The remaining cases are obtained by interchanging 1 and 0 in the above, and the associativity then follows.

2. Note that if any of (a) to (f) is not a group, then it is certainly not an abelian group.

(a) ($\mathbb{Z}$, -) is not a group, since $-$ is not associative.

(b) Addition on X is closed, associative, has an identity $0n$, inverse $(-z)n$ and is commutative, so $(X, +)$ is an abelian group.

(c) $X = \{nz \mid z \in \mathbb{Z}\}$ under multiplication. This is closed and associative, but has no identity unless $n = 1$ or 0, and has no inverses unless $n = 0$ (in which case we have a one-element group). So, in general we only have a (trivial) group (which is abelian) for $n = 0$.

(d) $\mathbb{Z}_5$ under multiplication modulo 5 is closed, associative and has an identity [1], but [0] has no inverse. So it is not a group.

(e) The set of $n \times n$ matrices with integer entries under matrix addition forms an abelian group since addition is componentwise, so it inherits all the properties of $\mathbb{Z}$.

(f) The set of $n \times n$ matrices with integer entries, under matrix multiplication. This is closed and associative (by properties of matrix multiplication) and the identity matrix belongs to the set. However, the inverse of a matrix with integer entries will not in general have integer entries. So this is not a group.

3. The set {2, 4, 6, 8} is a group under the operation of multiplication modulo 10, because (i) the set is closed for this operation, which is necessarily associative (because multiplication of integers is associative); (ii) 6 is the identity element (check!); (iii) $2^{-1} = 8, 4^{-1} = 4, 8^{-1} = 2$. Note that $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 6 =$ the identity element for this group. So this is what we call a cyclic group, generated by the element 2.

4. The set $\{1, 3, 6, 9, 12\}$ does not form a group under the operation multiplication modulo 15 since (for example) $3 \times 6 \equiv 3 \pmod{15}$ so 3 cannot have an inverse (otherwise we would have $6 \equiv 1 \pmod{15}$).

5. The set of equivalence classes mod 16 does not form a group under the operation multiplication modulo 16 because (for example) $4 \times 4 \equiv 0 \pmod{16}$, so 4 cannot have an inverse.

6. **Closure**: The sum of two even integers is even, so we have closure.

Associativity: This follows from the associativity of $+$ on the whole of $\mathbb{Z}$.

Identity: $0 \in \mathbb{E}$, so $\mathbb{E}$ has an identity for addition.

Inverse: If $n \in \mathbb{E}$, then $-n \in \mathbb{E}$, so we have inverses.

The set of odd integers does not form a group under addition because it is not closed (since odd plus odd is not an odd integer but is an *even* integer!).

7*. We have $R = \{p/q \mid p = 2n + 1 \text{ and } q = 2m + 1, \text{ for } n, m \in \mathbb{Z}\}$; that is, R is the set of rational numbers which can be written with both the numerator and denominator odd. To prove that R is a group under the usual operation of multiplication it suffices to note that:
(i) the set is closed for multiplication, since the set of odd integers is closed because odd times odd is odd;
(ii) $1 = 1/1$ is the identity element;
(iii) the inverse of each element is the reciprocal fraction, that is, the inverse of p/q is q/p; and
(iv) associativity is guaranteed because the full set of rational numbers under multiplication is associative.

For the rationals with even numerators and odd denominators we do not get a group under multiplication, because (ii) fails — there is no identity.

8*. (i) (a) True: $(g^{-1} = h) \to (gh = e = hg) \to h^{-1} = g$.

(b) True: this is just another way of writing the previous result.

(c) False (unless G is abelian): for a nonabelian group $(gh)^{-1} = h^{-1}g^{-1}$ (see next result).

(d) True: $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e$ and $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e$, so $(gh)^{-1} = h^{-1}g^{-1}$).

(ii) (a) True: $g_1(g_2g_2)g_1 = g_1eg_1 = g_1g_1 = e$.

(b) True: $g_1g_2g_1g_2 = (g_1g_2)^2 = e$.

(c) True: from (a) and (b) we have $g_1g_2g_1g_2 = g_1g_2g_2g_1$, so cancellation yields $g_1g_2 = g_2g_1$.

9*. Here is the multiplication table for this system:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_5	f_6	f_4
f_3	f_3	f_1	f_2	f_6	f_4	f_5
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

From the table we see *closure* (the entries are all from the original set), *identity* (f_1 is the identity) and *inverses* ($f_1^{-1} = f_1$, $f_2^{-1} = f_3$, $f_3^{-1} = f_2$, $f_4^{-1} = f_4$, $f_5^{-1} = f_5$, $f_6^{-1} = f_6$). *Associativity* holds since composition of relations and functions is associative. Hence this is a group.

10*. **Closure**: Since $\mathbb{Q}$ is closed under addition and multiplication, it is closed under $\circ$.

Associativity: $a\circ(b\circ c) = a\circ(b+ci+bc) = a+(b+c+bc)+a(b+c+bc) = (a+b+ab)+c+(a+b+ab)c$, and $(a\circ b)\circ c = (a+b+ab)\circ c = (a+b+ab)+c+(a+b+ab)c$. (Properties of $\mathbb{Q}$ used here.) Hence $\circ$ is associative.

Identity: $a \circ 0 = a + 0 + a0 = a = 0 \circ a$. Hence 0 is an identity element in $\mathbb{Q}$ for $\circ$.

Inverse: Say a' is to be an inverse for a. Then $a \circ a' = a + a' + aa' = 0$, so $a'(1 + a) = -a$, and this has no solution for a' when $a = -1$. Hence this is NOT a group.

11. The first is not a group because y has no inverse (here x is clearly the only identity element).
The second is not a group, because it is not closed.
The third is not a group because the last row and last column each contain two answers z; this would violate cancellation (which we have in a group thanks to inverese: if $x * z = y * z$ as here, then multiplying on the right by z^{-1} we'd get $x = y$, which is not true!).
The fourth is a group; the table is the same as that for the integers modulo 3 under addition.
The fifth is not a group because there is no identity (A is a right identity, but not a left); also the associative law does not hold ($B(CD) = C \neq (BC)D = A$).

12. The identity element must be b; it cannot be a because $a\circ a = c$; it cannot be c because $a \circ c = b$. Thus the Cayley table is

	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Then the inverse of each element may be read off from the table: $a^{-1} = c, c^{-1} = a$. We note that $G = \{b, a, a^2\}$ since we must also have $a^3 = a^2 \circ a = c \circ a = b$ and hence $c = a^2$. It follows that this group is commutative (this can also be seen from the table).

13. Let $G = \{g_1 = e, g_2, \ldots, g_n\}$ be a group of n elements and consider the Cayley table of G. Suppose that some row has two elements equal. This means that we have $x * y = x * z$ for some x, y and z (so in row x we have the entries in columns y and z the same, some element X).

$*$	$\ldots$	y	$\ldots$	z	
$\vdots$					
x		X		X	

Then since this is a group, x^{-1} exists; multiply on both sides on the left by this:

$$\begin{aligned} x * y &= x * z, \\ x^{-1} * (x * y) &= x^{-1} * (x * z) \\ \text{so from associativity, } (x^{-1} * x) * y &= (x^{-1} * x) * z \\ \text{so} \quad e * y &= e * z \text{ (where } e \text{ is the identity)} \\ \text{so} \quad y &= z. \end{aligned}$$

This means that in fact the two columns headed by y and z cannot be different, so in a group the Cayley table never contains two identical elements in any of its rows.

For columns, we repeat this, starting with the assumption that $s*t = u*t$, so column t contains (in rows s and u) two entries the same. So this time we'll multiply on the *right* by t^{-1}, and repeat the above argument.

14*. (i) This is filled in by using the rules that no element can occur twice in the same row or column (the cancellation laws):

	E	W	X	Y	Z
E	E	W	X	Y	Z
W	W	X	Y	Z	E
X	X	Y	Z	E	W
Y	Y	Z	E	W	X
Z	Z	E	W	X	Y

(ii) Here we have to be a little more cunning, and first observe that the only candidate for an identity is X. Once that is in, we can finish the process as for (i).

	W	X	Y	Z
W	X	W	Z	Y
X	W	X	Y	Z
Y	Z	Y	W	X
Z	Y	Z	X	W

15. See the answer to Ex G.1.9!

Exercises G.2: Solutions

1. (i) T is closed, associative and 1 is the identity, from the definition and properties of modular arithmetic. Also $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 4$, $4^{-1} = 2$, $5^{-1} = 3$, $6^{-1} = 6$, so we have inverses. Thus T is a group.

(ii) $S = \{1, 2, 4\}$ contains 1 and inverses for all elements (since $2 \times 4 = 1$) and is closed (since $2 \times 2 = 4$, $4 \times 4 = 2$, $2 \times 4 = 1$). Hence S is a subgroup of T.

(iii) The other proper subgroups of T are $\{1\}$ and $\{1, 6\}$.

(iv) The only proper subgroup of S is $\{1\}$.

(v) $o(T) = 6$ and $o(S) = 3$.

(vi) $o(1) = 1$, $o(2) = 3$, $o(3) = 6$, $o(4) = 3$, $o(5) = 6$, $o(6) = 2$.

(vii) T is cyclic, since it has elements of order 6 and T is of order 6. It can be generated by 3 or 5 (since these elements have order 6).

(viii) S is cyclic, since it has elements of order 3, and S is of order 3. It can be generated by 2 or 4, since these elements have order 3.

2. (i) Each of these two groups has order 4.

(ii) In the first group, $o(I) = 1$, $o(A) = o(B) = o(C) = 2$. In the second group $o(I) = 1$, $o(B) = 2$, $o(A) = o(C) = 4$.

(iii) Besides itself, the first group contains three non-trivial subgroups, $\{I, A\}$, $\{I, B\}$ and $\{I, C\}$. Besides itself, the second group contains only one non-trivial subgroup, $\{I, B\}$.

(iv) The second group is cyclic; it can be generated by A or C.

3. $X \neq \emptyset$, since $0 \in X$. Let $x = 3z$ and $y = 3w$ be elements of X. Then $x - y = 3z - 3w = 3(z - w) \in X$ (since $z - w \in \mathbb{Z}$). Hence $X \leq (\mathbb{Z}, +)$. The subgroup X has infinite order.

5. If $g = g^{-1}$, the possible values of the order of g are 1 or 2, depending on whether $g = e$ or not. (For we know that $g * g^{-1} = e$, so here we have $g * g = e$, which means that either $g = e$ or else $g \neq e$, in which case g has order 2.)