Keele UNIVERSITY

MAT-20025: Abstract Algebra

F. Olukoya

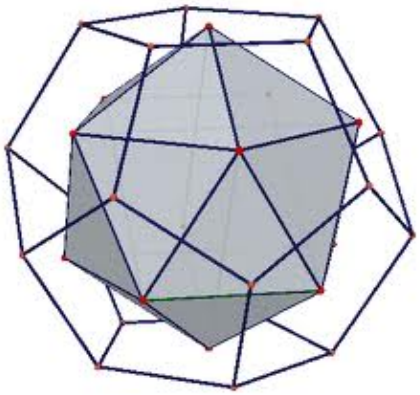


Table of contents

Welcome

Welcome to *MAT-20025: Abstract Algebra*. This module is compulsory for Single Honours BSc and MMath and optional for Combined Honours BSc. The majority of the module will be devoted to introducing 'Group Theory'. Groups are fundamental algebraic objects that crop up in a variety of different contexts: from crystal structures, to quantum physics and even in understanding DNA folding in biology. The following rule of thumb applies: wherever there is 'symmetry' there is a group. The remainder of the module will be devoted to considering other algebraic structures.

Structure

The module is comprised of the following parts:

Part I: An introduction to group Theory

1. Examples of groups.
2. The group concept and elementary group theory.
3. Lagrange's Theorem.
4. Homomorphisms and isomorphisms.
5. Permutation groups.
6. Structure of finite abelian groups.
7. Applications to Number Theory.

Part II: Other algebraic structures

7. Rings
8. Fields

Intended Learning Outcomes (ILO's)

Upon successful completion of this module you will be able to:

- define and identify abstract algebraic structures and concepts including binary operations, groups, rings, fields and permutations;
- select and apply concepts of group theory to mathematical problems;
- state and prove theorems involving groups, rings and fields, and synthesise theoretical material and concepts to solve problems.

Prerequisites for

This module if a prerequisite for:

- MAT-30013 Group Theory;
- MAT-30038 Number Theory and Cryptography;
- MAT-30045 Linear Algebra and Rings;
- MAT-40016 Fields and Galois Theory.

Lecture notes and recommended reading

A full-set of gapped notes is available on KLE[1]. The gaps will be revealed in due course as the term progress.

In addition, the following non-essential texts are recommended as providing more in-depth discussion/ a different point of view on topics covered in lectures as well as additional practise examples.

- Peter J. Cameron: Introduction to Algebra (2^{nd} edition).
- John B. Fraleigh: A First Course in Abstract Algebra (7^{th} edition).

[1]These are based on Neil Turner's excellent set of notes

- R. B. J. T. Allenby: Rings, Fields and Groups: an Introduction to Abstract Algebra (2^{nd} edition).

Copies of the above are available in the library. In addition, Cameron is available as an e-book.

Logistics

Lectures

The lecture material will be delivered by way of 2.5 standard, face-to-face lectures each week (3 in odd weeks and 2 in even). If you have any questions while going through the content then *do* email me f.a.olukoya@keele.ac.uk. I am more than happy to arrange a meeting over teams or in person.

Example classes

In weeks 2, 4, 6, 8, and 10 the Monday class will be split into two smaller examples classes (running at different times) and these two sessions will be given over to the study of specified problems which can be found at the end of the relevant section in the notes. You are expected to attempt the assigned problems prior to each example class; this is an important part of your learning process. As a guide, you should about invest approximately 5 hours of active-working time preparing for an example class. Please note that you should only attend the example class to which you have been allocated.

The table below details the problem sheets that will be covered in each example class:

Note that there will be no example class covering Sheets 8 and 9. Solutions to these problem sheets will be revealed at the appropriate time. Do ensure you attempt the problems and understand the solutions as the content will be examinable.

Table 1: Example Classes

Example Class	Problem Sheet
Week 2	Sheet 1
Week 4	Sheets 2 & 3
Week 6	Sheets 4 & 5
Week 8	Sheet 6
Week 10	Sheet 7

Timetable

Details of all sessions (lectures and examples classes) will be available on your eVision timetable. Please make sure that you have the correct day, time and room for each session. You should check this regularly as there are occasionally changes, particularly in the first couple of weeks of the semester.

Table 2 displays a detailed schedule for the semester.

Attendance requirements

You are expected to attend ***all*** scheduled teaching activities.

Lecturers

This semester Dr. Feyisayo (Shayo) Olukoya will be the lecturer on the module. As mentioned above you can reach me by **email**; you should also feel free to arrange an in-person meeting my office is **Mac2.30** in the Mackay Building; meeting virtually over teams is also an option.

KLE

All resources for the module (lecture notes, problem sheets, solutions e.t.c) will be made available on KLE at the appropriate time.

Assessment

Continuous Assessment

This will be made up of two week-long take-home assessments (each contributing 15% of the overall module mark). For each assessment, you would normally not be expected to invest more than 5 hours of active-working time. An assessment schedule will be available on the Mathematics Noticeboard on the KLE. Note that the first assessment is called an *assignment*, whilst the second is called a *coursework*; this nomenclature is purely for administrative convenience.

Formative assessment

At the end of each chapter in the notes, you will find problem sheets with questions addressing the content covered in that chapter. Although these sheets do not contribute to the continuous assessment component, you are strongly encouraged to attempt them as they are designed to consolidate your understanding and enhance your problem-solving skills. Full solutions are provided and will appear after the sheet or sheets have been covered in example classes.

Final Exam

This comprises 70% of the module mark. It is an unseen, closed-book examination, with all questions being compulsory. The use of calculators is governed by the University regulations. The examination will require you to state definitions, state (and possibly prove) results, and apply these to solving problems. You should be able to state every definition and result in the module unless they are marked in the lecture notes as non-examinable.

Student Support

For advice on academic and non-academic issue (resonable adjutsments, financial, international, personal or health matters) please contact Student Services. You can book a virtual appointment or email student.services@keele.ac.uk.

You can also contact the school's Student Experience and Support Officer by emailing student services student.services@keele.ac.uk.

Table 2: Timetable

Week Beginning	Day	Chapter	Material
23 Jan	M	1	Introduction and prerequisites
	T	2	Symmetries
	Thu	2	Congruences, Matrices and Roots of Unity
30 Jan	M		**Examples Class 1**
	T	2	Binary Operations
	Thu	3	The group concept
6 Feb	M	3	Elementary group theory & subgroups
	T	3	Subgroups
	Thu	3	Cyclic subgroups and cyclic groups
13	M		**Example Class 2**
	T	4	Cosets
	Thu	4	Lagrange's Theorem ***(Assignment)***
20	M	5	Isomorphisms
	T	5	Properties of Isomorphisms
	Thu	5	Example of isomorphisms ***(Assignment due)***
27	M		**Example Class 3**
	T	5	Group homomorphisms
	Thu	5	Image, preimage and kernel
6 Mar	M	6	Introduction to permutations
	T	6	Cycle decomposition and orbits
	Thu	6	Transpositions
13 Mar	M		**Example Class 4**
	T	6	Cayley's Theorem
	Thu	7	Structure of cyclic groups
20	M	7	Direct product of groups
	T	7	Structure of finite abelian groups
	Thu	7	Sylow's First Theorem
17 Apr	M		**Example Class 5**
	T	8	Applications to Number theory: introduction
	Thu	8	Congurence and residue classes ***(Coursework)***
24 Apr	M	8	Reduced residue system
	T	8	Fermat's Little Theorem/Euler's Theorem
	Thu	8	Wilson's Theorem ***(Coursework due)***
1 May	T	9	Rings and Subrings
	W	9	Homomorphism, Integral Domains & Division rings
	Thu	9	Fields
8			***Exams***

Part I

Groups and applications

Chapter 1

Pre-requisites

We begin with a very brief reminder of some important ideas from the theory of sets and functions from first-year Algebra. We shall return to these ideas frequently during the course of this module. We also have a reminder of some of the basics of congruencies.

Sets

Recall that a set is a collection of objects which may be finite or infinite in size. For our purposes, the order of the elements of a set is irrelevant and we ignore repeated elements. For example,

$$\begin{aligned} \{a, b, c, d\} &= \{b, d, c, a\} = \dots \\ \{a, a, c, b, a, c\} &= \{a, b, c\}. \end{aligned}$$

We use different notation for sets, depending on the size of the set and context. In addition, we shall frequently use the 'set-builder' notation. Some examples are:

- the set of natural numbers

$$\{0, 1, 2, \ldots\} \text{ or } \mathbb{N}.$$

- the set of even numbers

$$\{m \in \mathbb{Z} : m = 2k, k \in Z\} = \mathbb{E}.$$

- the set of numbers that are both even and odd

$$\emptyset = \{\}.$$

> **Note**
>
> - The set $\{\emptyset\} = \{\{\}\}$ is not empty since it contains the empty set!
> - Not every thing you can write down is a set! This is not an issue we will worry about in this course but it is worth knowing. A famous example of a non-set is *'The set of all sets that do not contain themselves'*. This is *Russel's Paradox* and you can read more about Russel and his paradox by following the link.

We use $x \in S$ to denote that x is an element of the set S and $A \subseteq S$ to denote that A is a subset of S (so, A contains only a sub-collection of things that are in S and nothing that is not in S and, as a consequence, for any set S, both $\emptyset$ and S itself are subsets of S). Note that $A \subset S$ means that A is a *proper* subset of S, that is, A cannot be S itself. Remember that if we wish to demonstrate that two sets, X and Y say, are equal, then it is necessary to show both that $X \subseteq Y$ and $Y \subseteq X$. If S and T are sets then we denote the set difference $S \backslash T$. This, itself, is a set and contains all of the elements that are in S but not in T. So, for example, we could denote the set of non-zero integers as $\mathbb{Z} \backslash \{0\}$ (note that this operation is defined with respect to two sets, so $\mathbb{Z} \backslash 0$ would be nonsense).

The Cartesian product of two sets, A and B say, is denoted $A \times B$ and is the set of all possible *ordered* pairs where the first element of the pair comes from set A and the second element

comes from set B. Since these are ordered pairs the order of the elements within each pair is critical, though the order in which the pairs themselves appear in $A \times B$ is irrelevant.

Example 1.1. Let $A = \{1, 2, 3\}$ and $B = \{s, t\}$. Then

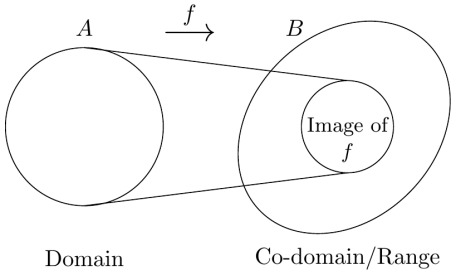
$$\begin{aligned} A \times B &= \{(1,s),(1,t),(2,s),(2,t),(3,s),(3,t)\} = \{(a,b) : a \in A, b \in B\} \\ B \times A &= \{(s,1),(s,2),(s,3),(t,1),(t,2),(t,3)\} = \{(b,a) : b \in B, a \in A\}. \end{aligned}$$

Functions

A function is a rule that determines a mapping from one set (the domain) to another set (the co-domain). The image of a function is the subset of the codomain onto which all elements from the domain are mapped. Recall that for a function to be well-defined it must be the case that the function can map a single element of the domain only onto a single element of the co-domain.

We say that a function, $f : A \to B$ is *injective* if and only if $f(a) = f(b) \implies a = b$ for all $a, b \in A$. A function is *surjective* if and only if $\forall b \in B \; \exists \; a \in A$ such that $f(a) = b$. In effect this says that the image of a surjective function coincides exactly with its co-domain. We say that a function is *bijective* if and only if it is both injective and surjective. Recall that any function that is bijective has a well-defined inverse.

Example 1.2.



Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$ for all $x \in \mathbb{R}$. Observe that f is not injective since

$f(x) = f(-x)$ for any $x \in \mathbb{R}$. In particular, $f(2) = f(-2)$.

We can, however, make f injective by changing its domain. More precisely, the map $f_1 : \mathbb{R}_{\geq 0} : \mathbb{R}$ by $f_1(x) = x^2$ is injective.

Now both f and f_1 are not surjective since the image of f equal to the image of f_1 is precisely $\mathbb{R}_{\geq 0}$. In particular, there is no x either in the domain of f or the domain of f_1 such that $f(x) = -1$.

We can however make f_1 surjective by changing is range. In particular, the map $f_2 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ by $f_2(x) = x^2$ is surjective. For $x \in \mathbb{R}_{\geq 0}$, the element $\sqrt{x} \in \mathbb{R}_{\geq 0}$ satisfies $f_2(\sqrt{x}) = x$.

Now as f_2 is injective as well, it is therefore a bijection. This means that f_2 is invertible. The map $f_2^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ by $f_2(x) = \sqrt{x}$ is the inverse of f_2.

Congruences

Recall that for any integers a and b and any positive integer m, then we define $a \equiv b \pmod{m}$ to mean that $m \,|\, (a - b)$. This is equivalent to saying that $a \equiv b \pmod{m}$ if and only if both a and b leave the same principal remainder on division by m.

Example 1.3.

- $3 \equiv 15 \pmod{6}$ since $6|(3 - 15)$, alternatively, since both 3 and 15 have remainder 3 upon division by 6.
- $0 \equiv 16 \pmod{4}$.
- $8 \equiv -4 \pmod{3}$.

Recall that when we do arithmetic modulo some positive integer m, we can either do the usual arithmetic first and then reduce modulo m or, more conveniently, reduce modulo m first and then do the arithmetic.

Example 1.4.

- $15 + 38 \pmod 6 = 53 \pmod 6 \equiv 5 \pmod 6$ and

$$\begin{aligned} 15 + 38 \pmod 6 &= 15 \pmod 6 + 38 \pmod 6 \\ &\equiv 3 \pmod 6 + 2 \pmod 6 \\ &\equiv 5 \pmod 6 \end{aligned}$$

-

$$\begin{aligned} 28 \times 117 \pmod 5 &\equiv 3 \times 2 \pmod 5 \\ &\equiv 6 \pmod 5 \\ &\equiv 1 \pmod 5. \end{aligned}$$

1.1 Problem Sheet 1

For the example class in Week 2; covers Chapter 1 material.

Question 1.1

Let A be the set $\{x, \{1, x\}, \{3\}, \{\{1, 3\}\}, 3\}$. Which of the following statements are true and which are false?

- $x \in A$.
- $\{x\} \notin A$.
- $\{1, x\} \subseteq A$.

- $\{3, \{3\}\} \subseteq A$.
- $\{1, 3\} \in A$.
- $\{\{1, 3\}\} \subseteq A$.
- $\{\{1, x\}\} \subseteq A$.
- $\{1, x\} \notin A$.
- $\emptyset \subseteq A$.

Show Solution 1.1 on P185

Question 1.2

Let $J = \{1, 2, 5, 6\}, K = \{3, 6, 7, 8\}, L = \{4, 5, 7\}, M = \{1, 4, 6, 8\}$ and $N = \{6, \{8\}\}$. Find the following sets:

- $J \cap K$.
- $(K \cap M) \cup L$.
- $\mathcal{P}(L)$.
- $L \times N$.
- $\{x + y \,|\, x \in J, y \in L\}$.
- $\{x \,|\, x \in L \times J, x \notin L \times M\}$.

Show Solution 1.2 on P186

Question 1.3

Show that, for any integers a, b and c,

$$a \mid b \text{ and } b \mid c \;\Rightarrow\; a \mid (b+c).$$

Show Solution 1.3 on P187

Question 1.4

Let $m > 0$ be a fixed integer and a, b and c be any integers. Prove that

$$a \equiv b \pmod{m} \;\Rightarrow\; ac \equiv bc \pmod{m}.$$

Is the converse true?

Show Solution 1.4 on P187

Chapter 2

Symmetry, Congruences, Matrices, and Roots of Unity

2.1 Symmetry

Suppose we take a square in the plane. If we rotate that square through an angle of $\pi/2$ radians about its centre, then it looks exactly the same as it did before - in the absence of any labelling we cannot tell that the square has been rotated and we say that a square has rotational symmetry. We may well ask whether there are symmetries other than the aforementioned rotation that leave the square unchanged. In general we are interested in geometrical transformations that leave shapes 'unchanged'.

We need to make the idea of a geometrical transformation more precise. The type of geometrical transformation that we have in mind can move a figure around, but must not change its size or shape, that is it must not alter distances or angles. In fact, a transformation which leaves distances unaltered must also leave angles unchanged, so all we need to build into our definition of a geometrical transformation is that it leaves distances unchanged. Such transformations are called *symmetries*.

Definition 2.1 (Symmetry)**.** A *symmetry* of the plane is a bijective mapping $f : \mathbb{R}^2 \to \mathbb{R}^2$

which preserves distances, that is $\forall\ x, y \in \mathbb{R}^2$ the distance between $f(x)$ and $f(y)$ equals the distance between x and y.

The symmetries of the plane include translations, rotations about a point, and reflections in a line. For our purposes we are not concerned with symmetries that move the location of the shape in space and, hence, our attention will be restricted only to rotations and reflections.

Example 2.1. The symmetries of an equilateral triangle

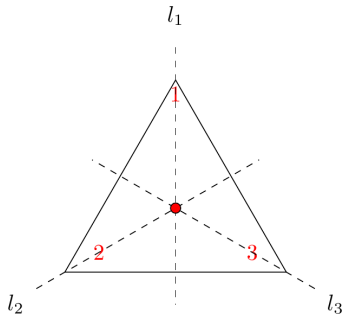


Figure 2.1: Equilateral Triangle

What are the symmetries of an equilateral triangle?

There are three possible lines of reflection and three rotations about the centre through $2\pi/3$ radians. Conventionally rotations are measured in the anticlockwise direction.

Thus the symmetries are:

$e = r_3$ – The identity map;

r_1 – anticlockwise rotation by $2\pi/3$ radians;

r_2 – anticlockwise rotation by $4\pi/3$ radians;

s_1 – reflection in the line l_1;

s_2 – reflection in the line l_2;

s_3 – reflection in the line l_3.

> **Note**
>
> The rotation r_3 is a rotation of $6\pi/3 = 2\pi$ radians is the 'identity mapping', in particular we can treat the rotations as working modulo 3.

Note that as symmetries are functions, we can combine symmetries in the same way as we compose functions. In particular, when combining of symmetries we do so from right to left. We work through some examples:

$r_1 \circ s_1$:

This is equal to s_3 as shown in Figure 2.2.

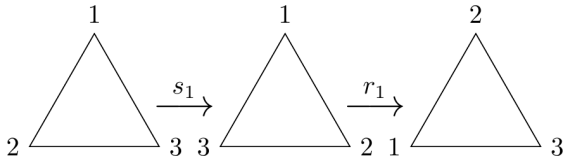


Figure 2.2: $r_1 \circ s_1$

$s_2 \circ s_3$:

This is equal to r_1 as shown in Figure 2.3.

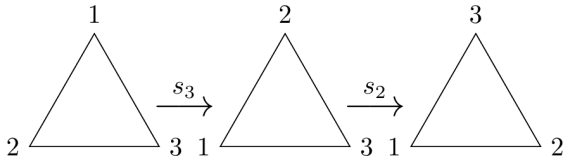


Figure 2.3: $s_2 \circ s_3$

$s_3 \circ s_2$:

This is equal to r_2 (see Figure 2.4). Therefore,

$$s_3 \circ s_2 \neq s_2 \circ s_3.$$

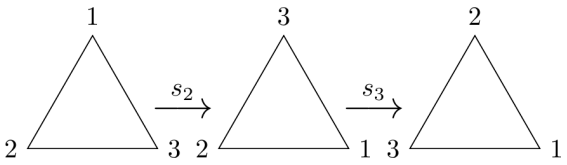


Figure 2.4: $s_3 \circ s_2$

> **Warning**
>
> The lines of symmetry are fixed and do not move with the triangle!

We can draw up the following multiplication table for combining symmetries:

	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_3	s_1	s_2
r_2	r_2	e	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r_1	r_2
s_2	s_2	s_3	s_1	r_2	e	r_1
s_3	s_3	s_1	s_2	r_1	r_2	e

> **Note**
>
> Note than entries in the table are read left to right. In particular, to find the value of $s_2 \circ s_3$ we look for the entry in row s_2 and column s_3 (which is r_1); likewise $s_3 \circ s_2$ is the entry in row s_3 and column s_2 (this is r_2).

Example 2.2. Develop suitable notation and construct an operation table for the symmetries of a square.

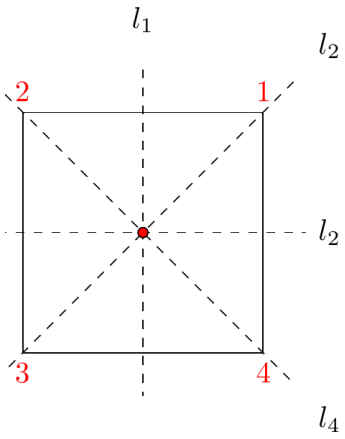


Figure 2.5: Square

The symmetries are:

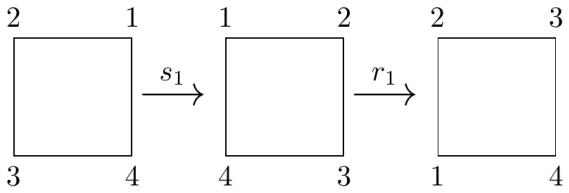
r_n – anticlockwise rotation by $2n\pi/4 = n\pi/2$ radians, $n \in \{0, 1, 2, 3\}$;

s_i – reflection in the line l_i, $i \in \{1, 2, 3, 4\}$.

> **Note**
>
> Observe that $r_0 = e$. As in the case of the triangle we can treat anticlockwise rotations as working modulo 4. Indeed rotating 4 times anticlockwise by $\pi/2$ is the same as r_0.

Some example compositions follow:

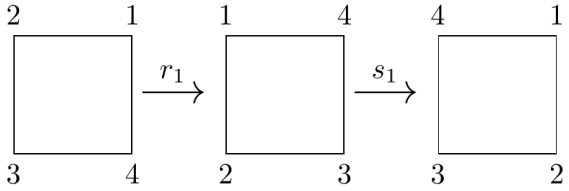
$r_1 \circ s_1$:



$$r_1 \circ s_1 = s_4.$$

Figure 2.6: $r_1 \circ s_1$

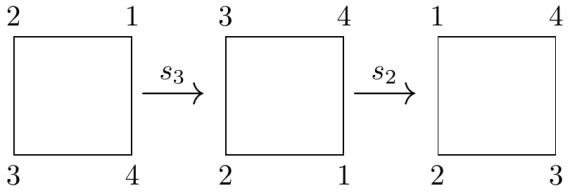
$s_1 \circ r_1$:



$$s_1 \circ r_1 = s_2 \neq r_1 \circ s_1.$$

Figure 2.7: $s_1 \circ r_1$

$s_2 \circ s_3$:



$$s_2 \circ s_3 = r_1.$$

Figure 2.8: $s_2 \circ s_3$

The operation table is:

$\circ$	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
e	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	e	s_4	s_1	s_2	s_3
r_2	r_2	r_3	e	r_1	s_3	s_4	s_1	s_2
r_3	r_3	e	r_1	r_2	s_2	s_3	s_4	s_1
s_1	s_1	s_2	s_3	s_4	e	r_1	r_2	r_3
s_2	s_2	s_3	s_4	s_1	r_3	e	r_1	r_2
s_3	s_3	s_4	s_1	s_2	r_2	r_3	e	r_1
s_4	s_4	s_1	s_2	s_3	r_1	r_2	r_3	e

2.2 Congruences

Recall the definition from the first-year Algebra module. For integers a and b and some fixed positive integer m, we say that a is congruent to b modulo m if and only if m divides $a - b$. Symbolically we have $a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$.

Let us consider the set of numbers $\{0, 1, 2, \ldots, n-1\}$ and, in particular, what happens if we add together those numbers pairwise, but working modulo n. For any given value of n we are able to construct a table as follows.

Example 2.3. Let $n = 7$.

Write $\oplus_7$ for the operation of addition modulo 7. For example

$$\begin{aligned} 2 \oplus_7 3 &= 5 \\ 6 \oplus_7 4 &= 3. \end{aligned}$$

The operation table is as follows:

$\oplus_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

2.3 Matrices

Consider the following four 2×2 matrices with real entries:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

We can multiply together these matrices pairwise (with the usual matrix multiplication) and construct the following table:

$\times$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$
$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

2.4 Roots of Unity

In the first-year Algebra module we investigated, in the complex numbers section, the roots of unity. We found that the n^{th} roots of unity are the n distinct complex numbers of the form $e^{i\frac{2k\pi}{n}}$ where $k = 0, 1, 2, \ldots, n-1$. Consider the fifth roots of unity, that is the complex numbers of the form $e^{i\frac{2k\pi}{5}}$, where $k = 0, 1, 2, \ldots, 4$ and let us see what happens when we multiply these together pairwise and form a table of the results.

$\times$	1	$\mathrm{e}^{\frac{2\pi i}{5}}$	$\mathrm{e}^{\frac{4\pi i}{5}}$	$\mathrm{e}^{\frac{6\pi i}{5}}$	$\mathrm{e}^{\frac{8\pi i}{5}}$
1	1	$\mathrm{e}^{\frac{2\pi i}{5}}$	$\mathrm{e}^{\frac{4\pi i}{5}}$	$\mathrm{e}^{\frac{6\pi i}{5}}$	$\mathrm{e}^{\frac{8\pi i}{5}}$
$\mathrm{e}^{\frac{2\pi i}{5}}$	$\mathrm{e}^{\frac{2\pi i}{5}}$	$\mathrm{e}^{\frac{4\pi i}{5}}$	$\mathrm{e}^{\frac{6\pi i}{5}}$	$\mathrm{e}^{\frac{8\pi i}{5}}$	1
$\mathrm{e}^{\frac{4\pi i}{5}}$	$\mathrm{e}^{\frac{4\pi i}{5}}$	$\mathrm{e}^{\frac{6\pi i}{5}}$	$\mathrm{e}^{\frac{8\pi i}{5}}$	1	$\mathrm{e}^{\frac{2\pi i}{5}}$
$\mathrm{e}^{\frac{6\pi i}{5}}$	$\mathrm{e}^{\frac{6\pi i}{5}}$	$\mathrm{e}^{\frac{8\pi i}{5}}$	1	$\mathrm{e}^{\frac{2\pi i}{5}}$	$\mathrm{e}^{\frac{4\pi i}{5}}$
$\mathrm{e}^{\frac{8\pi i}{5}}$	$\mathrm{e}^{\frac{8\pi i}{5}}$	1	$\mathrm{e}^{\frac{2\pi i}{5}}$	$\mathrm{e}^{\frac{4\pi i}{5}}$	$\mathrm{e}^{\frac{6\pi i}{5}}$

Note that if $k = 5$, then $\mathrm{e}^{\frac{2k\pi i}{5}} = \mathrm{e}^{2\pi i} = 1$.

The whole point of abstraction in Mathematics is to look at the properties of mathematical objects independently from their composition. We are interested in the general rules that govern the behaviour of particular types of object and, importantly, the generalised structure of such objects. With that in mind we now investigate the previous examples to see if there are any general properties that they *all* share.

(a) In each case we started with a non-empty *set* of elements as follows:

Symmetries of an equilateral triangle:

$$\{e, r_1, r_2, s_1, s_2, s_3\}.$$

Addition modulo 7:

$$\{0, 1, 2, 3, 4, 5, 6\}.$$

Matrices:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Fifth roots of unity:

$$\left\{1, \mathrm{e}^{\frac{2\pi i}{5}}, \mathrm{e}^{\frac{4\pi i}{5}}, \mathrm{e}^{\frac{6\pi i}{5}}, \mathrm{e}^{\frac{8\pi i}{5}}\right\}.$$

(b) In each case we had an *operation* that we used to combine elements from the set and,

more importantly gave a unique answer in each case:

Symmetries of an Equilateral triangle: Composition of functions, for example

$$r_1 \circ s_1 = s_3.$$

Congruences: For a positive integer m, addition modulo m ($\oplus_m$). For example for $m = 7$,

$$5 \oplus_7 6 = 4.$$

Matrices: Matrix multiplication. For example,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Roots of unity: Multiplication, for example

$$\mathrm{e}^{\frac{2\pi i}{5}} \mathrm{e}^{\frac{4\pi i}{5}} = \mathrm{e}^{\frac{6\pi i}{5}}.$$

Such operations are called *binary operations* and are defined as follows:

Definition 2.2 (Binary Operation)**.** A *binary operation* on a set, S, is an operation, $*$, such that $x * y$ is uniquely defined $\forall x, y \in S$.

So, in each case we have a set of objects and a binary operation that combines elements from the set. We now turn our attention to the structure of the tables that we have constructed.

(c) The entries in the body of the table only comprise elements of the set we are working with; the binary operation, when applied to elements of the set, never produced something not in the set. In such circumstances we say the the set is *closed* under the binary operation. Formally we have that a set S is closed under $*$ if and only if $\forall\, x, y \in S,\ x * y \in S$.

Example 2.4.

- **Symmetries of the square**: we can see from the table that composing any pair of symmetries gives another symmetry. For example $r_1 \circ s_4 = s_3$.
- **Congruence**: For a positive integer m, adding two numbers modulo m results in a number in the set $\{0, 1, 2, \ldots, m-1\}$. For example, for $m = 7$, $3 \oplus_7 6 = 2$.

(d) We can see that in each table there is one row and one column, associated with just one of the group elements, that repeats the index row and column. This tells us that each of the sets contains an *identity element*, that is an element that when combined under the binary operation with another element leaves that other element unchanged.

We often use the symbol e to represent a generic identity element and we say that the set has an identity with respect to a particular binary operation. Formally we have that $e \in S$ is an *identity element* of S with respect to $*$ if and only if $\forall\, x \in S$, $e * x = x$ and $x * e = x$. It is important to note that the identity elements in the above examples are all 'two-sided'.

Example 2.5.

Symmetries of the triangle: Here e is the identity element. We can check that, $e \circ x = x \circ e = e$ for *any* symmetry e of the triangle. For example

$$e \circ s_2 = s_2 \circ e = s_2.$$

Congruences: Here, 0 is the identity element. For example, working mod 7, we can check that, $0 \oplus_7 x = x \oplus_7 0 = x$ for *any* $x \in \{0, 1, 2, 3, 4, 5, 6, 7\}$. For example

$$0 \oplus_7 5 = 5 \oplus_7 0 = 5.$$

Matrices: The identity matrix is the identity:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

An important property of identity elements is given in the following lemma.

Lemma 2.1. *If S is a set closed under a binary operation, $*$, then S contains at most one identity.*

Proof.

Let e and f be identity elements of S. Then $e = e * f = f$ and so $e = f$.

□

(e) We note that in each table *the* identity element appears precisely once in each row and each column. This tells us that each element of the set has a corresponding element such that when the two are combined the result is the identity. We refer to the second element as an *inverse* of the first.

Example 2.6.

Symmetries of the square:

$$r_1 \circ r_3 = r_3 \circ r_1 = e.$$

Therefore r_1 is the inverse of r_3 and r_3 is the inverse of r_1.

Notice also that any reflection s is its own inverse. Since

$$s \circ s = e$$

for any reflection s of the square.

Addition Modulo 7:

$$2 \oplus_7 5 = 5 \oplus_7 2 = 0.$$

Therefore 5 is the inverse of 2 and 2 is the inverse of 5.

Matrices:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is its own inverse.

An important property of inverses of elements is given in the following lemma.

Lemma 2.2. *Let S be a set closed under an associative binary operation, $*$, with identity, e. Then $x \in S$ has, at most, one inverse.*

Proof.

Suppose u and v are both inverses of x. Then

$$\begin{aligned} u * x * v &= u * (x * v) = u * e = u \text{ and,} \\ u * x * v &= (u * x) * v = e * v = v. \end{aligned}$$

Therefore $u = v$.

Can you tell?

Can you tell at which points in the proof above we made use of the associative property of $*$?

□

We denote the inverse of an element x as x^{-1}. In the same way that the identity is 'two-sided' we can see from the tables that the combining of each element with its inverse is two-sided

and this leads to the following formal definition. Let S be a set, closed under a binary operation, $*$, with identity e. The *inverse* of $x \in S$ is any element $x^{-1} \in S$ such that $x * x^{-1} = x^{-1} * x = e$.

(f) One final property that all of our examples share, but which is not obvious from the tables, is that in each case the binary operation is *associative*. Formally we have that $*$ is *associative* on S if and only if $\forall\, x, y, z \in S$, $(x * y) * z = x * (y * z)$. Note that it is the binary operation that is associative, not the set of objects.

Example 2.7.

In the symmetries of the triangle: One can check that for any three symmetries, x, y, z,

$$(x \circ y) \circ z = x \circ (y \circ z)$$

.

For example,

$$\begin{aligned} (r_1 \circ s_1) \circ s_2 &= s_3 \circ s_2 = r_2 \\ r_1 \circ (s_1 \circ s_2) &= r_1 \circ r_1 = r_2. \end{aligned}$$

In addition modulo m: we know that this is an associative operation.

A set of elements, together with a binary operation that satisfies each of the conditions that we have explored above, forms an algebraic structure called a *group*. We shall start to deal with groups in a formal manner in the next chapter, but in the meantime we state and prove an important Lemma and explore further the properties of binary operations.

Lemma 2.3. *Let S be a set closed under an associative binary operation, $*$, with identity, e. If x^{-1} and y^{-1} exist, then $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Proof.

Since inverses are unique, it is enough to show that $(x * y) * (y^{-1} * x^{-1}) = e$ and $(y^{-1} * x^{-1}) * (x * y) = e$.

We have:

$$\begin{aligned}(x * y) * (y^{-1}) * x^{-1}) &= x * ((y * y^{-1}) * x^{-1})) \\ &= x * (e * x^{-1}) \\ &= x * x^{-1} \\ &= \mathrm{e}.\end{aligned}$$

In a similar way, one can show that $(y^{-1} * x^{-1}) * (x * y) = e$.

□

Properties of Binary Operations

- The above lemma extends easily to inverses of repeated 'products', e.g.

$$(a * b * c * d)^{-1} = d^{-1} * c^{-1} * b^{-1} * a^{-1}.$$

- Let S be a set closed under an associative binary operation, $*$. Then all ways of bracketing an expression, $x_1 * x_2 * \ldots x_n$, give the same answer.
- Let S be a set closed under an associative binary operation, $*$. Then $x^n = \underbrace{x * x * \ldots * x}_{n \text{ terms}}$, where n is a positive integer. It follows, from the generalised associative law, that for positive integer powers of a single element, the usual index laws are valid:

$$\begin{aligned}x^a * x^b &= x^{a+b} \\ (x^a)^b &= x^{ab}.\end{aligned}$$

- If S is a set closed under an associative binary operation, $*$, with an identity element, e, then we define $x^0 = e$, $\forall x \in S$.

  Since zero is not positive it now follows that the index laws are valid for all natural number powers of a single element, where $0 \in \mathbb{N}$.

- If x has an inverse, then we define

$$x^{-n} = (x^n)^{-1} = (x^{-1})^n,$$

  where n is a positive integer. Note that $(x^n)^{-1} = (x^{-1})^n$ by repeated application of Lemma 2.3. This now ensures that the index laws are valid for all integer powers of an element which has an inverse.

Example 2.8. A binary operation $*$ is defined on $\mathbb{R}$ by $x * y = x + y - xy$.

i. Show that $\mathbb{R}$ closed under $*$.

ii. Prove that $*$ associative on $\mathbb{R}$.

iii. Find the identity element w.r.t. $*$ and show that it satisfies the required conditions to be an identity.

iv. Does every element of $\mathbb{R}$ have an inverse under $*$?

i. For $x, y \in \mathbb{R}$, $x * y \in \mathbb{R}$ since addition and multiplication of real numbers are closed binary operations on $\mathbb{R}$ In, particular as $x + y$ and xy are real numbers, $(x + y) - xy$ is also a real number.

ii. Let $x, y, z \in \mathbb{R}$, then

$$\begin{aligned}(x * y) * z &= (x + y - xy) * z \\ &= (x + y - xy) + z - (x + y - xy)z \\ &= x + (y + z) - xy - x(z - yz) - yz \\ &= (x + (y + z) - yz) - x((y + z) - yz) \\ &= (x + (y * z)) - x(y * z) \\ &= x * (y * z).\end{aligned}$$

iii. Let $e \in \mathbb{R}$ be the identity element under $*$, then

$$x = e * x = e + x - ex \tag{2.1}$$

Solving this equation, we find that: $e(1-x) = 0$. Thus, as this must hold for all $x \in \mathbb{R}$, in particular, for $x \neq 1$, we find that $e = 0$. We now check that $0 * x = x = x * 0$ for all $x \in \mathbb{R}$.

$$\begin{aligned}0 * x &= 0 + x - 0x = x \\ x * 0 &= x + 0 - x0 = x.\end{aligned}$$

Therefore 0 is the identity element with respect to $*$.

iv. Let $x \in \mathbb{R}$ and suppose $y \in \mathbb{R}$ is the inverse of x. Then

$$0 = x * y = x + y - xy.$$

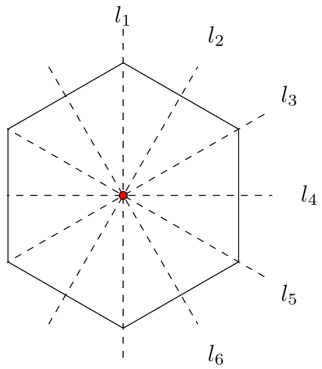
It follows that $y(1 - x) = -x$. Thus y must be $\frac{x}{x-1}$. This is only defined for $x \neq 1$. Hence every element of $\mathbb{R}$ other than 1 has an inverse under $*$. Notice that $1 * x = x * 1 = 1$ for all $x \in \mathbb{R}$.

2.5 Problem Sheet 2

For Week 4; covers Chapter 2 material.

Question 2.1

Develop suitable notation and construct an operation table for the symmetries of a regular hexagon, as shown below. For consistency with examples in the lecture notes, let the vertical line of symmetry be denoted l_1 and number the others in a clockwise direction.



Show Solution 2.1 on P188

Question 2.2

Lemma 2.3 states that if S is a set closed under an associative binary operation, $*$, with identity, e, and if x^{-1} and y^{-1} exist, then $(x * y)^{-1} = y^{-1} * x^{-1}$. Use mathematical induction to prove that this lemma extends to any finite product, that is

$$(x_1 * x_2 * \ldots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \ldots * x_2^{-1} * x_1^{-1}$$

for all natural numbers, n.

Show Solution 2.2 on P189

Question 2.3

A binary operation $*$ is defined on $\mathbb{R}$ by $x * y = xy - 2x - 2y + 6$.

i. Is $\mathbb{R}$ closed under $*$?

ii. Is $*$ associative on $\mathbb{R}$?

iii. Does $\mathbb{R}$ have an identity element w.r.t. $*$?

iv. Does every element of $\mathbb{R}$ have an inverse under $*$?

Show Solution 2.3 on P190

Question 2.4

A binary operation $*$ is defined on $\mathbb{R}\backslash\{2\}$ by $x * y = xy - 2x - 2y + 6$.

i. Is $\mathbb{R}\backslash\{2\}$ closed under $*$?

ii. Is $*$ associative on $\mathbb{R}\backslash\{2\}$?

iii. Does $\mathbb{R}\backslash\{2\}$ have an identity element w.r.t. $*$?

iv. Does every element of $\mathbb{R}\backslash\{2\}$ have an inverse under $*$?

Show Solution 2.4 on P192

Chapter 3

Group Theory

The algebraic structure that we now call a group had its roots in the nineteenth century and was developed from three distinct branches of Mathematics. Groups arise most naturally when we are considering symmetry and when we think of symmetry we immediately think of geometry. In 1872, Felix Klein (he of the bottle) announced his Erlangen Programme for classifying geometries in the wake of the development of novel non-Euclidean geometries such as hyperbolic, spherical, projective etc. He used groups of symmetries to assist in this classification. In addition, mathematicians were interested in transformations that left shapes effectively unchanged (*isometries*) and it became apparent that the transformations themselves had certain properties independent of the objects they acted on. The modern concept of a group arose also out of work on polynomial equations and, in particular, Lagrange's study of the permutations of the roots of such equations as a tool for solving them. Finally, in number theory, work by Gauss on quadratic forms, and Euler on the remainders on division of powers by primes, led also into the development of the concept of a group.

3.1 The Group Concept

Definition 3.1 (Group)**.** A group is a pair $(S, *)$, where S is a *non-empty* set and $*$ is a binary operation defined on S such that:

i. S is *closed* under $*$, that is $\forall\, x, y \in S,\ x * y \in S$.

ii. $*$ is *associative* on S,that is $\forall\, x, y, z \in S,\ (x * y) * z = x * (y * z)$.

iii. S has an *identity* with respect to $*$, denoted e, that is $\exists\, e \in S$ such that $\forall\, x \in S$ $e * x = x * e = x$.

iv. every $x \in S$ has an *inverse*, denoted $x^{-1} \in S$, that is $\forall\, x \in S, \exists x^{-1} \in S$ such that $x * x^{-1} = x^{-1} * x = e$.

One important property possessed by some, but not all, of our examples is commutativity. We say that a binary operation $*$ on a set S is *commutative* if and only if $\forall\, x, y \in S,\ x * y = y * x$.

Where it is the case that every element in a group commutes with every other element we say that the group is *abelian*

Definition 3.2 (Abelian)**.** A group $(G, *)$ is called *abelian* (or *commutative*) if and only if $\forall\, x, y \in G,\ x * y = y * x$.

It is important to note that the commutative property is *not required* for 'groupness'.

Example 3.1 (Positive and Negative Examples)**.**

(a) $(\mathbb{N}, +)$

- Closed as the sum of two natural numbers is a natural number.
- addition of natural numbers is associative.
- $0 \in \mathbb{N}$ is the identity element since $a + 0 = 0 + a = a$ for all $a \in \mathbb{N}$.
- Not all natural numbers have an inverse. For instance there is no natural number $a \in \mathbb{N}$ such that $a + 2 = 0$.

The natural numbers under addition, $(\mathbb{N}, +)$ is *not* a group.

(b) $(\mathbb{N}, -)$

- Subtraction is not a closed binary operation on $\mathbb{N}$. For example $0 - 2 = -2 \notin \mathbb{N}$.

- Subtraction is not an associative operation on $\mathbb{N}$. For example:

$$-4 = (1-2)-3 \neq 1-(2-3) = 2.$$

- There is no identity element. Since if $x \in \mathbb{N}$ was the identity element. Then, $a - x = a$ for all $a \in \mathbb{N}$, which means that $x = 0$. However, $0 - a = -a \neq a$ when $a \neq 0$.
- Without an identity element one cannot talk about inverses.

Therefore $(\mathbb{N}, -)$ is *not* a group.

(c) $(\mathbb{Z}, +)$

- Addition is a closed binary operation on $\mathbb{Z}$ — the sum of two integers is again an integer.
- Addition is an associative binary operation on $\mathbb{Z}$.
- The identity element is 0 since $0 \in \mathbb{Z}$ and $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}$.
- For $a \in \mathbb{Z}$, $a^{-1} = -a$ since $-a \in \mathbb{Z}$ and $-a + a = a + (-a) = 0$.

Therefore, $(\mathbb{Z}, +)$ *is* a group.

(d) $(\mathbb{Q}, \times)$

- Multiplication is a closed binary operation on $\mathbb{Q}$, since the product of two rational numbers is again a rational number. We can see this as follows: let $a, b \in \mathbb{Q}$. There there are $u, v \in \mathbb{Z}$ and $s, t \in \mathbb{N}\backslash\{0\}$ such that $a = u/s$ and $b = v/t$. Thus $a \times b = (u \times v)/(s \times t) \in \mathbb{Q}$.
- Multiplication is an associative binary operation on $\mathbb{Q}$.
- The identity element is 1 since $1 \in \mathbb{Q}$ and for any $a \in \mathbb{Q}$, $1 \times a = a \times 1 = 1$.
- Zero does not have an inverse in $\mathbb{Q}$ since there is no element $a \in \mathbb{Q}$ such that $a \times 0 = 0 \times a = 1$.

Therefore $(\mathbb{Q}, \times)$ *not* a group.

(e) $(\mathbb{Q}\backslash\{0\}, \times)$

This is a group by part d..

(f) $(\mathbb{R}_{3\times 3}, +)$

- Addition is a closed binary operation on $\mathbb{R}_{3\times 3}$. Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

and

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}$$

be elements of $\mathbb{R}_{3\times 3}$. Then

$$A + B = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & a_{13}+b_{13} \\ a_{21}+b_{21} & a_{22}+b_{22} & a_{23}+b_{23} \\ a_{31}+b_{31} & a_{32}+b_{32} & a_{33}+b_{33} \end{pmatrix} \in \mathbb{R}_{3\times 3}.$$

- Addition is an associative binary operation on $\mathbb{R}_{3\times 3}$.
- The zero matrix

$$\mathbf{0}_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

is the identity element. $\mathbf{0}_3 + A = A = A + \mathbf{0}_3$ for all $A \in R_{3\times 3}$ and $\mathbf{0}_3 \in \mathbb{R}_{3\times 3}$.

- Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \mathbb{R}_{3\times 3}.$$

Then

$$-A = \begin{pmatrix} -a_{11} & -a_{12} & -a_{13} \\ -a_{21} & -a_{22} & -a_{23} \\ -a_{31} & -a_{32} & -a_{33} \end{pmatrix} \in R_{3\times 3}$$

is the inverse of A. Since $A + (-A) = (-A) + A = \mathbf{0}_3$.

$(\mathbb{R}_{3\times 3}, +)$ *is* a group.

(g) $(\mathbb{R}_{3\times 3}, \times)$

- Multiplication of two 3×3 matrices with real entries is again a real 3×3 matrix with real entries.
- Matrix multiplication is an associative binary operation on $\mathbb{R}_{3\times 3}$.
- The identity element is the identity matrix

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

  Since $I_3 \in \mathbb{R}_{3\times 3}$ and for any $A \in \mathbb{R}_{3\times 3}$. $I_3 \times A = A \times I_3 = A$.
- The zero matrix $\mathbf{0}_3 \in \mathbb{R}_{3\times 3}$ does not have an inverse, since $\mathbf{0}_3 \times A = A \times \mathbf{0}_3 = \mathbf{0}_3$ for all $A \in \mathbb{R}_{3\times 3}$.

$(\mathbb{R}_{3\times 3}, \times)$ is *not* a group.

(h) $(\{1, -1\}, \times)$

- Multiplication is a closed binary operation on $\{1, -1\}$ since: $1 \times 1 = -1 \times -1 = 1$, $1 \times -1 = -1 \times 1 = -1$.
- Multiplication of integers is associative and so multiplication is an associative binary operation on $\{1, -1\}$.
- The identity element if 1.

- 1 is its own inverse and, likewise, -1 is its own inverse:

$$1 = 1 \times 1 = -1 \times -1.$$

$(\{1, -1\}, \times)$ *is* a group.

(i) $(\{1, -1, i, -i\}, \times)$

- Multiplication is a closed binary operation on $\{1, -1, i, -i\}$.
- Multiplication of complex numbers is associative and so multiplication is associative on $\{1, -1, i, -i\}$.
- 1 is the identity element.
- 1 and -1 are their own inverses; i and $-i$ are mutually inverses of each other: $1 = i \times (-i) = (-i) \times i$.

$(\{1, -1, i, -i\}, \times)$ *is* a group.

Example 3.2. Consider Example 2.8. Is $(\mathbb{R}, *)$ a group? Is $(\mathbb{R}\backslash\{1\}, *)$ a group?

Solution:

We showed in Example 2.8, that 1 does not have an inverse in $(\mathbb{R}, *)$. It follows that $(\mathbb{R}, *)$ is not a group.

What about $(\mathbb{R}\backslash\{1\}, *)$? We know that $*$ is an associative, binary operation on $(\mathbb{R}, *)$ and so it remains an associative binary operation on $(\mathbb{R}\backslash\{1\}, *)$; 0 remains the identity element of; every element $x \in \mathbb{R}\backslash\{1\}$ has an inverse $\frac{x}{x-1} \in \mathbb{R}\backslash\{1\}$ (notice that $\frac{x}{x-1} \neq 1$ for any $x \in \mathbb{R}\backslash\{1\}$.). Therefore the only way $(\mathbb{R}\backslash\{1\}, *)$ can fail to be a group is if $*$ is not a *closed* binary operation on $\mathbb{R}\backslash\{1\}$. Thus we check if $*$ is a closed binary operation on $\mathbb{R}\backslash\{1\}$.

Let $x, y \in \mathbb{R}\backslash\{1\}$ and suppose that $x * y \notin \mathbb{R}\backslash\{1\}$. This can only occur if $x * y = 1$ (since $x * y$ is necessarily a real number). It then follows that

$$x * y = x + y - xy = 1. \tag{3.1}$$

Therefore

$$x(1-y)+y=1$$

and so

$$x=\frac{1-y}{1-y}.$$

Since $y \neq 1$, then $1-y \neq 0$ and so $x=1$ which is a contradiction since $x \in \mathbb{R}\backslash\{1\}$.

It must therefore be the case that $x * y \in \mathbb{R}\backslash\{1\}$ for all $x, y \in \mathbb{R}\backslash\{1\}$.

We conclude that $(\mathbb{R}\backslash\{1\}, *)$ is a group.

3.2 Elementary Group Theory

We now derive some results about groups in general, building up this theory using only the axioms and results progressively proven (this is the manner in which all axiomatic systems are built).

3.2.1 Preliminary Definitions and Results

Lemma 3.1 (Cancellation Laws)**.** *If $(G, \times)$ is a group, then $\forall\, a, x, y \in G$:*

$$ax = ay \;\Rightarrow\; x = y;$$

$$xa = ya \;\Rightarrow\; x = y.$$

Proof.

Suppose $ax = ay$. Then $a^{-1}(ax) = a^{-1}(ay)$. Rebracketing:

$$(a^{-1}a)x = (a^{-1}a)y;$$

using the fact that $a^{-1}a = e$ we have

$$x = ex = ey = y.$$

The second law is demonstrated similarly.

Can you tell?

Can you tell which of the group axioms we used above and the points in which used them?

□

If G is finite, then these cancellation laws imply that in the operation table for $(G, \times)$ each element occurs exactly once in each row and exactly once in each column.

Lemma 3.2 (Division Laws). *If $(G, \times)$ is a group, then $\forall\ a, x, b \in G$:*

$$ax = b \ \Rightarrow\ x = a^{-1}b;$$

$$xa = b \ \Rightarrow\ x = ba^{-1}.$$

Proof.

Suppose $ax = b$. Then, $ax = eb = b$. writing $e = aa^{-1}$ we have $ax = aa^{-1}b$. Lemma 3.1 now implies that $x = a^{-1}b$.

The other statement is demonstrated similarly.

□

Corollary 3.1. *Let $(G, \times)$ be a group.*

i. If $ax = e$, then $x = a^{-1}$.

ii. If $xa = e$, then $x = a^{-1}$.

Note

In a group to check whether $x = a^{-1}$, we need only compute one of ax or ax. Also point ii. implies that $(x^{-1})^{-1} = x$ for all $x \in G$.

Proof.

i. If $ax = e$, then by Lemma 3.2, $x = a^{-1}e = a^{-1}$.

ii. If $xa = e$, then by Lemma 3.2, $x = ea^{-1} = a^{-1}$.

□

Definition 3.3 (Order)**.** The *order* of a set, S, denoted $|S|$, is the number of elements in S.

If S is an infinite set then we shall write $|S| = \infty$.

We are interested in the orders of groups, by which we mean the order of the set on which the binary operation has been defined.

- The order of the symmetry group of an equilateral triangle is 6.
- The order of $GL(n, \mathbb{R})$, under matrix multiplication, is infinite.

Definition 3.4 (Period)**.** Let $(G, \times)$ be a group with identity element e, and consider $a \in G$. If, for all positive integers (that is elements of the set $\{1, 2, 3, \ldots\}$) n, $a^n \neq e$, then a has *infinite period*. Otherwise, the *period* of a is the smallest positive integer k such that $a^k = e$.

Example 3.3.

(a) In $(\mathbb{C}\backslash\{0\}, \times)$,

(i) -1 has period

2, since $(-1)^2 = 1$.

(ii) i has period

4, since $i^2 = -1, i^3 = -i$ and $i^4 = 1$.

(iii) 2 has period

has infinite period since there is no positive integer k such that $2^k = 1$.

(b) In $(\mathbb{R}, +)$, 1 has

infinite period, $1^k = k$ for any positive integer k.

(c) In any group G, the identity e has period 1 and is the only element with this period.

(d) In the symmetry group of an equilateral triangle,

$\circ$	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_3	s_1	s_2
r_2	r_2	e	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r_1	r_2
s_2	s_2	s_3	s_1	r_2	e	r_1
s_3	s_3	s_1	s_2	r_1	r_2	e

(i) r_1 has period

3 since $r_1^2 = r_2$; $r_1^3 = r_2 \circ r_1 = e$.

(ii) s_2 has period

2, since $s_2^2 = e$.

3.2.2 Subgroups

We start, by way of illustration, with an example. Let $(G, \circ)$ be the group of symmetries of an equilateral triangle and $H = \{e, r_1, r_2\}$. Then $H \subset G$ and $(H, \circ)$ is a group.

$\circ$	e	r_1	r_2
e	e	r_1	r_2
r_1	r_1	r_2	e
r_2	r_2	e	r_1

Note that $(H, \circ)$ is abelian although $(G, \circ)$ is not abelian.

Definition 3.5 (Subgroup)**.** Let $(G, \times)$ be a group, $H \subseteq G$ (i.e. H is a subset of the elements of G). H is a *subgroup* of G if and only if $(H, \times)$ is a group.

Example 3.4 (Positive and Negative Examples)**.**

a. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

Clearly $\mathbb{Z} \subsetneq \mathbb{R}$. Is $(\mathbb{Z}, +)$ a group? Yes.

- For all $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$;
- addition is an associative binary operation on $\mathbb{Z}$;
- $e = 0$ and $0 \in \mathbb{Z}$ (for all $n \in \mathbb{Z}$, $0 + n = n + 0 = n$));
- For all $n \in \mathbb{Z}$, $n^{-1} = -n \in \mathbb{Z}$ since $(-n) + n = n + (-n) = 0$.

b. $(\mathbb{Z}\backslash\{0\}, \times)$ is not a subgroup of $(\mathbb{R}\backslash\{0\}, \times)$.

This is because, for example, $2^{-1} = \frac{1}{2} \notin \mathbb{Z}\backslash\{0\}$.

c. $(\mathbb{R}\backslash\{0\}, \times)$ is not a subgroup of $(\mathbb{R}, +)$.

The binary operations are different.

d. $(\{e, r_1\}, \circ)$ is not a subgroup of the group of symmetries of an equilateral triangle.

The set $\{e, r_1\}$ is not closed under $\circ$: $r_1 \circ r_1 = r_2 \notin \{e, r_1\}$.

Example 3.5. Consider the group of symmetries of a square (the table is reproduced below). List the period and inverse of each element. Find all of the subgroups and comment on their

order.

$\circ$	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
e	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	e	s_4	s_1	s_2	s_3
r_2	r_2	r_3	e	r_1	s_3	s_4	s_1	s_2
r_3	r_3	e	r_1	r_2	s_2	s_3	s_4	s_1
s_1	s_1	s_2	s_3	s_4	e	r_1	r_2	r_3
s_2	s_2	s_3	s_4	s_1	r_3	e	r_1	r_2
s_3	s_3	s_4	s_1	s_2	r_2	r_3	e	r_1
s_4	s_4	s_1	s_2	s_3	r_1	r_2	r_3	e

Solution:

Element	Period	Inverse
e	1	e
r_1	4	r_3
r_2	2	r_2
r_3	4	r_1
s_1	2	s_1
s_2	2	s_2
s_3	2	s_3
s_4	2	s_4

The subgroups are as follows:

Subgroup	Order
$H_1 = \{e\}$	1
$H_2 = \{e, r_2\}$	2
$H_3 = \{e, r_1, r_2, r_3\}$	4
$H_4 = \{e, r_2, s_1, s_3\}$	4

Subgroup	Order
$H_5 = \{e, r_2, s_2, s_4\}$	4
$H_6 = \{e, s_1\}$	2
$H_7 = \{e, s_2\}$	2
$H_8 = \{e, s_3\}$	2
$H_9 = \{e, s_4\}$	2
$H_{10} = \{e, r_1, r_2, r_3, s_1, s_2, s_3, s_4\}$	8

Note that in each case the order of the subgroup divides the order of the group.

We reserve a special notation for the groups of symmetries of a regular n-gon, we write D_n for this group and it is called *the dihedral group of order* $2n$ (since the order of D_n is 2_n). However, the nomenclature dihedral group of order n is also used in some textbooks — here 'order n' refers to the number of sides of the regular n-gon.

> **Note**
>
> For any group G, $\{e\}$ and G are subgroups.
>
> - $(\{e\}, *)$ is the *trivial* subgroup of $(G, *)$;
> - $(G, *)$ is the *improper* subgroup of $(G, *)$;
> - A subgroup $(H, *)$ of $(G, *)$ which is not improper is called a *proper* subgroup of $(G, *)$. For example $(\{e\}, *)$ is a proper subgroup of $(G, *)$.

Lemma 3.3. *Let $(H, \times)$ be a subgroup of $(G, \times)$. Then:*

i. the identity in $(H, \times)$ is the identity in $(G, \times)$;

ii. the inverse of h in $(H, \times)$ is the inverse of h in $(G, \times)$.

Proof.

i. Let e_H be the identity element of $(H, \times)$. Then $e_H \times e_H = e_H$. Now since $H \subseteq G$, it

follows that $e_H \in G$ and so e_H has an inverse in G. We find

$$(e_H)^{-1} \times e_H \times e_H = (e_H)^{-1} \times e_H,$$

and so

$$e_H = e_G \times e_H = e_G = (e_H)^{-1} \times e_H.$$

Therefore $e_G = e_H$ as required.

ii. Let $h \in H$. Let g be the inverse of h in H. Then $g \times h = e_H = e_G$. It follows by Corollary 3.1 that $g = h^{-1}$ the inverse of h in G.

□

In order to determine whether a given subset of the elements of a group forms a subgroup, we could check all of the group axioms in Definition 2.3. The following lemma states that this is not necessary, in particular associativity is 'inherited'.

Lemma 3.4 (Subgroup Test)**.** *Let H be a non-empty subset of the elements of a group $(G, \times)$. Then $(H, \times)$ is a subgroup of $(G, \times)$ if and only if , $\forall\, h_1, h_2 \in H$*

i. $h_1 \times h_2 \in H$ (i.e. H is closed under $\times$),

ii. $h_1^{-1} \in H$ (i.e. H is closed under inverse).

Proof.

If H is a subgroup then i. and ii. follow from the fact that $(H, \times)$ is a group.

For the reverse implication, assume $(H, \times)$ satisfies i. and ii. We show that $(H, \times)$ satisfies the group axioms (Definition 3.1). The closure and inverse axioms are assumed to hold (they are points i. and ii. above). We only need show that $\times$ is an associative binary operation on H and H contains an identity.

Associativity: Let $h_1, h_2, h_3 \in H$, then $(h_1 \times h_2) \times h_3 = h_1 \times (h_2 \times h_3)$ since $\times$ is an associative binary operation on G and h_1, h_2, h_3 are also elements of G.

Identity: Let $h \in H$, then by assumption $h^{-1} \in H$. It follows that $e_G = h \times h^{-1} \in H$ since H is closed under products.

□

Example 3.6. $(\mathbb{Q}\backslash\{0\}, \times)$ is a subgroup of $(\mathbb{R}\backslash\{0\}, \times)$.

Solution:

We apply the subgroup test.

We first observe that $\mathbb{Q}\backslash\{0\}$ is a non-empty subset of $\mathbb{R}$.

i. We note that the product of two rational numbers is again a rational number.

ii. Let $a = p/q \in \mathbb{Q}\backslash\{0\}$. Then $p \neq 0 \neq q$ and so $b = q/p \in \mathbb{Q}\backslash\{0\}$. Moreover, $ab = ba = 1$ and so $(\mathbb{Q}\backslash\{0\}, \times)$ is closed under inverses.

Therefore, $(\mathbb{Q}\backslash\{0\}, \times)$ is a subgroup of $(\mathbb{R}\backslash\{0\}, \times)$.

Example 3.7. Show that the set $M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{R}_{2\times 2} \,|\, a, b \text{ not both zero} \right\}$, forms a subgroup of $\mathrm{GL}(2, \mathbb{R})$ under matrix multiplication.

Solution:

We again apply Lemma 3.4. We observe that M is non-empty since it contains the identity matrix $(a = 1, b = 0)$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

i. Let $a, b, c, d \in \mathbb{R}$ such that a and b are not both zero and c and d are not both zero. Let

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

and

$$C = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

and consider the product

$$AC = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}.$$

Now, $AC \in M$ precisely if $(ac - bd)$ and $(ad + bc)$ are not both zero. Suppose for a contradiction that $ac = bd$ and $ad = -bc$. We have:

$$a(ad + bc) = a^2d + bac = a^2d + b^2d = d(a^2 + b^2) = 0$$

and

$$b(ad + bc) = abd + b^2c = a^2c + b^2c = c(a^2 + b^2) = 0.$$

Since a and b are not both zero, then $a^2 + b^2$ is not equal to 0. This means that both d and c must be zero. Which is a contradiction. Therefore $ac - bd$ and $ab + bc$ are not both zero.

ii. Let

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M.$$

Observe that $\det(A) = a^2 + b^2 \neq 0$ since a and b are not both zero. Therefore, the matrix

$$A^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

is such that $AA^{-1} = I_2 = A^{-1}A$. Moreover, $A^{-1} \in M$ since a and b are not both zero.

It is even easier to check whether a finite subset of the elements of a group forms a subgroup.

Lemma 3.5 (Finite Subgroups)**.** *Let H be a non-empty, finite subset of the elements of a group $(G, \times)$. Then $(H, \times)$ is a subgroup of $(G, \times)$ if and only if H is closed under $\times$.*

Proof.

If $(H, \times)$ is a subgroup of $(G, \times)$, then H is closed under $\times$.

Now assume that H is closed under $\times$. We use Lemma 3.4 again. Part i. is assumed.

Let $h \in H$ and consider the set $\{h^i : i \in \mathbb{N}\}$. By assumption that H is closed under $\times$, we observe that $\{h^i : i \in \mathbb{N}\} \subseteq H$. However since H is finite, it must be the case that $\{h^i : i \in \mathbb{N}\}$ is finite as well. Therefore there is $i, j \in \mathbb{N}$, such that $j > i$ and $h^i = h^j$. Since $j > i$ then $h^j = h^i h^{j-i}$. Therefore $h^i = h^i h^{j-i}$. Applying the Cancellation Laws, we conclude that $e = h^{j-i}$. Therefore $hh^{j-i-1} = e$. It follows that $h^{-1} = h^{j-i-1}$. Since $h^{j-i-1} \in H$, it follows that H is closed under inverses.

□

Example 3.8. $(\{1, -1, i, -i\}, \times)$ is a subgroup of $(\mathbb{C}\backslash\{0\}, \times)$.

Solution: The set $\{1, -1, i, -i\}$ is a finite subset of $\mathbb{C}$ and so we use Lemma 3.5. The easiest thing to do here is to write out the multiplication table; so long as only elements from $\{1, -1, i, -i\}$ appear in the table, then $(\{1, -1, i, -i\}, \times)$ is closed under multiplication and is a subgroup of $(\mathbb{C}, \times)$.

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	$-i$	i	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

It follows that $(\{1, -1, i, -i\}, \times)$ is a subgroup of $(\mathbb{C}, \times)$.

Example 3.9. Consider the set $H = \{2^n \,|\, n \in \mathbb{N}\} = \{1, 2, 4, 8, 16, 32, \ldots\}$. Then $(H, \times)$ is not a subgroup of $(\mathbb{Q}\backslash\{0\}, \times)$ even though $H \subsetneq \mathbb{Q}\backslash\{0\}$ is non-empty and closed under $\times$.

Solution: That $(H, \times)$ is not a subgroup of $(\mathbb{Q}\backslash\{0\}, \times)$ can be seen by observing that it is not closed under inverses. For instance the inverse of 2 is $\frac{1}{2}$ and $\frac{1}{2} \notin H$; H is however closed

under products: for $n, m \in \mathbb{N}$,

$$2^n \times 2^m = 2^{m+n} \in H.$$

> **Caution**
>
> This example illustrates that Lemma 3.5 really only works for showing that a *finite* subset of a group is a subgroup, for *infinite* subsets of a group, Lemma 3.4 is the lemma to use. **If in doubt then use Lemma 3.4**.

Now consider the set $I = \{2^n : n \in \mathbb{Z}\}$ (notice that I extends H to include negative powers of 2), $(I, \times)$ is a subgroup of $(\mathbb{Q}\backslash\{0\}, \times)$. We have to use Lemma 3.4 to demonstrate this since I is an infinite set. i. Let $m, n \in \mathbb{Z}$, then $2^m, 2^n \in I$ and $2^m \times 2^n = 2^{m+n} \in I$. Therefore, I is closed under products. ii. Let $2^m \in I$, then $2^{-m} \in I$, since $-m \in \mathbb{Z}$. Moreover, $2^m 2^{-m} = 1$. Therefore, I is closed under inverses.

Thus the set of all integer powers of 2 forms a subgroup of $(\mathbb{Q}\backslash\{0\}, \times)$. One might wonder if set of integral powers of an arbitrary element of a group more generally forms a subgroup under the group multiplication. This is the next result.

Theorem 3.1 (Cyclic Subgroup)**.** *Let $(G, \times)$ be a group and $a \in G$. Then $(\{a^n \,|\, n \in \mathbb{Z}\}, \times)$ forms a subgroup of $(G, \times)$ called the* cyclic subgroup generated by a*, denoted $\langle a \rangle$.*

Proof.

Note that the set $H = \{a^n \,|\, n \in \mathbb{Z}\}$ can be finite or infinite and we have seen examples of both (see Example 3.3 (a) for instance). Therefore Lemma 3.4 is what we have to use here. We begin as always by observing that H is non-empty since it contains both $e = a^0$ and $a = a^1$.

i. Let $a^m, a^n \in H$, then $a^m \times a^n = a^{m+n} \in H$ since $m + n \in \mathbb{Z}$. Therefore $(H, \times)$ is closed under products.

ii. Let $a^m \in H$, then $a^{-m} \in H$ since $-m \in \mathbb{Z}$. Moreover, $a^m a^{-m} = a^0 = e$. Therefore $(H, \times)$ is closed under inverses.

We conclude that $(H, \times) = (\{a^n \mid n \in \mathbb{Z}\}, \times)$ is a subgroup of $(G, \times)$.

□

1. In the group of symmetries of an equilateral triangle:
   - What are the elements of $\langle r_1 \rangle$?

     $\langle r_1 \rangle = \{e, r_1, r_2\}$.
   - What are the elements of $\langle s_1 \rangle$?

     $\langle s_1 \rangle = \{e, s_1\}$.
2. In $(\mathbb{R}, +)$:
   - What are the elements of $\langle 1 \rangle$?.

     $\langle 1 \rangle = \mathbb{Z}$.
   - What are the elements of $\langle 2 \rangle$?

     $\langle 2 \rangle = 2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$.
3. In $(\mathbb{R}\backslash\{0\}, \times)$:
   - What are the elements of $\langle 1 \rangle$?

     $\langle 1 \rangle = \{1\}$.
   - What are the elements of $\langle 2 \rangle$?

     $\langle 2 \rangle = \{2^n : n \in \mathbb{Z}\}$.

Definition 3.6 (Cyclic Generator)**.** A group, G, is called *cyclic* if and only if there exists an element $a \in G$, called a *generator* of G, such that $G = \langle a \rangle$.

Example 3.10 (Positive and Negative Examples)**.**

- $(\mathbb{Z}, +)$ is cyclic. What are its generators?

  Its generators are 1 and -1: $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.

- $(\{1, -1, i, -i\}, \times)$ is cyclic. What are its generators are?

  Its generators are i and $-i$: $\langle i \rangle = \langle -i \rangle = \{1, -1, i, -i\}$.

- The symmetry group of an equilateral triangle is not cyclic, which may be verified by trying each of its elements in turn.

Example 3.11. Consider the set $\{0, 1, 2, 3\}$ under addition modulo 4. Draw up the operation table. Is this a group? Is it cyclic?

Solution: The multiplication table is as follows:

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	1	0
3	3	0	1	2

This is a group as addition modulo 4 is an associative operation and the other axioms can be verified from the table.

This group is cyclic and its generators are 1 and $-1 = 3$:

$$1^0 = 0; \quad 1^1 = 1; \quad 1^2 = 1 \oplus_4 1 = 2; \quad 1^3 = 1 \oplus_4 1 \oplus_4 1 = 3$$

and

$$3^0 = 0; \quad 3^1 = 3; \quad 3^2 = 3 \oplus_4 3 = 2; \quad 3^3 = 3 \oplus_4 3 \oplus_4 3 = 1$$

Now consider the pair $(\{0, 1, 2, \ldots, n-1\}, \oplus_n)$, where the operation is addition modulo n. We call this $\mathbb{Z}_n$. Is it a group? Is it cyclic?

In proving the next theorem we will use the following 'obvious' fact (shown in Algebra).

> *For a given non-zero integer n, any integer k can be written in the form $k = qn+r$, where q and r are integers and $0 \leq r < |n|$.*

Theorem 3.2. *Let $(G, \times)$ be a cyclic group with generator a. Then $|G|$ = period of a.*

Proof.

There are two cases to consider:

case (a): Here we assume that a has infinite period. In this case it is clear that the group G is also infinite. For $G = \{a^n : n \in \mathbb{Z}\}$ and if $a^n = a^m$, then $a^n \times a^{-m} = a^{n-m} = e$ and so $n = m = e$ (since a has infinite order).

case (b): Here we assume that a has finite order n. In order to show that $|G| = n$, we have to show that for any $k \in \mathbb{Z}$, there is an $r \in \mathbb{N}$ such that $0 \leq r \leq n-1$ and $a^k = a^r$. We then also need to show that for integers r and s satisfying $0 \leq r, s \leq n-1$, $a^r = a^s$ if and only if $r = s$.

For the first let $k \in \mathbb{Z}$ be arbitrary. Using the fact from Algebra, there are $q, r \in \mathbb{Z}$ with $0 \leq r \leq n-1$ such that $k = qn + r$. Therefore,

$$a^k = a^{qn+r} = a^{qn} \times a^r = (a^n)^q \times a^r = e^q \times a^r = a^r$$

as required.

For the second, let $r, s \in \mathbb{Z}$ such that $0 \leq r \leq s \leq n-1$. Suppose $a^r = a^s$. Then $a^s \times a^{-r} = a^{s-r}e$. If $s \neq r$, then $(s-r) < n$. In this case, we conclude that the period of a must be less than $s-r$ and so must be strictly less than n. This is a contradiction since the period of a is n by assumption. Therefore $s = r$.

□

Example 3.12.

- Consider i in the group $(\mathbb{C}\backslash\{0\}, \times)$.

  The element i has period 4 in $(\mathbb{C}\backslash\{0\}, \times)$ and $\langle i \rangle = \{1, i, -1, -i\}$ has order 4.

- Consider r_1 in the symmetry group of an equilateral triangle, D_3.

  The element r_1 has period 4 in $(D_3, \circ)$ and $\langle r_1 \rangle = \{e, r_1, r_2\}$ has order 3.

3.3 Problem Sheet 3

For Week 4; covers Chapter 3.

Question 3.1

Decide whether or not the following are groups:

i. the set $S = \{1, 2, 3, 4, 5\}$ with operation $*$ defined by the following operation table

$*$	1	2	3	4	5
1	2	1	5	3	4
2	1	2	3	4	5
3	4	3	2	5	1
4	5	4	1	2	3
5	3	5	4	1	2

ii. the power set of a non-empty set A, with respect to set intersection;

iii. the set $S = \{a, b, c, d, e, f\}$ consisting of the six functions defined by

$$a(x) = x, \qquad b(x) = 1 - x, \; c(x) = \frac{1}{x},$$
$$d(x) = \tfrac{x-1}{x}, \quad e(x) = \frac{x}{x-1}, \; f(x) = \frac{1}{1-x},$$

together with the binary operation of function composition. Draw up an operation table.

Show Solution 3.1 on P193

Question 3.2

Let G be the symmetry group of a regular hexagon. Using the Cayley table below

$\circ$	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
e	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
r_1	r_1	r_2	r_3	r_4	r_5	e	s_6	s_1	s_2	s_3	s_4	s_5
r_2	r_2	r_3	r_4	r_5	e	r_1	s_5	s_6	s_1	s_2	s_3	s_4
r_3	r_3	r_4	r_5	e	r_1	r_2	s_4	s_5	s_6	s_1	s_2	s_3
r_4	r_4	r_5	e	r_1	r_2	r_3	s_3	s_4	s_5	s_6	s_1	s_2
r_5	r_5	e	r_1	r_2	r_3	r_4	s_2	s_3	s_4	s_5	s_6	s_1
s_1	s_1	s_2	s_3	s_4	s_5	s_6	e	r_1	r_2	r_3	r_4	r_5
s_2	s_2	s_3	s_4	s_5	s_6	s_1	r_5	e	r_1	r_2	r_3	r_4
s_3	s_3	s_4	s_5	s_6	s_1	s_2	r_4	r_5	e	r_1	r_2	r_3
s_4	s_4	s_5	s_6	s_1	s_2	s_3	r_3	r_4	r_5	e	r_1	r_2
s_5	s_5	s_6	s_1	s_2	s_3	s_4	r_2	r_3	r_4	r_5	e	r_1
s_6	s_6	s_1	s_2	s_3	s_4	s_5	r_1	r_2	r_3	r_4	r_5	e

i. find

   (a) a subgroup of order 2,

   (b) a subgroup of order 3,

   (c) a subgroup of order 4, and

   (d) a subgroup of order 6.

ii. Does G contain any subgroups which are not of order 2, 3, 4 or 6?

Show Solution 3.2 on P197

Question 3.3

For the sets $\{0, 1, 2, 3, 4\}$ and $\{0, 1, 2, 3, 4, 5\}$ construct operation tables under multiplication modulo 5 and multiplication modulo 6, respectively.

Do either of these form groups? Make a general conjecture concerning $\{0, 1, 2, \ldots, n-1\}$ under multiplication modulo n.

Now repeat the process with 0 removed from each set. How does this affect the result. Make a further general conjecture concerning $\{1, 2, \ldots, n-1\}$ under multiplication modulo n (you may need to try a few more examples to back up your idea – it's not immediately obvious what is going on).

For those instances that still do not form groups, can you generate a group by removing further elements from the set. If so, which ones? Is there a pattern? Try different examples of your own until you can make a further general conjecture.

Show Solution 3.3 on P199

Question 3.4

Giving a suitable notation, draw up the operation table for the symmetries of a rectangle. Do these form a group under function composition? If so, is the group abelian? Is it cyclic?

Show Solution 3.4 on P202

Chapter 4

Cosets and Lagrange's Theorem

The aim of this chapter is to prove Lagrange's Theorem, perhaps the most important result in finite group theory. Lagrange's Theorem states that the number of elements in a subgroup of a finite group $(G, \times)$ must divide the order of G. We begin with an important definition.

Definition 4.1 (Left Coset)**.** Let $(H, \times)$ be a subgroup of $(G, \times)$. For a fixed element $g \in G$, the set $gH = \{gh \mid h \in H\}$ is a *left coset* of H in $(G, \times)$. If $H = \{h_1, h_2, \ldots, h_m\}$ is finite, then $gH = \{g \times h_1, g \times h_2, \ldots, g \times h_m\}$.

Example 4.1. Let $(G, \circ)$ be the group of symmetries of an equilateral triangle, D_3. We reproduce the operation table for ease of reference.

$\circ$	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_3	s_1	s_2
r_2	r_2	e	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r_1	r_2
s_2	s_2	s_3	s_1	r_2	e	r_1
s_3	s_3	s_1	s_2	r_1	r_2	e

Now, if $H = \{e, s_1\}$, then:

- eH is equal to

  $\{e \circ e, e \circ s_1\} = \{e, s_1\}$

- r_1H is equal to

  $\{r_1 \circ e, r_1 \circ s_1\} = \{r_1, s_3\}$

- r_2H is equal to

  $\{r_2 \circ e, r_2 \circ s_1\} = \{r_2, s_2\}$

- s_1H is equal to

  $\{s_1 \circ e, s_1 \circ s_1\} = \{s_1, e\} = eH$

- s_2H is equal to

  $\{s_2 \circ e, s_2 \circ s_1\} = \{s_2, r_2\} = r_2H$

- s_3H is equal to

  $\{s_3 \circ e, s_3 \circ s_1\} = \{s_3, r_1\} = r_1H$

Example 4.2. Consider the group $\mathbb{Z}_{12}$. Draw the operation table. Find the distinct left cosets of the subgroup generated by 8

Solution:

$\oplus_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

Now $H = \langle 8 \rangle = \{0, 4, 8\}$. We compute the cosets:

$$
\begin{aligned}
0H &= \{0+0, 0+4, 0+8\} = \{0,4,8\} = 4H = 8H \\
1H &= \{1+0, 1+4, 1+8\} = \{1,5,9\} = 5H = 9H \\
2H &= \{2+0, 2+4, 2+8\} = \{2,6,10\} = 2H = 10H \\
3H &= = \{3+0, 3+4, 3+8\} = \{3,7,11\} = 3H = 7H = 11H.
\end{aligned}
$$

Note

- In D_3, the distinct left cosets of $H = \langle s_1 \rangle$ are

$$\{e, s_1\}, \quad \{r_1, s_3\} \text{ and } \{r_2, s_2\}.$$

- In $\mathbb{Z}_{12}$, the distinct left cosets of $H = \langle 8 \rangle$ are

$$\{0,4,8\}, \quad \{1,5,9\}, \quad \{2,6,10\}, \text{ and } \{3,7,11\}.$$

In both cases, the distinct left cosets *partition* the group. That is, each element of the group belongs to a unique left coset of the subgroup. Another way of saying this is

> The left cosets are disjoint (have no elements in common) and the union of all the left cosets is the group.

Notice also that all the left cosets have the same size as H. Therefore, as the cosets partition the group the size of H must be a divisor of the size of the group;

$$|D_3| = 3|H| \text{ and } |\mathbb{Z}_{12}| = 4|H|.$$

Lemma 4.1 (Cosets). *Let $(H, \times)$ be a subgroup of a finite group $(G, \times)$. Then,*

a. $\forall g \in G$, $g \in gH$,

b. $\forall g \in G$, $|gH| = |H|$,

c. $\forall g_1, g_2 \in G$, *either* $g_1 H = g_2 H$ *or* $g_1 H \cap g_2 H = \emptyset$.

Proof.

We take each in turn.

a. Since $e \in H$, then $g = g \times e \in gH$ and so $g \in gH$ for all $g \in G$.

b. Suppose $H = \{h_1, h_2, \ldots, h_m\}$. Let $g \in G$, then $gH = \{gh_1, gh_2, \ldots, gh_m\}$. To show that $|gH| = |H|$ we need to show that $gh_i \neq gh_j$ whenever $i \neq j$. Let i, j be such that $gh_i = gh_j$. Then by the Cancellation Laws, $h_i = h_j$. Thus, $|gH| = |H|$.

c. We prove the contrapositive, namely, we show that if two left cosets have an element in common then they are equal. Suppose $g_1, g_2 \in G$ and $g_1H_1 \cap g_2H_2 \neq \emptyset$. Let $g \in g_1H_1 \cap g_2H_2$. Then there are $h_1, h_2 \in H$ such that $g_1h_1 = g_2h_2 = g$. It follows that $g_1 = g_2(h_2h_1^{-1}) \in g_2H$. Thus, for any $h \in G$, $g_1h = g_2(h_2h_1^{-1})h \in g_2H$. We deduce that $g_1H \subseteq g_2H$. However by b. $|g_1H| = |g_2H|$ and so $g_1H = g_2H$.

□

Theorem 4.1 (Lagrange)**.** *Let $(H, \times)$ be a subgroup of a finite group $(G, \times)$. Then the number of elements in H divides the number of elements in G, that is $|H|$ divides $|G|$.*

Proof.

Let $g_1, g_2, \ldots, g_m \in G$ be such that $g_1H, g_2H, \ldots, g_mH$ are the distinct left cosets of H in G. We observe that by Lemma 4.1

$$G = g_1H \sqcup g_2H \sqcup \ldots \sqcup g_mH.$$

Using the facts that distinct cosets have trivial intersection (Lemma 4.1 part c.), we have

$$|G| = |g_1H| + |g_2H| + \ldots + |g_mH|.$$

The conclusion now follows from the fact that all the left cosets of H have the same size as H:

$$|G| = m \times |H|.$$

□

Example 4.3. The group of symmetries of an equilateral triangle, D_3. In the group of symmetries of an equilateral triangle, we have, by Lagrange's Theorem, that the *possible* subgroup orders are:

Divisor of $\lvert D3\rvert$	Subgroup
1	$\{e\}$
2	$\{e, s_i\}$, $i = 1, 2$
3	$\{e, r_1, r_2\}$
6	D_3

When faced with a result such as Lagrange's Theorem, most mathematicians start to think about the converse which, in this case, is if m divides $|G|$ does G necessarily have a subgroup of order m? The answer to this question turns out to be 'yes' if G is abelian, but 'no' for non-abelian groups. The smallest counter-example for non-abelian groups is the group of rotational symmetries of a regular tetrahedron, which is of order 12 but has no subgroup of order 6.

Corollary 4.1. *Let $(G, \times)$ be a finite group of order n and let g be an element with period k. Then*

i. k divides n (the period of an element divides the order of the group),

ii. $g^n = e$.

Proof.

i. By Theorem 3.2, $\langle g \rangle$ is a subgroup of G and $|\langle g \rangle| = k$. Therefore by Theorem 4.1, $k = |\langle g \rangle| \,|\, n = |G|$ as required.

ii. Since $k \mid n$, then there is an $l \in \mathbb{N}$ such that $kl = n$. It follows that

$$g^n = g^{kl} = (g^k)^l = e^l = e.$$

□

Example 4.4. Find the possible order of elements of the group of symmetries of an equilateral triangle, D_3 and identify the elements of D_3 (if any) of that order.

Solution:

Possible order	Element
1	e
2	s_i, $i = 1, 2$
3	r_1, r_2
6	none

An easy application of this corollary is that there is essentially only one type of group of prime order.

Theorem 4.2. *Let $(G, \times)$ be a finite group of order p, where p is prime. Then $(G, \times)$ is cyclic.*

Proof.

Let $a \in G$ be any non-identity element of $(G, \times)$. Then the period of a is a divisor of p. Now since a is not the identity element of $(G, \times)$, it cannot gave order 1 (since otherwise $a^1 = a = e$). It follows that a has order p. Thus, $\langle a \rangle = G$ since $| \langle a \rangle = |G|$. We conclude that $(G, \times)$ is cyclic.

□

4.1 Problem Sheet 4

For Week 6; covers Chapter 4.

Question 4.1

Let G be the symmetry group of a regular hexagon. The Cayley table is below.

$\circ$	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
e	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
r_1	r_1	r_2	r_3	r_4	r_5	e	s_6	s_1	s_2	s_3	s_4	s_5
r_2	r_2	r_3	r_4	r_5	e	r_1	s_5	s_6	s_1	s_2	s_3	s_4
r_3	r_3	r_4	r_5	e	r_1	r_2	s_4	s_5	s_6	s_1	s_2	s_3
r_4	r_4	r_5	e	r_1	r_2	r_3	s_3	s_4	s_5	s_6	s_1	s_2
r_5	r_5	e	r_1	r_2	r_3	r_4	s_2	s_3	s_4	s_5	s_6	s_1
s_1	s_1	s_2	s_3	s_4	s_5	s_6	e	r_1	r_2	r_3	r_4	r_5
s_2	s_2	s_3	s_4	s_5	s_6	s_1	r_5	e	r_1	r_2	r_3	r_4
s_3	s_3	s_4	s_5	s_6	s_1	s_2	r_4	r_5	e	r_1	r_2	r_3
s_4	s_4	s_5	s_6	s_1	s_2	s_3	r_3	r_4	r_5	e	r_1	r_2
s_5	s_5	s_6	s_1	s_2	s_3	s_4	r_2	r_3	r_4	r_5	e	r_1
s_6	s_6	s_1	s_2	s_3	s_4	s_5	r_1	r_2	r_3	r_4	r_5	e

For *the* subgroup of order 3, find its left cosets in G.

Show Solution 4.1 on P203

Question 4.2

Let G be the symmetry group of a regular octagon. Using the Cayley table below find all of the subgroups of orders 2 and 4. For each of those subgroups find the distinct left cosets.

$\circ$	e	r_1	r_2	r_3	r_4	r_5	r_6	r_7	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
e	e	r_1	r_2	r_3	r_4	r_5	r_6	r_7	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
r_1	r_1	r_2	r_3	r_4	r_5	r_6	r_7	e	s_8	s_1	s_2	s_3	s_4	s_5	s_6	s_7
r_2	r_2	r_3	r_4	r_5	r_6	r_7	e	r_1	s_7	s_8	s_1	s_2	s_3	s_4	s_5	s_6
r_3	r_3	r_4	r_5	r_6	r_7	e	r_1	r_2	s_6	s_7	s_8	s_1	s_2	s_3	s_4	s_5
r_4	r_4	r_5	r_6	r_7	e	r_1	r_2	r_3	s_5	s_6	s_7	s_8	s_1	s_2	s_3	s_4
r_5	r_5	r_6	r_7	e	r_1	r_2	r_3	r_4	s_4	s_5	s_6	s_7	s_8	s_1	s_2	s_3
r_6	r_6	r_7	e	r_1	r_2	r_3	r_4	r_5	s_3	s_4	s_5	s_6	s_7	s_8	s_1	s_2
r_7	r_7	e	r_1	r_2	r_3	r_4	r_5	r_6	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_1
s_1	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	e	r_1	r_2	r_3	r_4	r_5	r_6	r_7
s_2	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_1	r_7	e	r_1	r_2	r_3	r_4	r_5	r_6
s_3	s_3	s_4	s_5	s_6	s_7	s_8	s_1	s_2	r_6	r_7	e	r_1	r_2	r_3	r_4	r_5
s_4	s_4	s_5	s_6	s_7	s_8	s_1	s_2	s_3	r_5	r_6	r_7	e	r_1	r_2	r_3	r_4
s_5	s_5	s_6	s_7	s_8	s_1	s_2	s_3	s_4	r_4	r_5	r_6	r_7	e	r_1	r_2	r_3
s_6	s_6	s_7	s_8	s_1	s_2	s_3	s_4	s_5	r_3	r_4	r_5	r_6	r_7	e	r_1	r_2
s_7	s_7	s_8	s_1	s_2	s_3	s_4	s_5	s_6	r_2	r_3	r_4	r_5	r_6	r_7	e	r_1
s_8	s_8	s_1	s_2	s_3	s_4	s_5	s_6	s_7	r_1	r_2	r_3	r_4	r_5	r_6	r_7	e

Show Solution 4.2 on P205

Chapter 5

Isomorphisms and Homomorphisms

As we mentioned at the outset, abstract algebra is concerned with 'structure' rather than 'content'; it studies generalised properties of mathematical structures rather than the components of those structures. In this chapter we examine functions that preserve structure and allow us to decide when two structures are 'essentially the same'. We will begin with the latter.

5.1 Group Isomorphisms

Let G_1 be the group formed by $\{1, -1, i, -i\}$ under multiplication and G_2 be the subgroup of the group of symmetries of a square generated by r_1, an anticlockwise rotation of $\pi/2$ radians; thus G_2 is the group $(\{e, r_1, r_2, r_3\}, \circ)$ where the operation is function composition. These two groups produce the following operation tables:

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\circ$	e	r_1	r_2	r_3
e	e	r_1	r_2	r_3
r_1	r_1	r_2	r_3	e
r_2	r_2	r_3	e	r_1
r_3	r_3	e	r_1	r_2

These groups are 'essentially the same'. To see this, in the first table, replace 1 by e, -1 by r_2, i by r_1 and $-i$ by r_3. What we get is the second table re-ordered slightly:

$\circ$	e	r_2	r_1	r_3
e	e	r_2	r_1	r_3
r_2	r_2	e	r_3	r_1
r_1	r_1	r_3	r_2	e
r_3	r_3	r_1	e	r_2

We have swapped the 2nd and 3rd rows and columns. Notice that the multiplication works the same in the re-ordered table as in the original.

More formally, what we have is a *bijective* map $\theta : G_1 \to G_2$ by

$$\begin{aligned} \theta(1) &= e \\ \theta(-1) &= r_2 \\ \theta(i) &= r_1 \\ \theta(-i) &= r_3. \end{aligned}$$

The fact that when we replace the elements in the first table with their image under θ gives a rearrangement of the second table is captured precisely by the fact that for all $x, y \in G_1$, $\theta(x \times y) = \theta(x) \circ \theta(y)$.

Definition 5.1 (Isomorphism)**.** Let $(G_1, *)$ and $(G_2, \odot)$ be groups. Then $(G_1, *)$ and $(G_2, \odot)$ are *isomorphic* if and only if there exists a mapping $\theta : G_1 \to G_2$ (called an *isomorphism*) such that:

i. θ is bijective (i.e. both injective and surjective);

ii. $\theta(x * y) = \theta(x) \odot \theta(y),\ \forall\, x, y \in G_1$.

Notice that for any group, G, the identity mapping is an isomorphism from G to itself. Also, if θ is an isomorphism from G_1 to G_2, then θ^{-1} is an isomorphism from G_2 to G_1 (we therefore talk about groups being isomorphic to each other). Furthermore, if θ is an isomorphism from G_1 to G_2 and ϕ is an isomorphism from G_2 to G_3, then $\phi \circ \theta$ is an isomorphism from G_1 to G_3.

Notationally, if $\theta : G_1 \to G_2$ is an isomorphism, we say that G_1 and G_2 are isomorphic and write $G_1 \cong G_2$.

How do we show that two groups $(G_1, *)$ and $(G_2, \odot)$ are isomorphic? For small groups we can use trial and error, but for large groups, and certainly for infinite groups, we need a different approach.

Step 1: Find a candidate function $\theta : G_1 \to G_2$.

Step 2: Show that θ is injective. That is, we show that for any pair $a, b \in G_1$ such that $\theta(a) = \theta(b)$ then $a = b$.

Step 3: Show that θ is surjective. That is, we show that given $x \in G_2$ there is an element $a \in G_1$, such that $\theta(a) = x$.

Step 4: **Step 2** and **Step 3** above establish the fact that θ is a bijection. To show that θ is an homomorphism, we lastly need to verify that for all $a, b \in G_1$,

$$\theta(a * b) = \theta(a) \odot \theta(b).$$

Example 5.1 (Examples of isomorphic infinite groups)**.**

(a) $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}^+, \times)$.

Solution:

Step 1: Define $\theta : \mathbb{R} \to \mathbb{R}^+$ by $\theta(x) = e^x$. Notice that $e^x \in \mathbb{R}^+$ for all $x \in \mathbb{R}$.

Step 2: Let $a, b \in \mathbb{R}$ and suppose that $\mathrm{e}^a = \mathrm{e}^b$. Taking logs, we get that $a = b$. So θ is injective.

Step 3: Let $x \in \mathbb{R}^+$. Then since $x > 0$, $\ln(x)$ is an element of $\mathbb{R}$. Observe that

$e^{\ln(x)} = x$. Therefore, θ is surjective.

Step 4: Let $a, b \in \mathbb{R}$ be arbitrary. We have

$$\theta(a+b) = \mathrm{e}^{a+b} = \mathrm{e}^{a} \times \mathrm{e}^{b} = \theta(a) \times \theta(b).$$

We conclude that θ is an isomorphism and so $(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$.

(b) $(\mathbb{Z}, +)$ is isomorphic to $(2\mathbb{Z}, +)$.

Solution:

Step 1: Define $\theta : \mathbb{Z} \to 2\mathbb{Z}$ by $\theta(n) = 2n$.

Step 2: Let $m, n \in \mathbb{Z}$ and suppose that $\theta(m) = \theta(n)$. Then $2m = 2n$ which means that $m = n$. Therefore θ is injective.

Step 3: Let $k \in 2\mathbb{Z}$. Then $k = 2m$ for some $m \in \mathbb{Z}$. It follows that $\theta(m) = 2m = k$. Therefore θ is surjective.

Step 4: Let $m, n \in \mathbb{Z}$. We have

$$\theta(m+n) = 2(m+n) = 2m + 2n = \theta(m) + \theta(n).$$

How do we show that two groups $(G_1, *)$ and $(G_2, \odot)$ are not isomorphic? This would mean that there is no bijective function from G_1 to G_2 such that $\theta(x * y) = \theta(x) \odot \theta(y)$, for all $x, y \in G_1$. In general we cannot try all possible bijections unless, of course, none exist, for example when G_1 and G_2 have different orders.

Example 5.2. The group of symmetries of an equilateral triangle is not isomorphic to the group $(\{1, -1, i, -i\}, \times)$. There are six elements in D_3 so there is no bijection from D_3 to $\{1, -1, i, -i\}$ (and hence no isomorphism).

We say that the order of a group is *preserved by isomorphism*. The following lemma provides more such properties and these are frequently helpful in showing that two groups are not isomorphic, or in spotting an isomorphism if there is one.

Lemma 5.1. *Let $(G_1, *)$ and $(G_2, \odot)$ be groups and $\theta : G_1 \to G_2$ an isomorphism. Then:*

i. if e is the identity in $(G_1, *)$, then $\theta(e)$ is the identity in $(G_2, \odot)$;

ii. for all $x \in G_1$, $\theta(x^{-1}) = (\theta(x))^{-1}$;

iii. for all $x \in G_1$, x and $\theta(x)$ have the same period;

iv. $(G_1, *)$ is abelian if and only if $(G_2, \odot)$ is abelian;

v. if H is a subgroup of G_1, then $\theta(H) = \{\theta(h) \mid h \in H\}$ is a subgroup of G_2.

Proof. We take each in turn.

i. Observe that

$$\theta(e) = \theta(e * e) = \theta(e) \odot \theta(e).$$

Multiplying on both sides by $\theta(e)^{-1}$ give the result.

ii. Let $x \in G_1$. Then

$$\theta(e) = \theta(x * x^{-1}) = \theta(x) \odot \theta(x^{-1})$$

. Since $\theta(e)$ is the identity element of G_2, it follows by Corollary 3.1 that $(\theta(x))^{-1} = \theta(x^{-1})$.

iii. Let $x \in G_1$. We first establish by induction that $\theta(x^i) = (\theta(x))^i$ for all $i \in \mathbb{N}$.

base case: This occurs when $i = 0$. In this case

$$\theta(x^0) = \theta(e) = (\theta(x))^0$$

since $\theta(e)$ is the identity element of G_2.

inductive hypothesis: Assume that $\theta(x^j) = (\theta(x))^j$ for all $j \in N$ with $j < i$.

inductive step: We consider $\theta(x^i)$. We have

$$\theta(x^i) = \theta(x * x^{i-1}) = \theta(x) \odot \theta(x^{i-1}) = \theta(x) \odot (\theta(x))^{i-1} = (\theta(x))^i.$$

Now we consider two cases.

Firstly that x has infinite period. Suppose $(\theta(x))^i = \theta(e)$ for some $i \in \mathbb{Z}^+$. This means, by the preceding, that $\theta(x^i) = \theta(e)$. However, θ is a bijection, and so it is injective, it follows that $x^i = e$. This is a contradiction. We conclude that $(\theta(x))^i$ is not the identity element of G_2 for any $i \in \mathbb{Z}^+$ — $\theta(x)$ also has infinite order.

Now suppose that x has period m. We observe that

$$(\theta(x))^m = \theta(x^m) = \theta(e)$$

and so the period of $\theta(x)$ is at most m. However, if $(\theta(x))^l$ is not the identity element of G_2 for any $0 \leq l < m$, since, as in the previous case, this will mean that $\theta(x^l) = \theta(e)$ and so $x^l = e$ which is not possible.

iv. **(→):** Suppose that $(G, *)$ is abelian. Let $x, y \in G_2$ be arbitrary. There are elements $a, b \in G_1$ such that $\theta(a) = x$ and $\theta(b) = y$. Now observe

$$\begin{aligned} x \odot y &= \theta(a) \odot \theta(b) \\ &= \theta(a * b) \\ &= \theta(b * a) \\ &= \theta(b) * \theta(a) \\ &= y \odot x. \end{aligned}$$

We conclude that $x \odot y = y \odot x$ for all $x, y \in G_2$.

(←): Suppose that $(G_2, \odot)$ is abelian. Let $a, b \in G_1$. Since θ is a bijection, we can

find $x, y \in G_2$ such that $a = \theta(x)$ and $b = \theta(y)$. Now observe that

$$\begin{aligned} a * b &= \theta^{-1}(\theta((a * b) \\ &= \theta^{-1}(theta(a) \odot \theta(b)) \\ &= \theta^{-1}(\theta(b) \odot \theta(a)) \\ &= \theta^{-1}(\theta(b * a)) \\ &= b * a. \end{aligned}$$

Therefore, $a * b = b * a$ for all $a, b \in G_1$ and $(G_1, *)$ is abelian.

v. We apply The Subgroup Test to $\theta(H)$. Clearly $\theta(H)$ is non-empty as it contains $\theta(e)$ ($e \in H$.)

Closure: Let $h_1, h_2 \in H$. We want to show that $\theta(h_1) \odot \theta(h_2) \in \theta(H)$. We have:

$$\theta(h_1) \odot \theta(h_2) = \theta(h_1 * h_2).$$

Therefore, as $h_1 * h_2 \in H$, $\theta(h_1) \odot \theta(h_2) \in \theta(H)$.

Inverses: Let $h_1 \in H$. Then, by part ii. $(\theta(h_1))^{-1} = \theta(h_1^{-1})$. Since $h_1 \in H$, and H is a subgroup of $(G, *)$, then $h_1^{-1} \in H$ and $(\theta(h_1))^{-1} \in \theta(H)$.

□

One of the major questions in the study of groups is, for a given positive integer n, what are the groups of order n up to isomorphism? What we mean by this is, can we describe a set of isomorphically distinct groups of order n which is complete in the sense that every group of order n is isomorphic to a member of this set? We will show that the answer is easy to describe for abelian groups, but the answer for non-abelian groups required many years of research (and, arguably, has yet to be completed). Below we give a complete list of isomorphically distinct groups of order less than eight. We have already seen $\mathbb{Z}_n$ as the canonical form of a cyclic group of order n, generated by the element 1; we shall study groups

of the type $\mathbb{Z}_m \times \mathbb{Z}_n$ in Chapter 7.

Order	Group	
Order 1	$+ \mid 0$ $0 \mid 0$ $\mathbb{Z}_1$	
Order 2	$+ \mid 0 \;\; 1$ $0 \mid 0 \;\; 1$ $1 \mid 1 \;\; 0$ $\mathbb{Z}_2$	
Order 3	$+ \mid 0 \;\; 1 \;\; 2$ $0 \mid 0 \;\; 1 \;\; 2$ $1 \mid 1 \;\; 2 \;\; 0$ $2 \mid 2 \;\; 0 \;\; 1$ $\mathbb{Z}_3$	
Order 4	$+ \mid 0 \;\; 1 \;\; 2 \;\; 3$ $0 \mid 0 \;\; 1 \;\; 2 \;\; 3$ $1 \mid 1 \;\; 2 \;\; 3 \;\; 0$ $2 \mid 2 \;\; 3 \;\; 0 \;\; 1$ $3 \mid 3 \;\; 0 \;\; 1 \;\; 2$ $\mathbb{Z}_4$	$+ \mid 0 \;\; 1 \;\; 2 \;\; 3$ $0 \mid 0 \;\; 1 \;\; 2 \;\; 3$ $1 \mid 1 \;\; 0 \;\; 3 \;\; 2$ $2 \mid 2 \;\; 3 \;\; 0 \;\; 1$ $3 \mid 3 \;\; 2 \;\; 1 \;\; 0$ $\mathbb{Z}_2 \times \mathbb{Z}_2$

Order	Group

Order 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\mathbb{Z}_5$

Order 6

$+$	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

$\mathbb{Z}_6$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	0	5	3	4
2	2	0	1	4	5	3
3	3	4	5	0	1	2
4	4	5	3	2	0	1
5	5	3	4	1	2	0

D_3

Order	Group

Order 7

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\mathbb{Z}_7$

Note that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the smallest non-cyclic group and D_3 the smallest non-abelian group.

There are five isomorphically distinct groups of order 8; three of these are abelian, namely $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (spotting a pattern?) and two are non-abelian, namely D_4 and the quaternion group Q_8.

Observe, also, that so far we only have one group of order n when n is prime; this is a consequence of the following result combined with the fact that, by Theorem 4.2, a group of prime order is necessarily cyclic.

We now state and prove an extremely important and useful result:

Theorem 5.1. *Two cyclic groups of the same order are isomorphic.*

Proof.

Let $G_1 = \langle a \rangle$ and $G_2 = \langle b \rangle$ be cyclic groups of the same order. Define a map $\theta : G_1 \to G_2$ by $\theta(a^i) = b^i$ for all $i \in \mathbb{Z}$

Clearly θ is surjective since $G_2 = \{b^i : i \in \mathbb{Z}\}$.

Suppose $\theta(a^i) = \theta(a^j)$ for $i, j \in \mathbb{Z}$. Then $b^i = b^j$. Therefore, $b^{i-j} = e_{G_2}$. This only happens if b has finite period m such that $m|(i-j)$. In this case there is a $k \in \mathbb{Z}$ such that $i = j+km$. Now, since the period of a and b are equal, we must have that

$$a^i = a^{j+km} = a^j(a^m)^k = a^j e_{G_1} = a^j.$$

We conclude that θ is injective.

Finally let $a^i, a^j \in \langle a \rangle$. Then

$$\theta(a^i a^j) = \theta(a^{i+j}) = b^{i+j} = b^i b^j = \theta(a^i)\theta(a^j).$$

Therefore θ is an isomorphism and $G_1 \cong G_2$.

□

Example 5.3. We have shown that the set

$$M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{R}_{2\times 2} : a, b \text{ not both zero} \right\},$$

forms a subgroup of $\mathrm{GL}(2, \mathbb{R})$ under matrix multiplication. Show that M is isomorphic to $(\mathbb{C}\backslash\{0\}, \times)$.

Solution:

Step 1:

Define a map $\theta : M \to \mathbb{C}\backslash\{0\}$ by

$$\theta\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + ib.$$

Since a and b are not both zero, it is clear that $a + ib \neq 0$.

Step 2: We show that θ is injective. Let

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ and } C = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in M.$$

Suppose that $\theta(A) = \theta(C)$. Then $a + ib = c + id$. This is only possible if $a = c$ and $b = c$. This means that $A = C$. It follows that θ is injective.

Step3: We show that θ is surjective. Let $a + ib \in \mathbb{C}\backslash\{0\}$. Notice that since $a + ib \neq 0$, then a and b are not both zero. Therefore

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M.$$

Moreover, $\theta(A) = a + ib$.

Step 4: Let

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

and

$$C = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

be elements of M. Then

$$\begin{aligned} \theta(AC) &= \theta\left(\begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}\right) \\ &= (ac - bd) + i(ad + ab) \\ &= (a + ib)(c + id) \\ &= \theta(A)\theta(C). \end{aligned}$$

It follows that $\theta : (M, \times) \to (\mathbb{C}\backslash\{0\}, \times)$ is an isomorphism and so $(M, \times) \cong (\mathbb{C}\backslash\{0\}, \times)$.

Example 5.4. How do you know that the group represented by the following operation table must be isomorphic to $\mathbb{Z}_6$?

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	f	a	d	e
c	c	f	e	b	a	d
d	d	a	b	e	f	c
e	e	d	a	f	c	b
f	f	e	d	c	b	a

Find an isomorphism between the two groups.

Solution:

If the group represented by the table is isomorphic to $\mathbb{Z}_6$, then it must have an element of order 6. Notice that a has to be the identity element since $a*x = x$ for all $x \in \{a, b, c, d, e, f\}$. We can now work through the elements in turn to see which have order 6. For b we observe that

$$b^2 = c,\ b^3 = bc = f,\ b^4 = bf = e,\ b^5 = be = d,\ b^6 = bd = a.$$

Therefore b has order 6. Following the proof of Theorem 5.1, the map $\theta : \langle b \rangle \to \mathbb{Z}_6$ by $b^i = i$ for all $0 \leq i \leq 5$ is an isomorphism.

5.2 Group Homomorphisms

As we mentioned at the beginning of the chapter, we are interested in functions that preserve structure. Such functions are called homomorphisms. We begin with a definition.

Definition 5.2 (Homomorphism)**.** Let $(G_1, *)$ and $(G_2, \circ)$ be groups. A mapping $\phi : G_1 \to G_2$ is a (group) *homomorphism* if and only if for all $x, y \in G_1$

$$\phi(x * y) = \phi(x) \circ \phi(y).$$

Note that an isomorphism is precisely a bijective homomorphism.

Example 5.5 (Positive and Negative examples)**.**

1. $G_1 = G_2 = (\mathbb{R}, +),\ \phi(x) = |x|,\ \forall\, x \in \mathbb{R}.$

   This map is not a homomorphism. Consider $-2, 3 \in \mathbb{R}$,

   $$\phi(3 + (-1)) = \phi(2) = |2| \neq 4 = |3| + |-1| = \phi(3) + \phi(-1).$$

2. $G_1 = G_2 = (\mathbb{R}\backslash\{0\}, \times),\ \phi(x) = |x|,\ \forall\, x \in \mathbb{R}\backslash\{0\}.$

   This map is a homomorphism. Let $x, y \in \mathbb{R}\backslash\{0\}$. Then

   $$\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y).$$

   Note that ϕ is not an isomorphism since it is not a bijection.

3. $G_1 = GL(2, \mathbb{R}), G_2 = (\mathbb{R}\backslash\{0\}, \times),\ \phi(A) = \det A,\ \forall\, A \in GL(2, \mathbb{R}).$

   This map is a homomorphism. Let $A, B \in G_1$. Then,

   $$\phi(AB) = \det AB = \det A \det B = \phi(A)\phi(B).$$

   Note that ϕ is not an isomorphism. There are infinitely many elements of G_1 with determinant equal to 1 for example.

Example 5.6. Consider the function $f : \mathbb{C}\backslash\{0\} \to \mathbb{R}\backslash\{0\}$ defined by

$$\forall\, a, b \in \mathbb{R}, \quad f(a + ib) = a^2 + b^2.$$

Establish whether f is a homomorphism, and whether it is an isomorphism, from $(\mathbb{C}\backslash\{0\}, \times)$ to $(\mathbb{R}\backslash\{0\}, \times)$.

Solution:

Let $a+ib, c+id \in \mathbb{C}\backslash\{0\}$ for where $a, b, c, d \in \mathbb{R}$. Then

$$\begin{aligned} f((a+ib)(c+id)) &= f((ac-bd)+i(bc+ad)) \\ &= (ac-bd)^2+(bc+ad)^2 \\ &= a^2c^2-2acbd+b^2d^2+b^2c^2+2abcd+a^2d^2 \\ &= a^2c^2+b^2d^2+b^2c^2+a^2d^2 \\ &= c^2\left(a^2+b^2\right)+d^2\left(a^2+b^2\right) \\ &= \left(a^2+b^2\right)\left(c^2+d^2\right) \\ &= f(a+ib)f(c+id) \end{aligned}$$

It follows that f is a homomorphism. Note that f is not an isomorphism since it is not a bijection. Indeed f is not surjective since there is no $z \in \mathbb{C}\backslash\{0\}$ such that $f(z) = -1$ for example.

Example 5.7. Let $(G_1, \circ)$ and $(G_2, *)$ be groups and $\theta : G_1 \to G_2$ be a surjective homomorphism. For each of the following statements, either prove that it is true or provide a counter-example.

a. If $(G_1, \circ)$ is abelian, then $(G_2, *)$ is abelian.

b. If $(G_2, *)$ is abelian, then $(G_1, \circ)$ abelian.

What goes wrong?

What is wrong with the following argument: Let $a, b \in G_1$. Then:

$$\begin{aligned} \theta(a \circ b) &= \theta(a) * \theta(b) \\ &= \theta(b) * \theta(a) \\ &= \theta(b \circ a). \end{aligned}$$

Thus, $\theta(a \circ b) = \theta(b \circ a)$ and so $a \circ b = b \circ a$ for all $a, b \in G_1$.

This argument does not work because θ might not necessarily be injective and so we cannot conclude that $a \circ b = b \circ a$.

Solution:

a. This statement is true. Let $x, y \in G_2$. Since θ is surjective, there are $a, b \in G_1$ such that $\theta(a) = x$ and $\theta(b) = y$. We now have:

$$\begin{aligned} x * y &= \theta(a) * \theta(b) \\ &= \theta(a \circ b) \\ &= \theta(b \circ a) \\ &= \theta(b) \circ \theta(a) \\ &= y * x. \end{aligned}$$

Therefore $x * y = y * x$ for all $x, y \in G_2$.

b. This statement is false. Indeed we have already seen a counter example. The map $\det : GL(2, \mathbb{R}) \to \mathbb{R}\backslash\{0\}$ is a homomorphism, however $GL(2, \mathbb{R})$ is a non-abelian group.

As we have said, a homomorphism is a structure-preserving mapping. If ϕ is a homomorphism from a group G into a group G', then we can get information about the structural properties of G' from the structural properties of G. An example of this is provided by the following lemma:

Lemma 5.2. *Let ϕ be a homomorphism from a group G to a group G'. Then,*

i. if e is the identity in G, then $\phi(e)$ is the identity in G',

ii. for all $x \in G$, $\phi(x^{-1}) = (\phi(x))^{-1}$.

Proof.

i. We have

$$\phi(e) = \phi(ee) = \phi(e)\phi(e).$$

It follows that $\phi(e)$ must be the identity element of G' by cancelling.

ii. Let $x \in G$. We have,

$$\phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}).$$

We conclude that $\phi(x) = (\phi(x))^{-1}$.

□

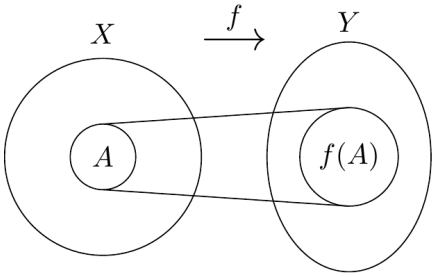
In the case of an isomorphism, the bijectivity of the function means that we preserve not only the structure but also the 'size', in the sense that isomorphic groups must have the same order. It is natural in the case of non-bijective homomorphisms, therefore, to investigate how structure is preserved between groups of different orders; that is, to investigate how the function 'scales' the structure that it preserves. A very loose analogy would be to consider a map of England, say, but being careful how the word 'map' is used. One possible scaling would be to map everything to a single point; small enough to fit in your pocket, totally useless, but still a map! Alternatively one could use a scale of 1:1 which would make the map an exact replica in terms of size, but again the utility of such a map is open to doubt. In practical terms we need something that scales down the original to a usable size. Using this as an analogy, where the 'scaling factor' is represented by our group homomorphism, the first case would be tantamount to mapping everything in G onto just one element of G', whereas the second case would represent an isomorphism. So, what about something in between? First, we make the following definitions.

Definition 5.3 (Image and Preimage)**.** Let f be a mapping of a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$ The *image* of A under f, which is a subset of Y, is denoted and defined by

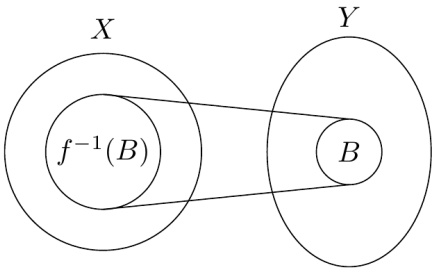
$$f(A) = \{f(a) \mid a \in A\}.$$

The *preimage* of B under f, which is a subset of X, is denoted and defined by

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$



The image of A in Y



The preimage of B in X

The first observation to make at this juncture is that *the image of a group under a group homomorphism is a group*. This follows if $H = G$ in the theorem below.

Theorem 5.2. *Let ϕ be a group homomorphism from G into G'. Then, for any subgroup H of G, $\phi(H)$ is a subgroup of G'.*

Proof.

We carry out the Subgroup Test on $\phi(H)$. We note that $\phi(H)$ is non-empty as it contains $\phi(e)$ the identity element of G'.

Let $a, b \in H$. We want to show that $\phi(a)\phi(b)$ is en element of $\phi(H)$. Observe that:

$$\phi(ab) = \phi(a)\phi(b).$$

Since $ab \in H$, it follows that $\phi(ab) \in \phi(H)$ and so $\phi(a)\phi(b) \in \phi(H)$ as required.

Let $a \in H$. We want to show that $(\phi(a))^{-1} \in \phi(H)$. However, $\phi(a^{-1}) = (\phi(a))^{-1}$. Since $a^{-1} \in H$, we conclude that $(\phi(a))^{-1} \in \phi(H)$ as required.

□

If we are to continue our analogy, we need to consider a suitable 'scaling' factor. Suppose we

consider the set of elements of G that map onto the identity in G' under some homomorphism ϕ. This leads to the following formal definition:

Definition 5.4 (Kernel)**.** Let ϕ be a group homomorphism from a group G into a group G' and e' be the identity in G'. The *kernel* of ϕ is denoted and defined by

$$\ker(\phi) = \{x \in G \mid \phi(x) = e'\}.$$

Example 5.8.

Let $\phi : \mathbb{Z} \to \mathbb{Z}_2$ be defined by

$$\phi(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \text{ is odd.} \end{cases}$$

Then ϕ is a homomorphism and $\ker(\phi) = 2\mathbb{Z}$.

Example 5.9.

Let $\phi : GL(2, \mathbb{R}) \to \mathbb{R}\backslash\{0\}$ by $\phi(A) = \det(A)$. Then ϕ is a homomorphism and $\ker(\phi) = \{A \in GL(2, \mathbb{R}) \mid \det(A) = 1\}$.

Example 5.10.

Let $G = \mathbb{Z}_6$ and G' be the subgroup $\langle r_1 \rangle = \langle r_2 \rangle = \{e, r_1, r_2\}$ of D_3.

Define $\phi : G \to G'$ by $\phi(n) = r_1^n$. Then ϕ is a homomorphism (check this as an exercise).

Looking at the image of ϕ we have:

$$\begin{aligned}
\phi(0) &= e \\
\phi(1) &= r_1 \\
\phi(2) &= r_2 \\
\phi(3) &= e \\
\phi(4) &= r_1 \\
\phi(5) &= r_2.
\end{aligned}$$

It follows that $\ker(\phi) = \{0, 3\}$. Observe that $\ker(\phi) = \langle 3 \rangle$ and so $\ker(\phi)$ is a subgroup of $\mathbb{Z}_6$.

What can we say about the kernel of a homomorphism? Actually, quite a lot, and such matters will be studied in detail in the Year 3 Group Theory module. For the moment, though, we shall restrict our attention to two properties.

Theorem 5.3. *Let ϕ be a group homomorphism from G into G'. Then, $\ker(\phi)$ is a subgroup of G.*

Proof.

Notice that $\ker(\phi)$ is a non-empty subset of G since it contains the identity element of G ($\phi(e) = e'$ where e' is the identity element of G').

Let $a, b \in \ker(\phi)$. Then,

$$\phi(ab) = \phi(a)\phi(b) = e'e' = e'.$$

Thus $ab \in \ker(\phi)$.

Let $a \in \ker(\phi)$. Then,

$$\phi(a^{-1}) = (\phi(a))^{-1} = (e')^{-1} = e'.$$

Therefore $a^{-1} \in \ker(\phi)$.

It follows that $\ker(\phi)$ is a subgroup of G.

□

In fact, the kernel of a homomorphism is more than a mere subgroup of the domain; it is what is known as a *normal subgroup*, which is characterised by the property that its left and right cosets coincide (again, more of normal subgroups next year).

For the second property we need to revisit the example above where we had a homomorphism mapping from $\mathbb{Z}_6$ to the subgroup of D_3 containing the identity and the rotations r_1 and r_2. Consider the sizes of the sets involved....

Size of set	Description
$\lvert\mathbb{Z}_6\rvert = 6$	Domain of ϕ
$\lvert\{e, r_1, r_2\}\rvert = 3$	Image of ϕ
$\lvert\ker(\phi)\rvert = \lvert\{0, 3\}\rvert = 2$	Kernel of ϕ

Notice that

$$\frac{\text{Size of group}}{\text{Size of kernel}} = \text{ Size of Image.}$$

This result holds for *finite* groups in general; that is, if a homomorphism ϕ maps from a group G to a group G', then the size of the image of G under ϕ is equal to the size of G divided by the size of the kernel of ϕ. This is scratching the surface of a major structural theorem of groups, namely the First Isomorphism Theorem (not surprisingly, studied in detail in Year 3 Group Theory!).

5.3 Problem Sheet 5

For Week 6; covers Chapter 5.

Question 5.1

Show that the group of real numbers under addition is isomorphic to the group of matrices representing shears parallel to the x-axis.

(Recall that this is a type of linear transformation and you studied these in Algebra II. It involves moving a point a fixed distance parallel to the x-axis, that distance being dependent on the y-coordinate of the point. Such transformations can be represented by 2×2 matrices of the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, where a is any real number.)

Show Solution 5.1 on P207

Question 5.2

Consider the set $G = \{1, 2, 3, 4, 5, 6\}$. This set forms a group under multiplication modulo 7.

a. Draw and complete the operation table for the group $(G, \otimes_7)$.

b. Find the period of each element in the group.

c. Find an isomorphism between this group and $\mathbb{Z}_6$.

Show Solution 5.2 on P208

Chapter 6

Permutation Groups

Consider the following, highly unrealistic, scenario. You have ten maths books on your bookshelf and one Friday evening, having nothing whatsoever better to do, you decide to arrange them in a different order. Having done this once you realise that there are many ways to rearrange the books and your mind turns to calculating that number. Clearly there are ten possible choices for the first book. For each of these ten possibilities there will be nine choices for the second book; thus there are 10×9 ways of choosing the first two books. Continuing this argument leads you to conclude that the total number of ways of ordering the ten books is $10 \times 9 \times 8 \times \ldots \times 2 \times 1 = 10! = 3,628,800$ and assuming that each rearrangement takes 30 seconds to complete it will take you 3 years 165 days (assuming no leap year) to try out all possible arrangements.

6.1 Permutations

In the above example we refer to each arrangement as a *permutation* of the set of books. It should be clear that each permutation is simply a mapping from the set of books onto itself, where the mapping determines the order of the particular arrangement or permutation. Obviously, the mapping is a bijection (think about it) and we can now make the following formal definition.

Definition 6.1 (Permutation)**.** A *permutation* of a finite set, X, is a function $f : X \to X$ that is bijective.

Example 6.1. Consider the set $S = \{a, b, c, d\}$. and let f be the permutation of S such that

$$\begin{aligned} f(a) &= c \\ f(b) &= b \\ f(c) &= d \\ f(d) &= a \end{aligned}$$

We write f in a more standard way, changing the columns to rows in parentheses and omitting equals signs, as follows:

$$f = \begin{pmatrix} a & b & c & d \\ c & b & d & a \end{pmatrix}$$

Since a permutation is a function, we can compose any number of permutations and, since a permutation is a bijective function, it makes sense to talk about its inverse.

Example 6.2. Let $S = \{1, 2, 3, 4, 5\}$ be a set and f and g be permutations of S defined by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \qquad \text{and} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}.$$

Find $f \circ g$, $g \circ f$ (are they the same?), g^2 and g^{-1}.

Solution:

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$
$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

So $f \circ g \neq g \circ f$.

We carry out the remaining compositions:

$$g^2 = g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$
$$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

Notice that

$$g \circ g^{-1} = g^{-1} \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathrm{id}\,.$$

Example 6.3. Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$. Calculate fg, gf, and f^{-1}.

Solution:

We have

$$
\begin{aligned}
fg &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \\
gf &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \\
f^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}
\end{aligned}
$$

So why study permutations in Abstract Algebra? Well, what should be obvious is that for any finite set S, we can collect together all of the possible permutations of that set into another set. Then, much less obviously, that set of permutations forms a group under function composition. Furthermore, and far more surprisingly, it turns out that every finite group is isomorphic to a group of permutations!

Theorem 6.1. *Let A be a non-empty set and S_A be the set of all permutations of A. Then, the pair $(S_A, \circ)$ forms a group, where $\circ$ is the binary operation of function composition.*

Proof.

We verify that the group axioms hold.

- Clearly composing a permutation of A with another permutation of A results in a permutation of A so S_A is closed under composition of functions.
- Composition of functions is associative.
- The permutation id of A defined such that $\mathrm{id}(a) = a$ for all $a \in A$ is the identity element. (One can easily verify that for any permutation $f \in S_A$, $f \circ \mathrm{id} = \mathrm{id} \circ f = f$.)
- Let $f \in S_A$. Then f^{-1} exists (since f is a bijection) and f^{-1} is again an element of S_A. Indeed, given $a \in A$, $f^{-1}(a)$ is the element $a' \in A$ such that $f(a') = a$. Thus we have:

$$f \circ f^{-1}(a) = f(f^{-1}(a)) = a = \mathrm{id}(a)$$

and

$$f^{-1} \circ f(a) = f^{-1}(f(a)) = a = \mathrm{id}(a).$$

Therefore, every element $f \in S_A$ has a *group theoretic inverse*, it is the usual inverse f^{-1}.

□

Definition 6.2 (Symmetric Group)**.** Let X be the finite set $\{1, 2, \ldots, n\}$. The group of all permutations of X is the *symmetric group* on n letters and is denoted S_n.

> **Note**
>
> S_n has order $n! = n \times (n-1) \times (n-2) \times \ldots \times 2 \times 1$ for all n.

6.2 Permutations as Cycles

An alternative (and more useful) notation for permutations is the one-row or *cycle* notation. Consider the set $S = \{1, 2, 3, 4, 5\}$ and the permutation of that set $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$. We can represent this as $(1\ 2\ 3\ 5\ 4)$ where 1 goes to 2, 2 goes to 3, 3 goes to 5, 5 goes to 4, and 4 goes to 1. In general, $f = (a_1\ a_2\ \ldots a_{m-1}\ a_m)$ is used to denote the permutation

$$f(a_1) = a_2,\ f(a_2) = a_3,\ \ldots, f(a_{m-1}) = a_m,\ f(a_m) = a_1.$$

Example 6.4.

Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 4 & 7 & 6 & 2 \end{pmatrix} \in S_7.$$

Then,

$$\begin{aligned} f &= (1\ 3\ 5\ 7\ 2)(4)(6) \\ &= (1\ 3\ 5\ 7\ 2) \\ &= (3\ 5\ 7\ 2\ 1) \\ &= (5\ 7\ 2\ 1\ 3) \\ &= (7\ 2\ 1\ 3\ 5) \\ &= (2\ 1\ 3\ 5\ 7) \end{aligned}$$

> **!** Important
>
> The cycle notation for a permutation is not necessarily unique!

It may seem that the single-row notation is more awkward than the two-line notation, but it does have some very useful properties that we now examine.

- A k-cycle can be written in k different ways, each with the same 'cyclic order'. For example the permutation $(1\ 3\ 5\ 7\ 2)$ in Example 6.4.
- If f is a k-cycle, then $f^k = id$ (that is, f has period k).

  For example take $f = (1\ 2\ 3) \in S_3$. Then, $f^2 = (1\ 3\ 2)$ and $f^3 = (1)(2)(3) = \mathrm{id}$.
- If $f = (a_1\ a_2\ \ldots a_k)$ is a k-cycle, then $f^{-1} = (a_k\ a_{k-1}\ \ldots\ a_2 a_1) = f^{k-1}$. (By the previous point $\mathrm{id} = ff^{-1} = ff^{k-1}$. Therefore $f^{-1} = f^{k-1}$ by cancelling.)
- A cycle of length 1 is the identity.
- Two cycles $(a_1\ a_2\ \ldots\ a_k)$ and $(b_1\ b_2\ \ldots\ b_n)$ are said to be *disjoint* if and only if $a_i \neq b_j$ for all i and j.

  For example $f = (1\ 2\ 4)$ and $g = (3\ 5\ 6)$ are *disjoint* — they have no points in common. However if we take $h = (1\ 2\ 3)$ and h and g are *not disjoint* – they have a point in

common. Notice that

$$hg = (1\ 2\ 3\ 5\ 6) \neq (1\ 2\ 5\ 6\ 3) = gh$$

however

$$fg = (1\ 2\ 4)(3\ 5\ 6) = (3\ 5\ 6)(1\ 2\ 4) = gf.$$

- Disjoint cycles commute.

  For example $(1\ 3\ 2)(4\ 6) = (4\ 6)(1\ 3\ 2)$.

6.3 Cycle Decomposition

Consider the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{pmatrix} \in S_9.$$

It should be clear that we can represent this as the 'product' of two disjoint cycles

$$f = (1\ 7\ 9\ 3)(2\ 4\ 8\ 6) = (2\ 4\ 8\ 6)(1\ 7\ 9\ 3).$$

This gives us what is called the *cycle decomposition* of f. As the cycles are disjoint, then the decomposition is commutative.

Example 6.5.

Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 6 & 1 & 9 & 10 & 2 & 7 & 3 & 12 & 5 & 4 & 11 \end{pmatrix} \in S_{12}.$$

Then

$$\begin{aligned} f &= (1\ 8\ 3)(2\ 6)(4\ 9\ 12\ 11)(5\ 10)(7) \\ &= (1\ 8\ 3)(2\ 6)(4\ 9\ 12\ 11)(5\ 10). \end{aligned}$$

Note that if we had given 'priority' to larger numbers in the above we would have obtained $(12\ 11\ 4\ 9)(10\ 5)(8\ 3\ 1)(6\ 2)$.

This looks different, but is equally valid since we know that disjoint cycles commute, so the order of disjoint cycles can be changed without affecting the product, and each cycle can be written in different ways that preserve the same cyclic order.

Example 6.6. Find the cycle decomposition of the following product of non-disjoint cycles:

$$(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5).$$

	1	2	3	4	5
$(3\ 4\ 5)$	1	2	4	5	3
$(2\ 3\ 4)$	1	3	2	5	4
$(1\ 2\ 3)$	2	1	3	5	4
	2	**1**	**3**	**5**	**4**

So,

$$(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5) = (1\ 2)(3)(4\ 5) = (1\ 2)(4\ 5).$$

Definition 6.3 (Orbits)**.** The disjoint cycles of a permutation, including singletons, are called the *orbits* of the permutation.

Example 6.7. Write the following permutations as the product of disjoint cycles and state

the number of orbits in each permutation.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 1 & 7 & 5 & 2 & 3 \end{pmatrix} \in S_7, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 5 & 4 & 2 & 3 \end{pmatrix} \in S_8.$$

Solution:

We have

$$\alpha = (1\ 4\ 7\ 3)(2\ 6)(5) = (1\ 4\ 7\ 3)(2\ 6)$$

and

$$\beta = (1\ 7\ 3)(2\ 6)(4\ 5)(8) = (1\ 7\ 3)(2\ 6)(4\ 5).$$

So α has three orbits and β has four orbits.

Example 6.8. Express the following permutation as a product of disjoint cycles.

$$\gamma = (1\ 3\ 2\ 5)(1\ 2\ 4\ 6)(3\ 6) \in S_6.$$

Solution:

	1	2	3	4	5	6
$(3\ 6)$	1	2	6	4	5	3
$(1\ 2\ 4\ 6)$	2	4	1	6	5	3
$(1\ 3\ 2\ 5)$	5	4	3	6	1	2
	5	**4**	**3**	**6**	**1**	**2**

Method 1: So

$$\gamma = (1\ 5)(2\ 4\ 6)(3) = (1\ 5)(2\ 4\ 6).$$

Method 2: We follow an element through respective cycles. For example,

$$1 \mapsto 1 \mapsto 2 \mapsto 5$$

and so, in total, $1 \mapsto 5$. Similarly, we have:

$$\begin{aligned} 2 &\mapsto 4 \\ 3 &\mapsto 3 \\ 4 &\mapsto 6 \\ 5 &\mapsto 1 \\ 6 &\mapsto 2. \end{aligned}$$

So $\gamma = (1\ 5)(2\ 4\ 6)$.

Example 6.9. Express the following permutation as a product of disjoint cycles.

$$\delta = (1\ 4\ 2)(2\ 3\ 5)(1\ 3\ 4) \in S_5$$

Applying method 2 as above, we have:

$$\delta = (1\ 5)(2\ 3)(4) = (1\ 5)(2\ 3).$$

6.4 Periods of Permutations

Consider the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 10 & 2 & 8 & 9 & 4 & 6 & 5 & 1 \end{pmatrix} \in S_{10}$. How do we calculate the period of α in S_{10}? Note, first, the following:

$$\begin{aligned} \alpha &= (1\ 3\ 10)\ (2\ 7\ 4)\ (5\ 8\ 6\ 9) \\ \text{so}\quad \alpha^2 &= (1\ 3\ 10)\ (2\ 7\ 4)\ (5\ 8\ 6\ 9)\ (1\ 3\ 10)\ (2\ 7\ 4)\ (5\ 8\ 6\ 9) \\ &= (1\ 3\ 10)(1\ 3\ 10)\ (2\ 7\ 4)(2\ 7\ 4)\ (5\ 8\ 6\ 9)(5\ 8\ 6\ 9) \\ &= (1\ 3\ 10)^2\ (2\ 7\ 4)^2\ (5\ 8\ 6\ 9)^2 \end{aligned}$$

since disjoint cycles commute. Note, also, that a k-cycle has period k. For example:

$$\begin{aligned} f &= (a\ b\ c\ d) \\ f^2 &= (a\ c)(b\ d) \\ f^3 &= (a\ d\ c\ b) \\ f^4 &= (a)(b)(c)(d) = id. \end{aligned}$$

We can now compute the period of α as follows:

$$
\begin{array}{rcccccccc}
\alpha & = & (1\,3\,10) & (2\,7\,4) & (5\,8\,6\,9) & = & (1\,3\,10) & (2\,7\,4) & (5\,8\,6\,9) \\
\alpha^2 & = & (1\,10\,3) & (2\,4\,7) & (5\,6)(8\,9) & = & (1\,10\,3) & (2\,4\,7) & (5\,6)(8\,9) \\
\alpha^3 & = & (1)(10)(3) & (2)(4)(7) & (5\,9\,6\,8) & = & id & id & (5\,9\,6\,8) \\
\alpha^4 & = & (1\,3\,10) & (2\,7\,4) & (5)(6)(8)(9) & = & (1\,3\,10) & (2\,7\,4) & id \\
\alpha^5 & = & (1\,10\,3) & (2\,4\,7) & (5\,8\,6\,9) & = & (1\,10\,3) & (2\,4\,7) & (5\,8\,6\,9) \\
\alpha^6 & = & (1)(10)(3) & (2)(4)(7) & (5\,6)(8\,9) & = & id & id & (5\,6)(8\,9) \\
\alpha^7 & = & (1\,3\,10) & (2\,7\,4) & (5\,9\,6\,8) & = & (1\,3\,10) & (2\,7\,4) & (5\,9\,6\,8) \\
\alpha^8 & = & (1\,10\,3) & (2\,4\,7) & (5)(6)(8)(9) & = & (1\,10\,3) & (2\,4\,7) & id \\
\alpha^9 & = & (1)(10)(3) & (2)(4)(7) & (5\,8\,6\,9) & = & id & id & (5\,8\,6\,9) \\
\alpha^{10} & = & (1\,3\,10) & (2\,7\,4) & (5\,6)(8\,9) & = & (1\,3\,10) & (2\,7\,4) & (5\,6)(8\,9) \\
\alpha^{11} & = & (1\,10\,3) & (2\,4\,7) & (5\,9\,6\,8) & = & (1\,10\,3) & (2\,4\,7) & (5\,9\,6\,8) \\
\alpha^{12} & = & (1)(10)(3) & (2)(4)(7) & (5)(6)(8)(9) & = & id & id & id.
\end{array}
$$

So, the period of the permutation is 12. It should be clear, from this example, that the period of a permutation can be determined by finding the lowest common multiple of the lengths of its orbits. In this example we have that the period of α is lcm(3, 3, 4) = 12.

6.5 Permutations as Transpositions

We begin with a definition.

Definition 6.4 (Transposition)**.** A cycle $(i\ j)$ of length two interchanges, or transposes, i and j and is called a *transposition*.

The importance of transpositions is that *any* cycle may be expressed as a product of transpositions. Suppose we wish to arrange ♠ ♡ ♢ ♣ as ♣ ♠ ♡ ♢ using only transpositions (that is, swapping symbols two at a time). This corresponds to expressing the permutation $(1\ 2\ 3\ 4)$ as a product of transpositions. One way to do this is as follows:

	1	2	3	4
	♠	♡	♢	♣
apply $(3\ 4)$:	♠	♡	♣	♢
apply $(2\ 3)$:	♠	♣	♡	♢
apply $(1\ 2)$:	♣	♠	♡	♢

Thus we have that

$$(1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4).$$

Recalling that this is function composition and, therefore, we start at the right-hand end of the product, we can state the following general formula:

$$(a_1\ a_2\ a_3\ \ldots\ a_{k-1}\ a_k) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}\ a_k).$$

We could use an alternative approach as follows:

	1	2	3	4
	♠	♡	♢	♣
apply $(1\ 2)$:	♡	♠	♢	♣
apply $(1\ 3)$:	♢	♠	♡	♣
apply $(1\ 4)$:	♣	♠	♡	♢

Thus we have that

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2).$$

This illustrates an alternative general formula:

$$(a_1\ a_2\ a_3\ \ldots\ a_{k-1}\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\ldots(a_1\ a_2).$$

Example 6.10. Express the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 9 & 7 & 1 & 5 & 10 & 8 & 3 & 4 & 6 \end{pmatrix}$ as a product of transpositions.

Solution:

First we express f as a product of disjoint cycles:

$$f = (1\ 2\ 9\ 4)(3\ 7\ 8)(6\ 10).$$

Using the first rule:

$$f = (1\ 2)(2\ 9)(9\ 4)(3\ 7)(7\ 8)(6\ 10).$$

Using the second rule:

$$(1\ 4)(1\ 9)(1\ 2)(3\ 8)(3\ 7)(6\ 10).$$

> **Note**
>
> We write the identity permutation as a product of transpositions as follows:
>
> $$(1\ 2)(1\ 2) = \text{id}$$

It is clear from what we have seen that the expression of a permutation as a product of transpositions is not unique. However, there is one feature of the composition that is constant and we shall now explore this. First, though, we consider the following example.

Example 6.11. Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 6 & 1 & 9 & 5 & 2 & 7 & 3 & 12 & 10 & 4 & 11 \end{pmatrix} \in S_{12}$. We can write this as the product of disjoint cycles:

$$f = (1\ 8\ 3)(2\ 6)(4\ 9\ 12\ 11) \in S_{12}$$

notice that f has 5 orbits.

We now consider what happens if we 'pre-multiply' this permutation by a transposition $(i\ j)$.

We need to consider two cases:

a. Let i and j be from different orbits

   For example we could take $i = 1$ and $j = 2$. Then

$$(1\ 2)f = (1\ 8\ 3\ 2\ 6)(4\ 9\ 12\ 11).$$

   The number of orbits of f is now 5 — the effect is to merge the orbits containing 1 and 2.

b. Let i and j be from the same orbit

   For example we can take $i = 1$ and $j = 3$. Then

$$(1\ 3)f = (1\ 8)(3)(2\ 6)(4\ 9\ 12\ 11).$$

   The effect is to split the orbit containing 1 and 3 into two distinct orbits. Notice that the number of orbits of $(i\ j)f$ and f in each case differ by 1.

Strictly, we ought also to consider whether or not it matters if i or j come from an orbit of size 1.

For example, we could consider $i = 1$ and $j = 5$.Then

$$(1\ 5)f = (1\ 8\ 3\ 5)(2\ 6)(4\ 9\ 12\ 11).$$

Or $i = 5$ and $j = 7$, then

$$(5\ 7)f = (5\ 7)(1\ 8\ 3)(2\ 6)(4\ 9\ 12\ 11).$$

Example 6.12. Consider the permutation $f = (1\ 7\ 9\ 3)(2\ 4\ 8\ 6) \in S_9$. Pre-multiply f by a transposition $(i\ j)$ (and note the effect this has on the orbits of f) where

i. i and j come from the same orbit of f, e.g. $(i\ j) = (4\ 8)$.

$$(4\ 8)f = (1\ 7\ 9\ 3)(2\ 8\ 6)(4) = (1\ 7\ 9\ 3)(2\ 8\ 6).$$

Notice that f has 3 orbits and $(4\ 8)f$ has 4 obits.

ii. i and j come from different orbits of f, e.g. $(i\ j) = (7\ 2)$.

$$(7\ 2)f = (1\ 2\ 4\ 8\ 6\ 7\ 9\ 3).$$

In this case $(7\ 2)f$ has 2 orbits — one less than f.

Lemma 6.1. *Let $f \in S_n$, $(n \geq 2)$, and $(i\ j)$ be a transposition in S_n. Then the number of orbits of f and $(i\ j)f$ differ by 1.*

Proof. We first express f as a product of disjoint cycles, $c_1, c_2, \ldots, c_r$ and consider two cases.

Case 1: i and j are from distinct orbits of f.

Without loss of generality, we may assume that i and j come from c_1 and c_2 respectively. Suppose $c_1 = (x_1\ x_2\ x_3\ \ldots\ x_a)$ and $c_2 = (y_1\ y_2\ \ldots\ y_b)$. We may assume, again without loss of generality that that $i = x_1$ and $j = y_1$. Now consider:

$$\begin{aligned}(i\ j)f &= (x_1\ y_1)(x_1\ x_2\ x_3\ \ldots\ x_a)(y_1\ y_2\ \ldots\ y_b)c_3 \ldots c_r \\ &= (x_1\ x_2 \ldots\ x_a\ y_1\ y_2 \ldots y_b)c_3 \ldots c_r.\end{aligned}$$

It follows that $(i\ j)f$ has one fewer orbit than f,

Case 2: i and j are from the same orbit of f.

We may assume without loss of generality that i and j come from c_1. Let $c_1 = (x_1\ x_2\ \ldots\ x_a)$. We may assume that $i = x_1$ and $j = x_d$ for $1 < d \leq a$ so that

$$c_1 = (i = x_1\ x_2\ \ldots\ x_d\ \ldots\ x_a).$$

Then

$$\begin{aligned}(x_1\ x_d)f &= (x_1\ x_d)(x_1\ x_2\ \ldots\ x_d\ \ldots\ x_a)c_2\ldots c_r\\ &= (x_1\ x_2\ \ldots\ x_{d-1})(x_d\ x_{d+1}\ \ldots\ x_a)c_2\ldots c_r.\end{aligned}$$

We see that c_1 is split into two disjoint cycles — the number of orbits of $(1\ j)f$ is one more than f.

□

Theorem 6.2. *No permutation can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.*

Proof.

First we make the following observation. Let $\tau_1, \tau_2, \ldots \tau_r$ be transpositions. Let m be the number of orbits of $\tau_1 \ldots \tau_r\,\mathrm{id}$. By Lemma 6.1, if r is even, m and n have the same parity (that is they are either both even or both odd) and if r is odd, then m and n have different parities (one is even and the other is odd). This is easily seen since Lemma 6.1 says each time we multiply a permutation by a transposition we change the parity of the number of its orbit and the identity element has n orbits.

Now let f be a permutation. Suppose there are transpositions $c_1, c_2 \ldots, c_r, d_1, d_2, \ldots d_s$ such that f can be expressed as

$$f = c_1c_2\ldots c_r = d_1d_2\ldots d_s.$$

Rearranging, it follows that

$$d_sd_{s-1}\ldots d_1c_rc_{r-1}\ldots c_1 = \mathrm{id}$$

and so

$$d_sd_{s-1}\ldots d_1c_rc_{r-1}\ldots c_1\,\mathrm{id} = \mathrm{id}\,.$$

By our observation above, we must conclude that if $r + s$ must be even. Since $d_s d_{s-1} \dots d_1 c_r c_{r-1} \dots c_1 \,\mathrm{id}$ has n orbits.

□

Definition 6.5 (Parity)**.** A permutation is *even* or *odd* according to whether it can be expressed as a product of an even number of transpositions or as an odd number of transpositions, respectively.

Example 6.13.

The identity permutation $\mathrm{id} \in S_n$ is an even permutation. This follows since $\mathrm{id} = (i\ j)(i\ j)$.

Theorem 6.3. *The number of even permutations in S_n is the same as the number of odd permutations in S_n.*

Proof.

Let A_n be the set of even permutations in S_n. Notice that $S_n \backslash \{A_n\}$ is the set of odd permutations in S_n. Let τ be any transposition in S_n. Define a map $\theta : A_n \to S_n \backslash A_n$ by $\theta(f) = \tau f$. Notice that by Lemma 6.1, for $f \in A_n$ $\tau f \in S_n \backslash A_n$ and so θ indeed maps elements of A_n into the set $S_n \backslash A_n$. We show that θ is injective and surjective.

Injective: Let $f_1, f_2 \in A_n$ and suppose $\theta(f_1) = \theta(f_2)$. This means that $\tau f_1 = \tau f_2$, cancelling then yields that $f_1 = f_2$.

Surjective: Let $g \in S_n \backslash A_n$. Then $\tau g \in A_n$ by Lemma 6.1 again. Moreover,

$$\theta(\tau g) = \tau(\tau g) = (\tau\tau)g = g.$$

Therefore θ is surjective.

The map θ is therefore a bijection and so the number of even permutations in S_n must be the same as the number of odd permutations in S_n.

□

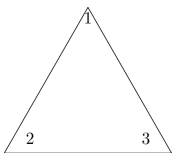
Since the product of two even permutations is even, and the identity permutation is even, we have, by Lemma 3.5, that the set of all even permutations of degree n forms a subgroup of S_n called the *alternating group of degree* n and denoted A_n. Both S_n and A_n are very important groups and you will encounter them again if you take the third-year optional module Group Theory. At present it is sufficient to note that A_4 (which has order 12 - think about it) is isomorphic to the group of rotational symmetries of a regular tetrahedron, which provided us with the smallest counterexample to the converse of Lagrange's Theorem.

6.6 Cayley's Theorem

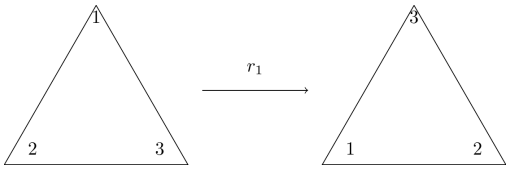
Consider the following examples.

Example 6.14. Notice that S_1 has only one element. So, $S_1 \cong \mathbb{Z}_1$ as there is only one group of order 1 (the trivial group containing only the identity). S_2 has 2!=2 elements, so $S_2 \cong \mathbb{Z}_2$ as there is only one group of order 2. What about S_3? This has 3!=6 elements, but there are two isomorphically distinct groups of order 6, namely $\mathbb{Z}_6$ and D_3. It is easy to see that S_3 is non-abelian so S_3 has to be isomorphic to D_3. However, a more direct and satisfying approach is as follows:

Consider, as below, an equilateral triangle with vertices labelled with the numbers 1, 2 and 3 anticlockwise:



Each symmetry of the triangle induces a permutation of the vertices $\{1, 2, 3\}$. For example the symmetry r_1 (see Example 2.1) has the effect:



Thus we have

$$r_1 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Similarly we have,

$$\begin{aligned} e &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \\ r_2 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ s_1 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ s_2 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ s_3 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{aligned}$$

This gives an isomorphism from D_3 to S_3. Clearly we have a bijection from D_3 to S_3 and it is easily verified that this bijection is also a homomorphism. For example, $r_1 \circ s_1 = s_3$ and

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Notice that a similar argument demonstrates that every dihedral group can be represented as a group of permutations. However, the example above is special — *it is the only example where a dihedral group is isomorphism to a full symmetric group*. When $n > 3$, the dihedral group D_n is isomorphic to a **subgroup** of the symmetric group.

It turns out, in fact, that every finite group is isomorphic to a subgroup of some symmetric

group. Formally, if $|G| = n$ then G is isomorphic to some subgroup of S_n. This is what is known as Cayley's Theorem and we prove this and study it in more detail in third-year Group Theory.

Theorem 6.4 (Cayley's Theorem)**.** *Every finite group is isomorphic to a group of permutations.*

Proof. Omitted. □

We finish this chapter with an interesting example: A 'riffle' shuffle consists of splitting a pack of cards in equal halves and then interlacing the cards from each half. In a perfect riffle a deck of 52 cards, numbered from 1 to 52 from the bottom up, would result in a deck with the cards numbered 1, 27, 2, 28, ... from the bottom up. How many perfect riffle shuffles are required before a deck returns to its original position? Does it matter if the halves are interlaced so that after one shuffle the order of the cards is 27, 1, 28, 2, ... ?

Solution:

We consider this as a simple permutation. Let the cards be numbered sequentially from 1 to 52, starting with 1 at the bottom of the pack; thus the card number, at this stage, will correspond to its position in the pack. Let the top row be the starting position and let the bottom row be the position that the respective card occupies after one perfect riffle:

$$f = \begin{pmatrix} 1 & 27 & 2 & 28 & 3 & 29 & 4 & 30 & 5 & 31 & 6 & 32 & 7 & 33 & 8 & 34 & 9 & 35 & 10 & 36 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \end{pmatrix}$$

$$\begin{pmatrix} 11 & 37 & 12 & 38 & 13 & 39 & 14 & 40 & 15 & 41 & 16 & 42 & 17 & 43 & 18 & 44 & 19 & 45 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 \end{pmatrix}$$

$$\begin{pmatrix} 20 & 46 & 21 & 47 & 22 & 48 & 23 & 49 & 24 & 50 & 25 & 51 & 26 & 52 \\ 39 & 40 & 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 & 51 & 52 \end{pmatrix}.$$

Now re-order so that the top row is sequential starting at 1 (our usual, two-row permutation representation).

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 & 17 & 19 & 21 & 23 & 25 & 27 & 29 & 31 & 33 & 35 & 37 & 39 \end{pmatrix}$$

$$\begin{matrix} 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 \\ 41 & 43 & 45 & 47 & 49 & 51 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 20 & 22 & 24 & 26 \end{matrix}$$

$$\begin{matrix} 40 & 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 & 51 & 52 \\ 28 & 30 & 32 & 34 & 36 & 38 & 40 & 42 & 44 & 46 & 48 & 50 & 52 \end{matrix} \Bigg).$$

Then, using the usual method of writing a permutation as a product of disjoint cycles, we have that

$$\begin{aligned} f &= (2\ 3\ 5\ 9\ 17\ 33\ 14\ 27)(4\ 7\ 13\ 25\ 49\ 46\ 40\ 28)(6\ 11\ 21\ 41\ 30\ 8\ 15\ 29) \\ &\quad (10\ 19\ 37\ 22\ 43\ 34\ 16\ 31)(12\ 23\ 45\ 38\ 24\ 47\ 42\ 32)(18\ 35) \\ &\quad (20\ 39\ 26\ 51\ 50\ 48\ 44\ 36). \end{aligned}$$

Hence, the period of f is lcm(8, 8, 8, 8, 8, 2, 8) = 8.

Using the same method to investigate the other arrangement following the first riffle:

$$f = \begin{pmatrix} 27 & 1 & 28 & 2 & 29 & 3 & 30 & 4 & 31 & 5 & 32 & 6 & 33 & 7 & 34 & 8 & 35 & 9 & 36 & 10 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \end{pmatrix}$$

$$\begin{matrix} 37 & 11 & 38 & 12 & 39 & 13 & 40 & 14 & 41 & 15 & 42 & 16 & 43 & 17 & 44 & 18 & 45 & 19 & 46 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 \end{matrix}$$

$$\begin{array}{cccccccccccccc} 20 & 47 & 21 & 48 & 22 & 49 & 23 & 50 & 24 & 51 & 25 & 52 & 26 \\ 40 & 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 & 51 & 52 \end{array}\Bigg).$$

Now re-order so that the top row is sequential starting at 1.

$$f = \Bigg(\begin{array}{cccccccccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 20 & 22 & 24 & 26 & 28 & 30 & 32 & 34 & 36 & 38 & 40 \end{array}$$

$$\begin{array}{cccccccccccccccccccc} 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 \\ 42 & 44 & 46 & 48 & 50 & 52 & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 & 17 & 19 & 21 & 23 & 25 \end{array}$$

$$\begin{array}{cccccccccccccc} 40 & 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 & 51 & 52 \\ 27 & 29 & 31 & 33 & 35 & 37 & 39 & 41 & 43 & 45 & 47 & 49 & 51 \end{array}\Bigg).$$

Then, using the usual method of writing a permutation as a product of disjoint cycles, we have that

$$\begin{aligned} f &= (1\ 2\ 4\ 8\ 16\ 32\ 11\ 22\ 44\ 35\ 17\ 34\ 15\ 30\ 7\ 14\ 28\ 3\ 6\ 12\ 24\ 48\ 43\ 33\ 13\ 26\ 52\ 51\ 49\ 45 \\ &\quad 37\ 21\ 42\ 31\ 9\ 18\ 36\ 19\ 38\ 23\ 46\ 39\ 25\ 50\ 47\ 41\ 29\ 5\ 10\ 20\ 40\ 27). \end{aligned}$$

Hence, the period of f is now 52.

6.7 Problem Sheet 6

For Week 8; covers Chapter 6.

Question 6.1

Let $(G_1, \circ)$ and $(G_2, *)$ be groups and $\theta : G_1 \to G_2$ be an injective homomorphism. For each of the following statements, either prove that it is true or provide a counter-example:

a. If $(G_1, \circ)$ is abelian, then $(G_2, *)$ is abelian.

b. If $(G_2, *)$ is abelian, then $(G_1, \circ)$ abelian.

Beware spurious 'proofs'!

Show Solution 6.1 on P210

Question 6.2

Recall that the kernel of the homomorphism is a subgroup of the domain. Recall, also, that we said in lectures that the size of the image of a homomorphism equals the size of the domain divided by the size of its kernel. That, of course, related to examples where both the domain and the image were finite. What happens if we now consider examples where infinity plays a part? So, investigate the kernels of the following homomorphisms in light of the above relationship:

a. $\theta : (\mathbb{Z}, +) \to \mathbb{Z}_n$ defined by $\forall a \in \mathbb{Z},\ \theta(a) = a \pmod{n}$,

b. $\phi : GL(2, \mathbb{R}) \to \mathbb{R}\backslash\{0\}$ defined by $\forall A \in GL(2, \mathbb{R}),\ \phi(A) = |A|$.

Show Solution 6.2 on P211

Question 6.3

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$. Calculate $g \circ f$, $f \circ g$, f^2, and g^2.

Show Solution 6.3 on P213

Question 6.4

For each of the following permutations

- write the permutation as a product of disjoint cycles,
- state the number of orbits of the permutation,
- find the inverse permutation,
- write the permutation as a product of transpositions in two different ways,
- state whether the permutation is even or odd,
- find the period of the permutation.

a. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 12 & 8 & 6 & 9 & 11 & 3 & 1 & 2 & 10 & 4 & 5 \end{pmatrix} \in S_{12}$.

b. $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 12 & 10 & 9 & 3 & 11 & 7 & 5 & 1 & 8 & 4 & 2 \end{pmatrix} \in S_{12}$.

c. $\gamma = (1\ 3\ 8\ 5)(2\ 9\ 3)(1\ 4\ 3\ 7)(4\ 5\ 8\ 9) \in S_9$.

d. $\delta = (1\ 5\ 3\ 6)(6\ 3\ 2\ 1)(1\ 2\ 5)(3\ 5\ 7\ 1)(4\ 6\ 1\ 5) \in S_8$.

e. $\epsilon = (1\ 3\ 4)(3\ 2\ 1)(4\ 3\ 1)(5\ 4\ 3)(2\ 5\ 1) \in S_5$.

Show Solution 6.4 on P215

Question 6.5

Find the maximum period of a permutation in S_{15} and give an example of such a permutation.

Show Solution 6.5 on P218

Chapter 7

The Structure of Finite Abelian Groups

In this chapter it will be our aim to give a complete description of finite abelian groups in the sense that, for any given n, we will be able to describe all of the abelian groups of order n up to isomorphism. In other words, we are aiming for a theorem that will give us complete structural information about all finite abelian groups. This is a staggeringly long way from the humble beginnings of a set, a binary operation, and four simple axioms!

7.1 Structure of Cyclic Groups

We start by considering the structure of cyclic groups and, in particular, by proving that all cyclic groups are abelian. Recall that a group G is cyclic if and only if it contains at least one element a such that $G = \langle a \rangle = \{a^i : i \in \mathbb{Z}\}$.

Theorem 7.1. *Every cyclic group is abelian.*

Proof.

Let G be a cyclic group and $a \in G$ be a generator. Let $x, y \in G$. There are $i, j \in \mathbb{Z}$ such

that $x = a^i$ and $y = a^j$. Therefore:

$$xy = a^i a^j = a^{i+j} = a^{j+i} = a^j a^i = yx.$$

It follows that G is abelian.

□

> **Note**
>
> This says that if a group is cyclic, then it must be abelian. The converse is not necessarily true; an abelian group does not have to be cyclic.

The following theorem tells us that there is, essentially, only one cyclic group of any given order. This is an extension of Theorem 5.1 which said that two cyclic groups of the same order are isomorphic.

Theorem 7.2. *Let G be a cyclic group with generator a. Then,*

i. if G is infinite, $G \cong (\mathbb{Z}, +)$;

ii. if G is finite and of order n, then $G \cong \mathbb{Z}_n$.

Proof.

Let $a \in G$ be a generator for G.

(i) Define a map $\theta : G \to \mathbb{Z}$ by $\theta(a^i) = i$. We note firstly that θ is well-defined, since all the integer powers of a are distinct as a has infinite order. Clearly θ is bijective. It remains to see that θ is a homomorphism. Let $i, j \in \mathbb{Z}$, then

$$\begin{aligned} \theta(a^i a^j) &= \theta(a^{i+j}) \\ &= i + j \\ &= \theta(a^i) + \theta(a^j). \end{aligned}$$

It follows that θ is a bijective homomorphism and so θ is an isomorphism.

(ii) We note that the order of a is also n. In particular, $a^0, a^1, \ldots, a^{n-1}$ are the distinct elements of G. Define a map $\theta : G \to \mathbb{Z}_n$ by $\theta(a^i) = i$ for all $0 \leq i \leq n-1$. Then θ is a bijection. It remains to see that θ is a homomorphism: let $a^i, a^j \in G$, $0 \leq i, j \leq n-1$, then

$$\begin{aligned} \theta(a^i a^j) &= \theta(a^{i \oplus_n j}) \\ &= i \oplus_n j \\ &= \theta(a^i) \oplus_n \theta(a^j). \end{aligned}$$

It follows that θ is a homomorphism and so an isomorphism.

□

Recall that in Chapter 4 we proved, by a simple application of Lagrange's Theorem, that every group of prime order is cyclic. We may now conclude that *every group of order a prime, p, is isomorphic to $\mathbb{Z}_p$*. Thus we now have a complete classification for groups of prime order. We now need to extend this to abelian groups of any given order. We begin with the following theorem.

Theorem 7.3. *Any subgroup of a cyclic group is also cyclic.*

Proof.

Let G be a cyclic group with generator a. Let H be a subgroup of G. If H is the trivial subgroup $\{e\}$, then clearly H is cyclic generated by e. Therefore we may assume that H is not the trivial subgroup.

Let $i \in \mathbb{Z}$, $i > 0$ be minimal such that $a^i \in H$. (We note that i exists since H is not trivial.) Let $x \in H$ be any other element. There is a $j \in \mathbb{Z}$ such that $x = a^j$. There are $q, r \in \mathbb{Z}$ such that $j = qi + r$ where $0 \leq r < i$. Notice $a^r = a^j a^{-qi} \in H$, as H is closed under products,

$a^j \in H$ and $a^{-qi} = (a^{-i})^q \in H$. However as $r < i$, it must follows that $r = 0$ (since $i > 0$ is minimal such that $a^i \in H$). We conclude that $a^j a^{-qi} = e$ and so $a^j = (a^i)^q$.

It follows that every element of H is a power of a^i and H is cyclic and generated by a^i.

□

Theorem 7.4. *Let G be a cyclic group of order n with generator a, and let $1 \leq m < n$. Then $\langle a^m \rangle = \langle a^d \rangle$ where d is the greatest common divisor of m and n.*

Proof.

It is clear that $\langle a^m \rangle \subseteq \left\langle a^d \right\rangle$ since $m = ld$ for some $l \in \mathbb{Z}$ and so $a^m = (a^d)^l$.

Since $d = \gcd(m, n)$ there are $u, v \in \mathbb{Z}$ such that $d = um + vn$. It follows that

$$a^d = a^{um+vn} = a^{um} a^{vn} = (a^m)^u (a^n)^v = a^{mu}.$$

Therefore $a^d \in \langle a^m \rangle$.

We conclude that $\left\langle a^d \right\rangle = \langle a^m \rangle$.

□

Example 7.1. Consider the cyclic subgroups of $\mathbb{Z}_{12}$.

The distinct divisors of 12 are $1, 2, 3, 4, 5, 6, 12$. So the subgroups of $\mathbb{Z}_{12}$ are

$$\begin{aligned}
\langle 1 \rangle &= \mathbb{Z}_{12} = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle \\
\langle 2 \rangle &= \{0, 2, 4, 6, 8, 10\} = \langle 10 \rangle \\
\langle 3 \rangle &= \{0, 3, 6, 9\} = \langle 9 \rangle \\
\langle 4 \rangle &= \{0, 4, 8\} = \langle 8 \rangle \\
\langle 6 \rangle &= \{0, 6\} \\
\langle 12 \rangle &= \{0\}.
\end{aligned}$$

Example 7.2. What are the elements of $\langle 28 \rangle$ in $\mathbb{Z}_{38}$.

Notice that $28 = 2^2 \times 7$ and $38 = 2 \times 19$. It follows that $\gcd(38, 28) = 2$. Therefore $\langle 28 \rangle = \langle 2 \rangle$. It follows that the elements of $\langle 28 \rangle$ are

$$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36\}.$$

Corollary 7.1. *If a is a generator of a cyclic group G of order n, then the other generators of G are the elements of the form a^r where r is relatively prime to n.*

Example 7.3.

(a) Write down all of the generators of $\mathbb{Z}_{15}$.

The generators are the elements of $\mathbb{Z}_{15}$ co-prime to 15, these are 1, 2, 4, 7, 8, 11, 13 and 14.

(b) Write down all of the generators of $\mathbb{Z}_{24}$.

They are 1, 5, 7, 11, 13, 17, 19, 23.

Lemma 7.1. *Let $a \in \mathbb{Z}_n$. Then the period of a in $\mathbb{Z}_n$ can be found by dividing n by the $\gcd(a, n)$.*

Proof. Let $a \in \mathbb{Z}_n$ and $d = \gcd(a, n)$.

First observe that $\langle a \rangle = \langle d \rangle$ and so a and d have the same period in $\mathbb{Z}_n$ by Theorem 3.2. It therefore suffices to show that the period of d in $\mathbb{Z}_d$ is $\frac{n}{d}$.

Clearly $d\frac{n}{d} = n \equiv 0 \pmod{n}$. Therefore the period of $d \in \mathbb{Z}_n$ is at most $\frac{n}{d}$. However for any $q \in \mathbb{Z}$ with $0 \leq q < \frac{n}{d}$, $qd < n$ and so $qd \not\equiv 0 \pmod{n-1}$. We conclude that the period of $d \in \mathbb{Z}_n$ is precisely $\frac{n}{d}$. Thus, the period of $a \in \mathbb{Z}_n$ is also $\frac{n}{d}$ as required. □

7.2 Direct Products of Groups

In this section we demonstrate how we can use familiar groups as building blocks to construct larger groups. Recall that the Cartesian product of two sets, S and T say, is the set, denoted $S \times T$, consisting of all possible ordered pairs of elements where the first element of the pair comes from S and the second element comes from T. We can extend this idea to any finite number of sets so, for example, we can take the product of three sets, A, B and C, say, and then $A \times B \times C$ will consist of ordered triples with the first element from A, the second from B and the third from C. So, for example, $(3, 2, 4) \in \mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7$.

Definition 7.1 (Cartesian Product of Sets)**.** Let $S_1, S_2, \ldots, S_n$ be sets. Then the *Cartesian product* of these sets is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in S_i$ for $i = 1, 2, \ldots, n$. We denote the Cartesian product

$$S_1 \times S_2 \times \ldots \times S_n.$$

We now let $G_1, G_2, \ldots, G_n$ be groups (not necessarily distinct, nor abelian). We can form the Cartesian product of the sets of elements of these groups and then form a group by defining '*multiplication component-wise*'. Consider, for example, $\mathbb{Z}_2 \times \mathbb{Z}_2$. Its elements are $(0,0), (0,1), (1,0), (1,1)$ and the binary operation is addition modulo 2 (this is what is meant by multiplication component-wise in this case). We can then construct the operation table as follows:

$\oplus_2$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

It is clear that $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus_2)$ forms a group. It is an abelian group (this is clear from the multiplication table) but it is now cyclic — it has no element of order 4.

Theorem 7.5. *Let $G_1, G_2, \ldots, G_n$ be groups. For $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ in $G_1 \times G_2 \times \ldots \times G_n$ we define*

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Then $G_1 \times G_2 \times \ldots \times G_n$ forms a group, called the direct product of the groups G_i *under this binary operation.*

Proof.

We verify the group axioms hold.

- Since $G_1, G_2, \ldots G_n$ are groups, the binary operation on $G_1 \times G_2 \times \ldots \times G_n$ is closed.
- Let $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n), (c_1, c_2, \ldots, c_n) \in G_2 \times G_2 \times \ldots \times G_n$. Then

$$\begin{aligned}
&((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n))\,(c_1, c_2, \ldots, c_n) = \\
&(a_1 b_1, a_2 b_2, \ldots, a_n b_n)(c_1, c_2, \ldots, c_n) = \\
&((a_1 b_2)c_1, (a_2 b_2)c_2, \ldots, (a_n b_n)c_n) = \\
&(a_1(b_2 c_1), a_2(b_2 c_2), \ldots, a_n(b_n c_n)) = \\
&(a_1, a_2, \ldots, a_n)\,(b_1 c_1, b_2 c_2, \ldots, b_n c_n) = \\
&(a_1, a_2, \ldots, a_n)\,((b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n))\,.
\end{aligned}$$

The binary operation is associative.

- Let e_i be the identity element of G_i for all $1 \leq i \leq n$. Then $(e_1, e_2, \ldots, e_n)$ is the identity element of $G_1 \times G_2 \times \ldots \times G_n$.
- Let $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \ldots \times G_n$, then $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}) \in G_1 \times G_2 \times \ldots \times G_n$.

□

Example 7.4.

Let $G_1 = \mathbb{Z}_2$ and $G_2 = D_3$. Then $G_1 \times G_2 = \mathbb{Z}_2 \times D_3$ has order 12 and its elements are:

$$(0, e), (0, r_1), (0, r_2), (0, s_1), (0, s_2), (0, s_3)$$
$$(1, e), (1, r_1), (1, r_2), (1, s_1), (1, s_2), (1, s_3).$$

We compute products component wise. For example:

$$\begin{aligned} (1, r_1)(0, s_2) &= (1 + 0, r_1 \circ s_2) = (1, s_1) \\ (0, s_2)(1, r_1) &= (0 + 1, s_2 \circ r_1) = (1, s_3). \end{aligned}$$

Notice that the group is not abelian (precisely because D_3 is not abelian.)

Lastly, observe that

$$\{(x, e) : x \in \mathbb{Z}_2\} = \{(0, e), (1, e)\}$$

is a subgroup of $\mathbb{Z}_2 \times D_3$ isomorphic to $\mathbb{Z}_2$. Similarly,

$$\{(0, y) : y \in D_3\} = \{(0, e), (0, r_1), (0, r_2), (0, s_1), (0, s_2), (0, s_3)\}$$

is a subgroup of $\mathbb{Z}_2 \times D_3$ isomorphic to D_3.

Reminder

Let m and n be integers. Recall that the largest positive integer that divides both m and n is known as the *greatest common divisor* of m and n and is denoted $\gcd(m, n)$. For example, $\gcd(12, 15) = 3$. We shall be particularly interested in cases where the greatest common divisor of two integers is 1. In this case we refer to the integers as being *relatively prime*. It is important to note that even if two integers are relatively prime, neither of them needs to be prime; for example, $\gcd(8, 9) = 1$, so 8 and 9 are relatively prime, though neither is a prime number. Recall, also, that the *lowest common multiple* of two integers m and n is the smallest positive integer that is divisible by both m and n. This is denoted $\text{lcm}(m, n)$. Now, let $m, n \in \mathbb{Z}$. Then $mn = \gcd(m, n) \times \text{lcm}(m, n)$.

$$e.g. \qquad \gcd(6, 9) = 3, \qquad \text{lcm}(6, 9) = 18 \qquad \text{and} \qquad 6 \times 9 = 3 \times 18 = 54.$$

So $\text{lcm}(m, n) = mn$ if and only if $\gcd(m, n) = 1$ if and only if m and n are relatively prime.

Lemma 7.2. *Let $(a_1, a_2) \in G_1 \times G_2$. If a_i is of finite period r_i in G_i then the period of (a_1, a_2) in $G_1 \times G_2$ is equal to the lowest common multiple of r_1 and r_2.*

Proof.

Let $l = \text{lcm}(r_1, r_2)$. Then there are $s_1, s_2 \in \mathbb{N}$ such that $r_1 s_1 = l$ and $r_2 s_2 = l$. It follows that

$$(a_1, a_2)^l = \left(a_1^l, a_2^l\right) = (a_1^{r_1 s_1}, a_2^{r_2 s_2}) = (e_1, e_2)$$

where e_i is the identity element of G_i $(i = 1, 2)$.

Now let m be a positive integer such that $(a_1, a_2)^m = (e_1, e_2)$. Then $a_1^m = e_1$ and $a_2^m = e_2$. It follows that r_1 and r_2 both divide m. Consequently, l divides m as well. Therefore l is the period of (a_1, a_2).

□

Example 7.5. In the following cases, find the period of the given element of the direct product group.

(a) $(3, 7)$ in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{21}$.

The period of 3 in $\mathbb{Z}_{12}$ is 4 and the period of 7 in $\mathbb{Z}_{21}$ is 3. It follows that $(3, 7)$ has period 12 in $\mathbb{Z}_{12} \times \mathbb{Z}_{21}$.

(b) $(8, 4, 10)$ in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

Observe that 8 has period $3 = \frac{12}{\gcd(8,12)}$ in $\mathbb{Z}_{12}$, 4 has period $15 = \frac{60}{\gcd(60,4)}$ in $\mathbb{Z}_{60}$ and 10 has period $12 = \frac{24}{\gcd(24,10)}$ in $\mathbb{Z}_{24}$. Thus the period of $(8, 4, 10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$ is $\operatorname{lcm}(3, 15, 12) = 60$.

Example 7.6. Find the period of $(3, 7, 12)$ in the group $\mathbb{Z}_4 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$.

Solution:

We first find the period of 3, 7 and 12 in $\mathbb{Z}_4$, $\mathbb{Z}_{10}$ and $\mathbb{Z}_{15}$ respectively:

The period of 3 in $\mathbb{Z}_4$ is 4 since $\gcd(3, 4) = 1$; 7 has period 10 in $\mathbb{Z}_{10}$ by a similar argument, lastly 12 has period $5 = \frac{15}{\gcd(15,12)}$ in $\mathbb{Z}_{15}$.

The period of $(3, 7, 12)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$ is the lowest common multiple of 4, 10 and 5 which is 20.

We now turn our attention to the question of whether or not a direct product of groups is

cyclic. Consider the direct product group $\mathbb{Z}_2 \times \mathbb{Z}_4$.

$\oplus$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,3)$	$(1,0)$	$(1,1)$
$(0,3)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,3)$	$(1,0)$	$(1,1)$	$(1,2)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,3)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$
$(1,3)$	$(1,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$

Notice that although $\mathbb{Z}_2$ and $\mathbb{Z}_4$ are both cyclic, $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic — it has no element of period 8. For $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_4$, the period of a in $\mathbb{Z}_2$ is either 1 or 2 while the period of b (in $\mathbb{Z}_4$) is one of 1, 2 or 4. Therefore the largest possible value of the lowest common multiple of the period of a and the period of b is 4. This means that the largest possible period of an element of $\mathbb{Z}_2 \times \mathbb{Z}_4$ is 4.

Notice though that any element of $\mathbb{Z}_2 \times \mathbb{Z}_4$ can be written as a power of $(1,0)$ times a power of $(0,1)$.

More generally it is the case that the direct product of n cyclic groups, each of which is

either $\mathbb{Z}$ or $\mathbb{Z}_m$ for some positive integer m, is generated by the n-tuples

$$(1, 0, 0 \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1).$$

Such a direct product might also be generated by fewer elements; for example, $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{35}$ is generated by the single element $(1, 1, 1)$.

Example 7.7.

Consider $\mathbb{Z}_2 \times \mathbb{Z}_3$. This is a group of order 6. We know that there is only one abelian group of order 6, namely $\mathbb{Z}_6$ and so $\mathbb{Z}_2 \times \mathbb{Z}_3$ must be cyclic. How do we find an element of order 6in $\mathbb{Z}_2 \times \mathbb{Z}_3$? Let $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$. Let r be the period of $a \in \mathbb{Z}_2$ and s be the period of $b \in \mathbb{Z}_3$. If (a, b) is a generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$ then $\mathrm{lcm}(r, s) = 6$. Thus if we can find an element $a \in \mathbb{Z}_2$ of period 2 and an element $b \in \mathbb{Z}_3$ of period 3, then (a, b) will be a generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$. We can chose $a = 1$ and $b = 1$, the element $(1, 1)$ is therefore a generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Example 7.8.

Consider the group $\mathbb{Z}_3 \times \mathbb{Z}_3$. Let $(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_3$. Notice that the possible periods of $a, b \in \mathbb{Z}_3$ is 1 or 3. It follows that the largest possible value of the lowest common multiple of the period of a and the period of b is 3. There is no element of order 9 in $\mathbb{Z}_3 \times \mathbb{Z}_3$ — it is not a cyclic group.

The above examples are illustrations of the following general result.

Theorem 7.6. *The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic (and, hence, isomorphic to $\mathbb{Z}_{mn}$) if and only if m and n are relatively prime.*

Proof.

Suppose m and n are co-prime. This means that the lcm of m and n is mn. Consider the element $(1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$. The period of $1 \in \mathbb{Z}_m$ is m and the period of 1 in $\mathbb{Z}_n$ is n, it follows that the period of $(1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is $mn = \mathrm{lcm}(m, n)$.

Suppose $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic. This means there is an element $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ with period mn. Let l be the period of $a \in \mathbb{Z}_m$ and p be the period of b in $\mathbb{Z}_n$. Then $\operatorname{lcm}(l, p) = mn$. Notice that $l|m$ and $p|n$ by Theorem 4.1 therefore $l|\operatorname{lcm}(m, n)$ and $p|\operatorname{lcm}(m, n)$. Therefore $\operatorname{lcm}(l, p) \leq \operatorname{lcm}(m, n)$. It follows that $\operatorname{lcm}(m, n) = mn$. Now if $\gcd(m, n) \neq 1$, then $\operatorname{lcm}(m, n) < mn$. We conclude that $\gcd(m, n) = 1$ as required.

□

This theorem can be extended, by similar arguments, to a product of more than two factors. We state this result as a corollary without proof.

Corollary 7.2. *The group $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_n}$ is cyclic (and, hence, isomorphic to $\mathbb{Z}_{m_1 m_2 \ldots m_n}$) if and only if $m_1, m_2, \ldots, m_n$ are pairwise relatively prime.*

Example 7.9.

- The group $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_9$ is cyclic and isomorphic to $\mathbb{Z}_{90}$.
- The group $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic — $\gcd(2, 4) = 2$.
- The group $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_8$ is not cyclic — $\gcd(2, 8) = 2$.

7.3 Structure of Finite Abelian Groups

We said at the outset of the module that, in our study of Abstract Algebra, we would be interested in structure rather than content. It bears repeating, as we embark on the final part of our introduction to group theory and encounter another major structural theorem, just how far we have travelled from a set, an associated binary operation, and four simple axioms. Everything that we have encountered along the way, the entire edifice of structural theory that we have assembled, has emanated from those rudimentary foundations (and we have barely scratched the surface of the theory of groups). In the final section of this chapter we examine the structure of finite abelian groups and we begin by stating, without proof, the theorem that gives us complete structural information about *all* finite abelian groups.

Theorem 7.7 (Fundamental Theorem of Finite Abelian Groups)**.** *Every finite abelian group is isomorphic to a direct product of cyclic groups of the form*

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers.

Note that the direct product is unique, except for the possible rearrangement of the factors. We can now classify (up to isomorphism) the abelian groups of any order according to the Fundamental Theorem.

Order 1: There is only one group of order 1 (up to isomorphism), $\mathbb{Z}_1$.

Order 2: There is only one group (up to isomorphism) of order 2 (2 is prime) and it is $\mathbb{Z}_2$

Order 3: As above only $\mathbb{Z}_3$.

Order 4: There are two isomorphically distinct abelian groups of order 4, $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$.

Order 5: Only $\mathbb{Z}_5$ as 5 is prime.

Order 6: There is only one abelian group (up to isomorphism) $6 = 2 \times 3$ and $\gcd(2,3) = 1$. Therefore $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Order 7: $\mathbb{Z}_7$ as 7 is prime.

Order 8: There are 3 abelian groups of order 8 up to isomorphism. We decompose $8 = 2^3 = 2 \times 4$ this gives isomorphically distinct groups

$$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4 \text{ and } \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Order 9: There are two isomorphically distinct abelian groups of order 9: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Order 10: Decompose $10 = 2 \times 5$. Notice that $\gcd(2,5) = 1$, therefore $\mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_10$. There is only one abelian group of order 10 — $\mathbb{Z}_{10}$.

Order 11: Only $\mathbb{Z}_{11}$ as 11 is prime.

Order 12: We have $\mathbb{Z}_{12}$ and$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. We decompose

$$12 = 2^2 \times 3 = 2 \times 2 \times 3.$$

Observe that $\gcd(3,4) = 1$ therefore $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_12$. Notice that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ (since $\gcd(2,3) = 1$) and so $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$. However, $\mathbb{Z}_6 \times \mathbb{Z}_2$ is not in the form of TFTFAG (Theorem 7.7).

Example 7.10. Classify, according to the Fundamental Theorem of Finite Abelian Groups, all of the abelian groups of order

i. 54

ii. 600.

Indicate which of the groups of order 54 listed is cyclic, and which is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_9$.

Solution:

i. We decompose $54 = 2 \times 3^3$. This gives isomorphically distinct groups

- $\mathbb{Z}_2 \times \mathbb{Z}_{3^3}$
- $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$
- $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

The group $\mathbb{Z}_2 \times \mathbb{Z}_{27}$ is cyclic since $\gcd(2,27) = 1$; the group $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$ is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_9$ since $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

ii. We decompose $600 = 2^3 \times 3 \times 5^2$. This gives isomorphically distinct groups

- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_2 \times \mathbb{Z}_4 \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$.

Observe that $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$ is isomorphic to $\mathbb{Z}_{600}$ since 8, 3 and 25 are pairwise relatively prime.

We are now in a position to prove that the converse of Lagrange's Theorem is true for all abelian groups. We shall use the following lemma.

Lemma 7.3. *If d divides n, then $\mathbb{Z}_n$ contains a subgroup of order d.*

Proof.

Let $c = \frac{n}{d}$. Then $c|n$ and so $\frac{n}{\gcd(c,n)} = \frac{n}{c} = d$. It follows that the element $c \in \mathbb{Z}_n$ has period d and so $\langle c \rangle$ is a subgroup of $\mathbb{Z}_n$ of order d.

□

Example 7.11.

Consider $\mathbb{Z}_{12}$. We note that $3|12$ and $\langle 4 \rangle$ is a subgroup of $\mathbb{Z}_{12}$ of order 3. Indeed $\langle 4 \rangle = \{0, 4, 8\}$.

Theorem 7.8. *Let G be a finite abelian group of order n and let d be any divisor of n. Then G has a subgroup of order d.*

Proof.

Let $p_1, p_2, \ldots, p_m$ be primes and let $r_1, r_2, \ldots, r_m$ be positive integers so that $p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m} = n$ and $G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_m^{r_m}}$.

Now since d is a divisor of n, there are positive integers $s_1, s_2, \ldots, s_m$, where $0 \leq s_i \leq r_i$, $i = 1, 2 \ldots, m$, such that $d = p_1^{s_1} p_2^{s_2} \ldots p_m^{s_m}$.

Now as $p_i^{s_i} | p_i^{r_i}$ for all $1 \leq i \leq m$, $\mathbb{Z}_{p_i^{r_i}}$ has a subgroup H_i of order $p_i^{s_i}$. Notice that $H_1 \times H_2 \times \ldots \times H_m$ is a subgroup of $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_m^{r_m}}$. Moreover the order of $H_1 \times H_2 \times \ldots \times H_m$ is precisely $p_1^{s_1} p_2^{s_2} \ldots p_m^{s_m} = d$. Therefore $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_m^{r_m}}$ has a subgroup of order d and so G has a subgroup of order d.

□

Example 7.12. Consider $\mathbb{Z}_9 \times \mathbb{Z}_4$.

Notice that $\gcd(9,4) = 1$ and so $\mathbb{Z}_9 \times \mathbb{Z}_4$ is isomorphic to $\mathbb{Z}_{36}$. Indeed, $\mathbb{Z}_9 \times \mathbb{Z}_4$ is generated by $(1,1)$. If we want to find a subgroup of $\mathbb{Z}_9$ of order 3, then this corresponds to an element of order 3 (subgroups of cyclic groups are cyclic). Notice that $(1,1)^{12} = (3,0)$ has order 3. Indeed $\langle (3,0) \rangle = \{(0,0), (3,0), (6,0)\}$.

A subgroup of order 6 corresponds to an element of order 6. Notice that $(1,1)^6 = (6,2)$ is an element of order 6 (6 has order 3 in $\mathbb{Z}_9$ and 2 has order 2 in $\mathbb{Z}_4$; $6 = \operatorname{lcm}(2,3)$). We observe that

$$\langle (6,2) \rangle = \{(0,0), (6,2), (3,0), (0,2), (6,0), (3,2)\} = \langle (3,0) \rangle \times \langle (0,2) \rangle .$$

Example 7.13. Find two isomorphically distinct subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ of order 12.

(a) Notice that $\mathbb{Z}_4 \times \mathbb{Z}_9 \cong \mathbb{Z}_{36}$. Indeed $\mathbb{Z}_4 \times \mathbb{Z}_9 = \langle (1,1) \rangle$. We can find a subgroup of order 12 of $\mathbb{Z}_4 \times \mathbb{Z}_9$ by finding an element of order 12 — $(1,1)^3 = (3,3)$ for instance. To extend this to a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ we simply take $(0,3,3)$. Thus $\langle (0,3,3) \rangle$ is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ of order 12.

(b) How do we find another isomorphically distinct subgroup? Notice that abelian groups of order 12 (up to isomorphism) are $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Thus to find a subgroup of order 12 isomorphically distinct from $\mathbb{Z}_{12}$, we need to find a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. We find the first $\mathbb{Z}_2$ factor from $(1,0,0)$, the second from $(0,2,0)$ and the $\mathbb{Z}_3$ factor from $(0,0,3)$. The second subgroup of order 12 is generated by these three elements:

$$\{(0,0,0), (1,0,0), (0,2,0), (0,0,3),$$
$$(1,2,0), (1,0,3), (0,2,3), (0,0,6),$$
$$(1,0,6), (0,2,6), (1,2,6), (1,2,3)\}$$

Example 7.14. Find a subgroup of $\mathbb{Z}_{14} \times \mathbb{Z}_{28}$ of order 98.

Solution

Notice that $98 = 14 \times 7$. Thus to find a subgroup of order 98, we take $\mathbb{Z}_{14} \times H$ where H is a subgroup of $\mathbb{Z}_{28}$ of order 7. We note that such a subgroup H exists since 7 divides 28 indeed we can take $H = \langle 4 \rangle$. Thus $\mathbb{Z}_{14} \times \langle 4 \rangle$ is a subgroup of $\mathbb{Z}_{14} \times \mathbb{Z}_{28}$ of order 98.

Theorem 7.8 says that the converse of Lagrange's Theorem is true for all finite abelian groups. But what about non-abelian groups? We know that, in general, the converse of Lagrange's Theorem is false, but can we say more than that, in the sense that given a group of a given order we know the orders of the subgroups that it *must* contain? It turns out that we can say more and that is the subject of the following theorem, due to the Norwegian mathematician Peter Sylow. We state it without proof - for the proof you will have to take the third-year Group Theory module.

Theorem 7.9 (Sylow's First Theorem)**.** *Let G be a finite group of order $p^\alpha m$, where p is a prime not dividing m. Then G has a subgroup of order p^β for each integer β such that $0 \leq \beta \leq \alpha$.*

We can see that this theorem tells us, for groups of a particular order, which order subgroups must exist. This is the closest that we can get to the converse of Lagrange's Theorem.

Example 7.15.

Let G be a group of order $80 = 2^4 \times 5$. By Sylow's First Theorem, G has subgroups of order 2^0, 2, 2^2, 2^3 and 2^4 and also a subgroups of order 5.

Note that Sylow's first theorem tells us nothing about the existence subgroups of order 20! We would have to dig further to determine if these exists or not.

7.4 Problem Sheet 7

For Week 10; covers Chapter 7.

Question 7.1

List the generators in each of the following cyclic groups:

i. $\mathbb{Z}_{10}$;

ii. $\mathbb{Z}_{24}$;

iii. $\mathbb{Z}_3 \times \mathbb{Z}_4$.

Show Solution 7.1 on P219

Question 7.2

In each of the following cases find the period of the given element of the direct product group:

i. (1, 3) in $\mathbb{Z}_4 \times \mathbb{Z}_9$;

ii. (4, 12) in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$;

iii. (3, 4, 2) in $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_9$.

Show Solution 7.2 on P219

Question 7.3

i. Classify, according to the Fundamental Theorem of Finite Abelian Groups all of the abelian groups of order 100. Which of the groups is cyclic? Which is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_{20}$?

ii. Classify, according to the Fundamental Theorem of Finite Abelian Groups all of the abelian groups of order 504. Which of the groups is cyclic? Which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{21}$?

iii. How many isomorphically distinct abelian groups are there of order 104,544?

Show Solution 7.3 on P220

Question 7.4

i. Find a subgroup of $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ of order 9.

ii. Find a subgroup of $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{35}$ of order 252.

Show Solution 7.4 on P222

Question 7.5

Show, by exhibiting a counter-example, that the following converse of Theorem 7.3 is false.

> If a group G is such that every proper subgroup is cyclic, then G is cyclic.

Can you find infinitely many counter-examples?

Show Solution 7.5 on P222

Chapter 8

Groups and Numbers

The aim of this chapter is to look at the relationship between group theory and number theory. We begin by revisiting some basic ideas that we met in first-year Algebra before considering what happens when we examine the set $\mathbb{Z}_n$ under multiplication rather than addition. This leads to a consideration of what we call the Reduced Residue System. We then use the results of that analysis to shed light on some problems in number theory.

8.1 Basic Concepts

We first state, as a reminder, some results from Algebra that we shall be using in this chapter (though the proofs are omitted and will not be required).

a. Let $d, n \in \mathbb{Z}$, then d divides n if and only if n is an integer multiple of d, that is, $d \,|\, n$ if and only if $\exists\, q \in \mathbb{Z}$ such that $n = qd$.

b. If $d \,|\, m$ and $d \,|\, n$, then $\forall\, a, b \in \mathbb{Z}$, we have that $d \,|\, (am + bn)$.

c. Let $d, n \in \mathbb{Z}$, $d > 0$. Then $\exists$ unique $q, r \in \mathbb{Z}$ such that $n = qd + r$, $0 \leq r < d$.

d. Let $a = qb + r$, where a, b, q, r are all integers. Then d is a common divisor of a and b if and only if d is a common divisor of b and r.

e. Let $a = qb + r$, where a, b, q, r are all integers. Then $\gcd(a, b) = \gcd(b, r)$. This is known as Euclid's algorithm.

f. Let a, b, m be integers, $m > 0$. Then a is *congruent* to b *modulo* m if and only if $m \mid (b - a)$. We denote this $a \equiv b \pmod{m}$.

g. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then

   i. $a + b \equiv a' + b' \pmod{m}$,

   ii. $ab \equiv a'b' \pmod{m}$.

This last property means that the result obtained from doing the arithmetic first and then reducing modulo m is the same as the result obtained by reducing all of the numbers modulo m first and then doing the arithmetic.

Example 8.1.

Consider:

$$14 \times 7 \pmod{6} = 98 \pmod{6} \equiv 2 \pmod{6}.$$

However $14 \equiv 2 \pmod{6}$ and $7 \equiv 1 \pmod{6}$, therefore

$$14 \times 7 \equiv 2 \times 1 \pmod{6} \equiv 2 \pmod{6}.$$

Euclid's algorithm does two things of interest; it finds $\gcd(a, b)$ and it enables us to express this greatest common divisor in the form $(ma + nb)$ where m and n are integers.

Example 8.2. Find $\gcd(207, 567)$ and then find integers s and t such that

$$\gcd(207, 567) = 207s + 567t.$$

Set $a = 567$ and $b = 207$, then:

$$
\begin{array}{r|l}
a = 567 & \\
\underline{\qquad 2b = 414} & b = 207 \\
a - 2b = 153 & \underline{a - 2b = 153} \\
\underline{-2a + 6b = 108} & -a + 3b = 54 \\
3a - 8b = 45 & \underline{3a - 8b = 45} \\
 & -4a + 11b = 9
\end{array}
$$

Thus the greatest common divisor if 207 and 567 is 9; $s = 11$ and $t = -4$.

An important property of gcd (a, b) is that it is the smallest positive integer which can be expressed in the form $ma + nb$; this result is a corollary to the following theorem.

Theorem 8.1. *Let a and b be non-zero integers. Then,*

$$\{ma + nb \mid m, n \in \mathbb{Z}\} = \{k \times \textit{gcd}\,(a, b) \mid k \in \mathbb{Z}\}.$$

Proof. Let $S = \{ma + nb \mid m, n \in \mathbb{Z}\}$ and $T = \{k \times \text{gcd}\,(a, b) \mid k \in \mathbb{Z}\}$.

Let $d = \gcd(a, b)$.

We first show that $T \subseteq S$. We can find $u, v \in \mathbb{Z}$ such that $d = ua + vb$. Thus for any $k \in \mathbb{Z}$, $kd = (ku)a + (kv)b \in S$.

Let $m, n \in \mathbb{Z}$. Since d divides both a and b, there are $\alpha, \beta \in \mathbb{Z}$ such that $a = d\alpha$ and $b = d\beta$. It follows that

$$ma + nb = (m\alpha)d + (n\beta)b = (m\alpha + n\beta)d \in T.$$

Therefore $S \subseteq T$.

We conclude that $S = T$.

□

Corollary 8.1. *Let $a, b \in \mathbb{Z}$, $S = \{ma + nb \mid m, n \in \mathbb{Z}\}$. Then gcd (a, b) is the smallest*

positive integer in S.

Proof.

Let $d = \gcd(a, b)$. By Theorem 8.1 $S = \{kd : k \in \mathbb{Z}\}$. Clearly d is the smallest positive integer in $\{kd : k \in \mathbb{Z}\}$ and so d is the smallest positive integer in S.

□

We have already been using the following concept, but we repeat the formal definition.

Definition 8.1 (Relatively Prime)**.** Two integers a and b are *relatively prime* if and only if $\gcd(a, b) = 1$.

Pairs of integers which are relatively prime include (7, 11), (8, 9), (12, 55), (-14, 65). Pairs of numbers which are not relatively prime include (6, 6), (15, 126), (-4, 18). When asked to prove something about relatively prime numbers we often use the following fact.

Corollary 8.2. *Two integers a and b are relatively prime if and only if there exist integers m and n such that $ma + nb = 1$.*

Proof.

If $\gcd(a, b) = 1$, then we can find integers $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

On the other hand, $d = \gcd(a, b)$ is the smallest positive integer in the set $S = \{ma + nb : m, n \in \mathbb{Z}\}$. If $1 \in S$, then it is clear that $d = 1$.

□

Corollary 8.3. *If $d \mid ab$ and d and a are relatively prime, then $d \mid b$.*

Proof.

We can find $m, n \in \mathbb{Z}$ such that $1 = md + na$. It follows that

$$b = b(md + na) = bmd + bna.$$

Since $d|ab$ and $d|d$ we conclude that $d|(bmd + abn)$. Therefore $d|b$ as required.

□

Example 8.3. The numbers 7 and 5 are relatively prime hence if 7 divides $5n$ for $n \in \mathbb{Z}$, then $7|n$.

Now consider 6 and 15. We have $\gcd(6, 15) = 3$ and so 6 and 15 are not relatively prime. Observe that $6|30$ but 6 divides neither 2 nor 15.

Of fundamental importance in number theory is the class of numbers called prime numbers.

Definition 8.2 (Prime Number)**.** A positive integer p is *prime* if and only if $p > 1$ and the only positive divisors of p are p and 1.

We refer to any positive integer that is not prime as *composite*. It is worth noting that if p is prime and a is any integer then the statement 'p does not divide a' is equivalent to saying that p and a are relatively prime (that is, $\gcd(p, a) = 1$). This is not the case if p is not prime, for example 10 does not divide 18 but 10 and 18 are not relatively prime. The importance of the class of primes is a consequence of the following theorem which we state without proof.

Theorem 8.2 (Fundamental Theorem of Arithmetic)**.** *Let n be a natural number. If $n \geq 2$ then n is uniquely expressible as a product of primes (except for reordering).*

Proof. Omitted. □

Example 8.4. Some examples

- $42 = 2 \times 3 \times 7$

- $64 = 2^6$
- $100 = 2^2 \times 5^2$
- 101 is prime.

The uniqueness property of a prime decomposition may seem obvious, but it depends on the number system. Of course who would have to first make precise what the definition of a 'prime' is in the new number system. Consider the following example.

Example 8.5. Consider the even integers $2\mathbb{Z}$. What are the primes? We consider a positive integer $m \in 2\mathbb{Z}$ prime if it is a not composite. Using this definition, the primes in $2\mathbb{Z}$ are

$$\{2(2k+1) : k \geq 0\} = \{2, 6, 10, 14 \ldots\}.$$

It is clear that any element of $2\mathbb{Z}$ can be factorised as a product of primes. Indeed any element of $2\mathbb{Z}$ which is not prime is of the form $2^i m$ for some $m \in \{2(2k+1) : k \geq 0\} = \{2, 6, 10, 14 \ldots\}$.

Do we have unique factorisation into primes? Take the number 36. This can be factorised either as 2×18 (both of which are prime with our definition) or as 6×6. Therefore we do not have unique factorisation.

Perhaps we have the wrong definition. What if we stick with Definition 8.2 unchanged. With this definition of prime, the only element of $2\mathbb{Z}$ that is prime is 2. In this case we do not always have a factorisation into primes! Indeed any even integer that is not a power of 2 cannot be factorised as a product of primes in $2\mathbb{Z}$.

Theorem 8.3. *Let $a, b, m \in \mathbb{Z}$. Then gcd$(a, m) = 1$ and gcd$(b, m) = 1$ if and only if gcd$(ab, m) = 1$.*

Proof.

Suppose $\gcd(a, m) = \gcd(b, m) = 1$. There are numbers $u, v, s, t \in \mathbb{Z}$ such that $ua + vm =$

$sb + tm = 1$. it now follows that $(ua + vm)(sb + tm) = 1$. Expanding:

$$(ua + vm)(sb + tm) = (as)ab + m(atu + bsv + mtv) = 1.$$

It follows that 1 is the smallest positive integer in $\{j(ab) + km : j, k \in \mathbb{Z}\}$. Therefore $\gcd(ab, m) = 1$ as required.

On the other hand suppose that $\gcd(ab, m) = 1$. Then 1 is the smallest positive integer in $\{j(ab) + km : j, k \in \mathbb{Z}\}$. However, $\{j(ab) + km : j, k \in \mathbb{Z}\} \subseteq \{j'a + k'm : j', k' \in \mathbb{Z}\}$ and $\{j(ab) + km : j, k \in \mathbb{Z}\} \subseteq \{j'b + k'm : j', k' \in \mathbb{Z}\}$. Therefore 1 is the smallest positive integer in each of $\{j'a + k'm : j', k' \in \mathbb{Z}\}$ and $\{j'b + k'm : j', k' \in \mathbb{Z}\}$. Therefore $\gcd(a, m) = \gcd(b, m) = 1$ as required.

□

8.2 Reduced Residue System

In the Algebra module we explored the idea of congruence modulo some positive integer n. It is worth reminding ourselves of the definition:

Definition 8.3 (Congruence)**.** Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. We say a *is congruent to* b *modulo* n, and write $a \equiv b \pmod{n}$, to mean that $n \mid (a - b)$.

Example 8.6.

- $15 \equiv 1 \pmod{7}$ since $7|(15 - 1)$;
- For any integer x and any positive integer n, $x \equiv x \pmod{n}$ as $n|(x - x)$.

It should be clear that for some given n there will be an infinite number of integers congruent to some fixed a modulo n and that we can group those integers together in a set. This is best illustrated by example.

Example 8.7.

Let $a = 2$ and $n = 5$. Then:

$$\begin{aligned} 2 &\equiv 2 \pmod 5 \\ 7 &\equiv 2 \pmod 5 \\ 12 &\equiv 2 \pmod 5 \\ -3 &\equiv 2 \pmod 5. \end{aligned}$$

This leads to the following definition.

Definition 8.4 (Residue Class)**.** Let a, n be integers, n positive. The *residue class* of a modulo n is denoted and defined by

$$[a]_n = \{m \mid m \in \mathbb{Z}, m \equiv a \pmod n\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Example 8.8.

$$\begin{aligned} [1]_5 &= \{\ldots, -14, -9, -4, 1, 6, 11, \ldots\} \\ [3]_7 &= \{\ldots, -11, -4, 3, 10, 17, \ldots\} \\ [0]_4 &= \{\ldots, -12, -8, -4, 0, 4, 8, \ldots\}. \end{aligned}$$

Aside

Consider $H = \{5k : k \in \mathbb{Z}\}$. This is a subgroup of $(\mathbb{Z}, +)$. Notice that the left coset of H containing 1 is precisely the left coset

$$1H = \{1 + h : h \in H\} = \{5k + 1 : k \in \mathbb{Z}\} = \{\ldots, -14, -9, -4, 1, 6, 11, \ldots\} = [1]_5.$$

So the left coset of H containing 1 is the residue class of 1 modulo 5. Notice that H is precisely $[0]_5$.

This is not a coincidence.

Let n be a positive integer. Then $H = \{nk : k \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. For any integer $a \in \mathbb{Z}$, the left coset aH of H containing a is precisely

$$\{a + h \in h \in H\} = \{a + nk : k \in \mathbb{Z}\} = [a]_n.$$

Clearly $H = [0]_n$.

Notice that grouping together in sets the integers that are congruent to each other modulo some given n results in a partitioning of the integers such that each integer appears in exactly one of the residue classes. This partitioning of $\mathbb{Z}$ is a direct consequence of the fact that congruence modulo n is what is known as an equivalence relation on a set (more of this in third-year Group Theory).

Example 8.9.

We take $n = 5$. Then:

$$\begin{aligned}
[0]_5 &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1]_5 &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2]_5 &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3]_5 &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4]_5 &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}.
\end{aligned}$$

Lemma 8.1. *Every integer is in exactly one of the residue classes $[0]_n, [1]_n, \ldots, [n-1]_n$ for a given positive integer n.*

Proof.

We note that for i between 0 and $n-1$ and $a \in \mathbb{Z}$, $a \in [i]_n$ precisely when a has remainder i when divided by n. Therefore every integer belongs to one of the residue classes $[0]_n, [1]_n, \ldots, [n-1]_n$.

□

Recall that when we first introduced the concept of $\mathbb{Z}_n$, we defined this to be the set $\{0, 1, 2, \ldots, n-1\}$. Strictly speaking, we should have defined $\mathbb{Z}_n$ as

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\},$$

though for practical purposes we tend to use the former representation.

Definition 8.5. Let $A, B \in \mathbb{Z}_n$ (so A and B are residue classes, not numbers). Choose $a \in A$ and $b \in B$. Then

i. $A + B = [a+b]_n$ or, equivalently, $[a]_n + [b]_n = [a+b]_n$,
ii. $A \times B = [ab]_n$ or, equivalently, $[a]_n[b]_n = [ab]_n$.

Note that this is a set with two binary operations defined on it. This forms the triple $(\mathbb{Z}_n, +, \times)$ and such a structure is called a ring, provided that certain axioms are satisfied. We shall see more of this in the final chapter.

Example 8.10.

Take $n = 5$. Then $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$. We compute

i. $[1]_5 + 2_5 = [1+2]_5 = [3]_5$;
ii. $[3]_5[4]_5 = [3 \times 4]_5 = [2]_5$.

It is important to check that these operations are well defined. That is, if we were to choose different members of A and B, say a' and b' instead of a and b respectively, does

$[a' + b']_n = [a']_n + [b']_n$ and does $[a'b']_n = [a']_n[b']_n$? The fact that the answer is in the affirmative follows from statement (g) in the introductory section to this chapter.

Lemma 8.2. $(\mathbb{Z}_n, +)$ *is an abelian group.*

Proof.

This is clear from the definition of $+$ on $\mathbb{Z}_n$.

□

Suppose that we now change the binary operation on $\mathbb{Z}_n$ from addition modulo n to multiplication modulo n. Let us take $\mathbb{Z}_5$ as an example and construct the operation table (in all of the following examples we shall, for convenience, write a in place of $[a]_n$).

$\otimes_5$	0	1	2	3	4
0	0	1	2	3	4
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

As we can see, $(\mathbb{Z}_5, \times)$ cannot be a group as the element 0 has no inverse; recall that under multiplication the identity element is 1 and in the table above it is clear that there does not exist an element of $\mathbb{Z}_5$, a say, such that $0 \times a = a \times 0 = 1$. So what if we remove 0 from the set and consider $(\mathbb{Z}_5 \backslash \{0\}, \times)$? It should be clear, from an examination of the table above, that this results in the following group (check the axioms):

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The obvious question to ask at this point is whether or not this process works for all $n \in \mathbb{N}$. Consider $(\mathbb{Z}_8 \backslash \{0\}, \times)$:

$\otimes_8$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Clearly this does not form a group for two reasons. First, the set is not closed under $\otimes_8$ and, second, not all elements have an inverse in the set (1, 3, 5, and 7 have inverses in the set, but 2, 4, and 6 do not). Notice, also, that it is the non-invertible elements that cause the system to be not closed. So, what if we were to remove the elements that have no inverse in the set?

$\otimes_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

This system now forms a group. But what is the relationship between the elements of $\mathbb{Z}_n$

that have no inverse and n itself? On the face of the above example, it looks like we simply remove the even numbers from the set. However, if we consider $(\mathbb{Z}_{12}\backslash\{0\}, \times)$, in order for that to be a group we need to remove the elements 2, 3, 4, 6, 8, 9, and 10. So how do we identify the invertible elements in $\mathbb{Z}_n$? The answer comes from the following definition:

Definition 8.6 (Reduced Residue System)**.** The *reduced residue system* modulo n is denoted and defined by

$$\mathbb{Z}_n^\times = \{\, [a]_n \in \mathbb{Z}_n \mid \exists\, [b]_n \in \mathbb{Z}_n \text{ s.t. } [a]_n[b]_n = [1]_n \,\}.$$

Theorem 8.4. *For any positive integer n, $\mathbb{Z}_n^\times$ is an abelian group.*

Proof.

If $\mathbb{Z}_n^\times$ is a group then it must be an abelian group since the product is commutative. We therefore verify that $\mathbb{Z}_n^\times$ forms a group under multiplication.

Closure: Let $[a]_n, [b]_n \in \mathbb{Z}_n^\times$. Then there are elements $[a']_n, [b']_n \in \mathbb{Z}_n$ such that $[a]_n[a']_n = [1]_{[}n] = [b]_n[b']_n$. Now consider $[ab]_n$. Observe

$$[ab]_n[a'b']_n = [(ab)(a'b')]_n = [1]_n$$

since $ab \equiv 1 \pmod{n}$ and $a'b' \equiv 1 \pmod{n}$.

Assoociativity: Let $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n^\times$. Then,

$$\begin{aligned}
([a]_n[b]_n)[c]_n &= [ab]_n[c]_n \\
&= [(ab)c]_n \\
&= [a(bc)]_n \\
&= [a]_n[bc]_n \\
&= [a]_n([b]_n[c]_n).
\end{aligned}$$

Identity: It is clear that $[1]_n \in \mathbb{Z}_n^\times$ is the identity element.

Inverses: Let $[a]_n \in \mathbb{Z}_n^\times$. By definition, there is an element $[a']_n \in \mathbb{Z}_n$ such that $[a]_n[a']_n = [1]_n$. Notice that $[a']_n[a]_n = [1]_n$ also. It follows that $[a']_n \in \mathbb{Z}_n^\times$ and every element $[a]_n \in \mathbb{Z}_n^\times$ has an inverse in $\mathbb{Z}_n^\times$.

□

One consequence of the definition is that we can characterise $\mathbb{Z}_n^\times$ in a different way, namely as the set of all positive integers less than n that are relatively prime to n (from here on in we shall, in general, use a single representative of a residue class to represent the class itself). Note, however, that this is not an alternative definition, just a convenient way of 'seeing' $\mathbb{Z}_n^\times$. One advantage of this characterisation is that it makes it easy to identify the elements in the set and, hence, to determine the size of the set (more of that later).

Example 8.11. The elements of $\mathbb{Z}_{15}^\times$ are the positive integers that are relatively prime to 15.

$$\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

and the operation table is

$\otimes_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

What we have discussed above leads to the following corollary.

Corollary 8.4. $(\mathbb{Z}_n \backslash \{[0]_n\}, \times)$ *is a group if and only if* n *is prime.*

Proof.

$\Rightarrow$: Suppose $(\mathbb{Z}_n \backslash \{[0]_n\}, \times)$ is a group. Suppose $n = pq$ for some positive integers $p, q \leq n$. If $p, q < n$, then $[p]_n, [q]_n \in \mathbb{Z}_n \backslash \{[0]_n\}$ and

$$[p]_n [q]_n = [pq]_n = [n]_n = [0]_n.$$

This is a contradiction since, by assumption, $(\mathbb{Z}_n \backslash \{[0]_n\}, \times)$ is a group and so it is closed under time. It follows that one of p and q is equal to n and the other is equal to 1. Thus the only divisors of n and 1 and itself — n is prime.

$\Leftarrow$: If n is prime then $\mathbb{Z}_n^\times = \mathbb{Z}_n \backslash \{[0]_n\}$ (by the alternative characterisation above). Therefore, $(\mathbb{Z}_n \backslash \{[0]_n\}, \times)$ is a group since it is precisely $(\mathbb{Z}_n^\times, \times)$.

□

Example 8.12.

a. Write down the elements of $\mathbb{Z}_{20}^\times$ and $\mathbb{Z}_{24}^\times$.

   We have

   $$\mathbb{Z}_{20}^\times = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

   and

   $$\mathbb{Z}_{24}^\times = \{1, 5, 7, 11, 13, 17, 19, 23\}.$$

b. Classify, according to the Fundamental Theorem of Finite Abelian Groups, all of the abelian groups of order 8.

   We decompose $8 = 2^3$. This gives isomorphically distinct abelian groups

   $$\mathbb{Z}_4, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

c. The groups in (a) are isomorphic to which of the groups in (b)?

The group $Z_{20}^{\times}$ has elements of order 4 and none of order 8 and so must be isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$; for $Z_{24}^{\times}$ all of its elements have order 2 and so it is also isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 8.13.

a. List the elements of $\mathbb{Z}_9^{\times}$.

$$\mathbb{Z}_9^{\times} = \{1, 2, 4, 5, 7, 8, \}.$$

b. Show that this group is isomorphic to $\mathbb{Z}_6$.

We need only show that $\mathbb{Z}_9^{\times}$ is cyclic. Indeed it is generated by 2, and also by 5.

c. Find two distinct isomorphisms between $\mathbb{Z}_9^{\times}$ and $\mathbb{Z}_6$.

The two distinct isomorphisms arise from the two different generators:

- $\theta_1 : \mathbb{Z}_9^{\times} \to \mathbb{Z}_6$ by $\theta_1(2^i) = i$ for $0 \leq i \leq 5$;
- $\theta_2 : \mathbb{Z}_9^{\times} \to \mathbb{Z}_6$ by $\theta_2(5^i) = i$ for $0 \leq i \leq 5$.

We note that $\theta_1 \neq \theta_2$ since $\theta_1(5) = 5$ and $\theta_2(5) = 1$.

8.3 Applications to Number Theory

In the last part of this chapter we shall examine how we can use our knowledge of groups to solve problems in number theory and, in particular, we shall be studying three theorems, namely Fermat's Little Theorem (FLT), Euler's Theorem, and Wilson's Theorem. It is hoped that this very short review of number theoretic problems will not only convince you of the power of the abstract algebra that we have studied to date, but also whet your appetite for the third-year Number Theory and Cryptography module.

We begin with a statement of Fermat's Little Theorem.

Theorem 8.5 (Fermat's Little Theorem)**.** *Let p be a prime and let a be any integer such that p does not divide a. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof.

First we note that if p does not divide a, then $[a]_p \in \mathbb{Z}_p^\times$ (a is co-prime to p).

The result is now a consequence of Theorem 4.1. We can see this as follows: $|\mathbb{Z}_p^\times| = p - 1$ since $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash \{[0]_p\}$. Now Theorem 4.1 states that the order of $[a]_p$ divides $|\mathbb{Z}_p^\times|$. It follows that $([a]_p)^{p-1} = [a^{p-1}]_p = [1]_p$. Thus $a^{p-1} \equiv 1 \pmod{p}$.

□

Example 8.14. What is the principal remainder on dividing 6^{82} by 17?

Solution:

Observe that 17 is prime and so we can make use of Fermat's Little Theorem to simplify this calculation. Write $82 = (5 \times 16) + 2$. Then $6^{82} = (6^{16})^5 \times 6^2$. By FLT, $6^{16} \equiv 1 \pmod{17}$. Therefore,

$$(6^{16})^5 \times 6^2 \equiv 6^2 \pmod{17} \equiv 2 \pmod{1}7.$$

Example 8.15. Show that, for every positive integer n, the number $n^{33} - n$ is divisible by 15.

First observe that $n^{33} - n = n(n^{32} - 1)$. Next observe that $15|n^33 - n$ if and only if both 5 and 3 divide $n^{33} - n$. Since 5 and 3 are prime we can make use of FLT. We show that both 5 and 3 divide $n(n^{32} - 1)$.

- $3|(n^{33} - n)$: If 3 divides n we are done. If 3 does not divide n, then n and 3 are relatively prime. Write $32 = 2 \times 16$. Then

  $$n^{32} \equiv (n^2)^{16} \equiv 1 \pmod{3}$$

  by FLT. Therefore $n^{32} - 1 \equiv 0 \pmod{3}$ and $3|(n^32 - 1)$.

- $5|(n^{33} - n)$: If 5 divides n we are done. If 5 does not divide n, then n and 5 are relatively prime. Write $32 = 4 \times 8$. Then

$$n^{32} \equiv (n^4)^8 \equiv 1 \pmod 5$$

by FLT. Therefore $n^{32} - 1 \equiv 0 \pmod 5$ and $5|(n^32 - 1)$.

The obvious question to ask is whether we can generalise the above result to include composite moduli. Consider the conditions that apply for FLT to work; first, we work modulo a prime, second we have that p does not divide a. Recall that if p is prime the statement p does not divide a is equivalent to saying that p and a are relatively prime. So, a naive approach to extending the theorem to composite numbers would be to conjecture as follows:

Let a and n be integers such that $\gcd(a, n) = 1$. Then $a^{n-1} \equiv 1 \pmod n$.

Does this work?

This does not work. A counterexample is as follows: take $n = 4$ and $a = 3$. Then $\gcd(a, n) = \gcd(3, 4) = 1$. However

$$3^3 \equiv 3 \pmod 4.$$

So, is there a way in which we can generalise FLT to cover non-prime moduli? The answer is 'yes' and the solution lies in considering the exponent of a; if we are raising a to the power of $p - 1$, where p is prime, that is the same as raising it to the power of the order of $\mathbb{Z}_p^\times$ since this group has $p - 1$ elements (a fact that was used in our proof of FLT). We consider, then, raising a to the power of the order of $\mathbb{Z}_n^\times$ where $n \in \mathbb{N}$ and working modulo n.

Definition 8.7 (Euler Totient Function)**.** Let $m, n \in \mathbb{N}$. The *Euler totient function*, denoted ϕ, is the function $\phi : \mathbb{N} \to \mathbb{N}$ defined by

$$\phi(n) = |\{m \in \mathbb{N} \mid m \leq n \text{ and } \gcd(m, n) = 1\}|, \quad \forall\, n \in \mathbb{N}.$$

Note that this is, in fact, $|\mathbb{Z}_n^\times|$.

Example 8.16.

$\phi(30) = |\{1, 7, 11, 13, 17, 19, 23, 29\}| = 8.$

We can now generalise FLT to include composite moduli as follows:

Theorem 8.6 (Euler's Theorem)**.** *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that a and n are relatively prime. Then,*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof.

The proof is almost identical to the proof of FLT. The key ingredient is once more Lagrange's Theorem.

Let $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then $[a]_n \neq [0]_n$ and $[a]_n \in \mathbb{Z}_n^\times$. Now as $|\mathbb{Z}_n^\times| = \phi(n)|$, we have, by Lagrange's Theorem that

$$([a]_n)^{\phi(n)} = [1]_n.$$

Therefore $a^{\phi(n)} \equiv 1 \pmod{n}$ as required.

□

Hopefully, the success or failure of our chosen attempts to generalise FLT will now make complete sense.

Let us revisit the $n = 4$ and $a = 3$ example. Notice that $\phi(4) = 2$ and $3^2 \equiv 1 \pmod{4}$.

This function, together with Euler's Theorem, prove to be extremely useful tools in solving number-theoretic problems.

Example 8.17. Find the unit digit of 3^{101}.

Notice that if $d \in \{0, 1, \ldots, 9\}$ is the unit digit of 3^{101}, then $3^{101} \equiv d \pmod{10}$ since there is a $q \in \mathbb{Z}$ such that $3^{101} = 10q + d$. We use Euler's Theorem to compute d. Note that $\phi(10) = |\{1, 3, 7, 9\}| = 4$ and $101 = 4 \times 25 + 1$. It follows that

$$3^{101} = (3^4)^{25} \times 3) \equiv 1 \times 3 \pmod{10}.$$

The last digit of 3^{101} is therefore 3.

The function $\phi : \mathbb{N} \to \mathbb{N}$ has some remarkable properties. But, given $n \in \mathbb{N}$, how do we calculate $\phi(n)$? If n is large it will be very time consuming to investigate all of the natural numbers less than n to establish which are relatively prime to n. We might hope for a formula to allow us to calculate $\phi(n)$ for any $n \in \mathbb{N}$, but where do we start in trying to find such a formula? The following table lists $\phi(n)$ for $1 \leq n \leq 30$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\phi(n)$	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

There does not appear to be a pattern, except that $\phi(n)$ appears to always be even for $n > 2 \ldots$ to find out more you need to sign up for third-year Number Theory and Cryptography!

Notice the very close link between FLT and Euler's Theorem.

FLT is a corollary of Euler's Theorem: if p is prime, $\phi(p) = p - 1$ and so for $a \in \mathbb{Z}$ relatively prime to p, $a^{\phi(p)} = a^{p-1} \equiv 1 \pmod{p}$.

It is worth noting that Euler's totient function and Euler's Theorem are central to a cryptosystem called RSA, an algorithm for public-key cryptography, developed in 1977, that relies on the prime factorisation of extremely large integers and which is used for, inter alia, encrypting

credit card data during purchases over the internet. Again, more of that in third-year Number Theory and Cryptography.

We conclude our very brief survey of applications of group theory to number theory with an investigation. Returning to that Friday evening from Chapter 6, having become bored with rearranging your ten Maths text books, and having already deduced that there are 10! possible arrangements of those books on your shelf, your mind turns to modular arithmetic (you really need to get out more...). You decide to investigate the relationship between the number of arrangements of $n \in \mathbb{N}$ books and that number modulo n. You realise that this is trivial since $n! \equiv 0 \pmod{n}$ for all natural numbers n so, determined to find something more interesting (and still waiting for someone to invite you out), you decide to investigate the relationship between $(n-1)!$ and itself modulo n. Some rapid calculations yield the following table:

n	$(n-1)!$	$(n-1)! \pmod{n}$
2	1	1
3	2	2
4	6	2
5	24	4
6	120	0
7	720	6
8	5040	0
9	40320	0
10	362880	0
11	3628800	10
12	39916800	0

You think that you are spotting a pattern, but now, so engrossed in it all, you carry on to test your hypothesis further...

n	$(n-1)!$	$(n-1)! \pmod n$
13	big	12
⋮	⋮	⋮
17	very big	16
⋮	⋮	⋮
19	humongous	18

Satisfied, you postulate that there is a relationship between $(n-1)!$ and itself modulo n if n is prime. You have discovered Wilson's Theorem.

Theorem 8.7 (Wilson's Theorem)**.** *If p is prime, then $(p-1)! \equiv -1 \pmod p$.*

Proof.

We begin with the following observation. Let $1 \leq x \leq p-1$ and suppose that x is its own inverse in $\mathbb{Z}_p^\times$. This means that $x^2 \equiv 1 \pmod p$. Rearranging, $x^2 - 1 \equiv 0 \pmod p$. Therefore $p|(x^2-1)$. Using the difference of two squares $p|((x-1)(x+1)$. Since p is prime either $p|(x-1)$ or $p|(x+1)$. Thus $x \equiv \pm 1 \pmod p$. Since $1 \leq x \leq p-1$, then $x = 1$ or $x = p-1$. Thus $x \in \mathbb{Z}_p^\times \backslash \{1, p-1\}$, the inverse of $x \in \mathbb{Z}_p^\times$ is not equal to x. For $2 \leq x < p-1$ write x^{-1} for the element of $y \in \{2, 3, \ldots, p-2\}$ such that $xy \equiv 1 \pmod p$. Thus we can find elements $x_1, x_2, \ldots, x_{\left(\frac{p-3}{2}\right)} \in \{2, 3, \ldots, p-2\}$ such that

$$(p-1)! = 1 \times (x_1 \times x_1^{-1}) \times (x_2 \times x_2^{-1}) \ldots \left(x_{\left(\frac{p-3}{2}\right)} x^{-1}_{\left(\frac{p-3}{2}\right)}\right) \times (p-1).$$

Working modulo p, we have

$$\begin{aligned}(p-1)! &= 1 \times (2 \times 2^{-1}) \times (3 \times 3^{-1}) \ldots \left(\left(\frac{p-1}{2} \right) \left(\frac{p-1}{2} \right)^{-1} \right) \times (p-1) \\ &\equiv 1 \times 1 \times 1 \ldots 1 \times (p-1) \pmod{p} \\ &\equiv (p-1) \pmod{p} \\ &\equiv -1 \pmod{p}\end{aligned}$$

as required.

□

Example 8.18. Arrange the integers $2, 3, \ldots, 11$ into pairs $(a \times b)$ satisfying $ab \equiv 1 \pmod{13}$.

Solution: We have

$$(2 \times 7)(3 \times 9)(4 \times 10)(5 \times 8)(6 \times 11).$$

Example 8.19. Find the principal remainder when 15! is divided by 17.

We use Wilson's Theorem: $16! = 16 \times 15! \equiv -1 \pmod{17}$. It follows that $15! \equiv (-1)(16)^{-1} \pmod{17}$. Since 16 is its own inverse in $\mathbb{Z}_{17}^{\times}$. It follows that $15! \equiv -16 \pmod{17}$; $15! \equiv 1 \pmod{17}$. The principal remainder when $15!$ is divided by 17 is therefore 1.

Example 8.20. Find the inverses of 10, 9 and 8 in $\mathbb{Z}_{11}^{\times}$ and hence find the remainder when 7! is divided by 11.

We note that $10 \equiv -1 \pmod{11}$ and so 10 is its own inverse i $\mathbb{Z}_{11}$.

Now $9 \equiv -2 \pmod{11}$. Therefore

$$9 \times 5 \equiv -10 \pmod{11} \equiv 1 \pmod{11}$$

and so $9^{-1} = 5$

Lastly $8 \equiv -3 \pmod{11}$ and so

$$8 \times -4 \equiv 12 \pmod{11} \equiv 1 \pmod{11}.$$

It follows that $8^{-1} = 7$.

We apply Wilson's Theorem to compute the remainder of 7! when divided by 11. We have:

$$10! = 10 \times 9 \times 8 \times 7! \equiv -1 \pmod{11}.$$

Therefore

$$7! \equiv -(10^{-1} \times 9^{-1} \times 8^{-1}) \pmod{11}.$$

Hence

$$7! \equiv 35 \pmod{11} \equiv 2 \pmod{11}.$$

Example 8.21. Use Wilson's Theorem to find the principal remainder on dividing 51! by 61.

Applying Wilson's Theorem:

$$51! \equiv -(60 \cdot 59 \cdot \ldots \cdot 52)^{-1} \pmod{61}.$$

Now we use the fact that

$$60 \equiv -1 \pmod{61}, 59 \equiv -2 \pmod{61}, \ldots, 52 \equiv -9 \pmod{61}.$$

Therefore

$$60 \cdot 59 \cdot \ldots \cdot 52 \equiv -(9!) \pmod{61}.$$

Now $9! = 7! \times 72$. We decompose $7! = 7 \times 60 \times 12$. Thus

$$7! \equiv -84 \pmod{61} \equiv 38 \pmod{61}.$$

On the other hand $72 \equiv 11 \pmod{61}$. Therefore $9! \equiv 38 \times 11 \pmod{61} \equiv 52 \pmod{61}$.

Now we compute $52^{-1} \in \mathbb{Z}_{61}^{\times}$. We use the fact that $52 \equiv -9 = -3 \times 3 \pmod{61}$. Now $3^{-1} \in \mathbb{Z}_{61}^{\times}$ is -20. Therefore

$$(-9)^{-1} = (-3)^{-1} \times 3^{-1} \equiv 20 \times -20 = 27 \pmod{61}.$$

It follows that $51! \equiv 9! \equiv 27 \pmod{61}$.

It is worth noting that the converse of Wilson's Theorem is also true (it is, in fact, an if and only if statement), that is if $(p-1)! \equiv -1 \pmod{p}$ then p is prime. This is, however, not much use as a primality test!

8.4 Problem Sheet 8

Covers Chapter 8.

Question 8.1

a. Use Euclid's algorithm to find the greatest common divisor of 440 and 189. Then find integers s and t such that $\gcd(440, 189) = 189s + 440t$.

b. Use Euclid's algorithm to find the greatest common divisor of 1343 and 391. Then find integers s and t such that $\gcd(1343, 391) = 1343s + 391t$.

c. Use Euclid's algorithm to find the greatest common divisor of 975 and 121. Then find integers s and t such that $\gcd(975, 121) = 121s + 975t$.

Show Solution 8.1 on P223

Question 8.2

Use your result from Question 8.1 c. to find the inverse of $[121]_{975}$ in $\mathbb{Z}_{975}^{\times}$.

Show Solution 8.2 on P226

Question 8.3

Show that $\mathbb{Z}_{12}^{\times}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and write down an isomorphism between the two groups.

Show Solution 8.3 on P226

Question 8.4

Use Fermat's Little theorem to find the principal remainder on dividing:

a. 5^{25} by 13;

b. 17^{44} by 7;

c. 19^{53} by 11.

Show Solution 8.4 on P227

Question 8.5

Show that $2^{11,213} - 1$ is not divisible by 11.

Show Solution 8.5 on P229

Question 8.6

Find the inverses of 16, 17 and 18 in $\mathbb{Z}_{19}^{\times}$. Use those results, together with Wilson's Theorem, to find the remainder when 15! is divided by 19.

Show Solution 8.6 on P230

Question 8.7

Let p be a prime except 2 and 5. Deduce from Fermat's Little Theorem that there is a multiple of p, all of whose digits in decimal notation are 9's.

[Example: $142857 \times 7 = 999999$.]

Show Solution 8.7 on P231

Question 8.8

Consider the set of Hilbert Numbers, $\mathbb{S} = \{n \in \mathbb{N} \,|\, n \equiv 1 \pmod 4\}$. This is the set of all integers that are of the form $4k + 1$, where $k \in \mathbb{N}$. Find the first five 'primes' in this set (called Hilbert Primes). What is the smallest number in $\mathbb{S}$ that does not have a unique factorisation in Hilbert Primes?

Show Solution 8.8 on P232

Part II

Other algebraic structures

Chapter 9

Rings and Fields

So far we have restricted our attention to the algebraic structure known as a group. In this final chapter of our introduction to Abstract Algebra we shall consider, albeit very briefly, algebraic structures other than groups, in particular rings, integral domains, and fields. This will give you a flavour of what to expect if you decide to go for the third-year optional module 'Linear Algebra and Rings'.

9.1 Rings

In certain respects rings will probably seem more intuitive than groups since you have been using rings, and closely related structures, in your mathematical studies since primary school. On the other hand, though, the study of rings and fields is more complicated than the study of groups by virtue of the fact that we are now dealing with sets on which we are defining two binary operations, which we generally label addition and multiplication. Although we shall only be taking a cursory glance at these structures we shall be adopting an axiomatic approach, so we begin with a definition.

Definition 9.1 (Ring)**.** A *ring* is a triple consisting of a non-empty set R equipped with two binary operations that we denote $+$ and $\times$, such that the following are satisfied.

R1: For all $a, b \in R$, $a + b \in R$ *(closure under $+$)*.

R2: For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$ *($+$ is associative on R)*.

R3: There exists 0_R such that, $\forall\, a \in R, a + 0_R = 0_R + a = a$ *($+$ has an identity)*.

R4: For all $a \in R$, $\exists\, -a \in R$ such that $a + (-a) = (-a) + a = 0_R$ *(inverses under $+$)*.

R5: For all $a, b \in R$, $a + b = b + a$ *($+$ is commutative on R)*.

R6: For all $a, b \in R$, $ab \in R$ *(closure under $\times$)*.

R7: For all $a, b, c \in R$, $((ab)c = a(bc)$ *($\times$* is associative on R).

R8: For all $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ *(distributive laws)*.

Strictly speaking we should denote a ring as $(R, +, \times)$ but, similarly to groups, we shall often simply refer to a ring as R.

Note that the above definition can be summed up as: $(R, +, \times)$ is a ring if and only if $(R, +)$ is an abelian group which, along with the binary operation $\times$, satisfies **R6**-**R8**.

Note, also, that whilst the axioms demand that the additive operation is commutative for any ring, there is no such requirement for the multiplicative operation. In the case where the ring R has $ab = ba\ \forall\, a, b \in R$ we say that R is a *commutative ring*.

Example 9.1. The following are rings:

$$\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_n, \mathbb{R}_{2\times 2}.$$

The natural numbers do not form a ring as $(\mathbb{N}, +)$ is not a group (it is not closed under inverses).

The following should be very familiar to everyone.

Theorem 9.1. *If R is a ring with additive identity 0_R then, for any $a, b \in R$, we have*

i. $0_R a = a0_R = 0_R$,

ii. $a(-b) = (-a)b = -(ab)$,

iii. $(-a)(-b) = ab$.

Proof.

We take each in turn.

i. We have

$$0_R a = (0_R + 0_R)a = 0_R a + 0_R a.$$

By cancellation ($(R, +)$ is a group) we deduce that $0_R a = 0_R$. A similar argument demonstrates that $a0_R = 0_R$.

ii. It suffices to show that $ab + a(-b) = ab + (-a)b = 0_R$ since $(\mathbb{R}, +)$ is an abelian group and inverses are unique. We have:

$$ab + a(-b) = a(b + (-b)) = a0_R = 0_R$$

where the last equality follows from i.. One can similarly show that $ab + (-a)b = 0_R$.

iii. We have by ii. that $-(a(-b)) = (-a)(-b)$. Again by ii., $a(-b) = -(ab)$. Therefore,

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

using the fact that $-(-(ab)) = ab$ since $(\mathbb{R}, +)$ is a group.

□

9.1.1 Identity Elements

An identity element in a ring, R, is a *multiplicative identity*. Hence, an identity element $1_R \in R$ is such that $a1_R = 1_R a = a$ for all $a \in R$. We ***assume that all of the rings that we encounter in this chapter have multiplicative identities***. A ring with an identity element is sometimes referred to as a *ring with a one*.

9.1.2 Subrings

The concept of a subring is the same, in principle, as the concept of a subgroup. A subset of a ring R forms a subring of R if and only if it is a ring in its own right. As with groups, we have tests for whether or not a subset of R forms a subring and that is the subject of the following theorem.

Let R be a ring and let $S \subseteq R$. Then S is a subring of R if and only if the three conditions below are satisfied:

i. S has an identity element;

ii. $a, b \in S \Rightarrow a - b \in S$;

iii. $a, b \in S \Rightarrow ab \in S$

Proof. Let R be a ring and let S be a subset of R.

($\Rightarrow$) First we show that if S is a subring of R then the three conditions hold.

i. As S is a subring then $1_S \in S$ by definition (all our rings have a one).

ii. Now let $a, b \in S$. Since S is a ring it must be closed under addition. Further there is an additive inverse for b in S (**R4**) and since additive inverses are unique in R this inverse is the same as $-b$ in R. Hence $a - b = a + (-b) \in S$.

iii. Similarly, S is closed under multiplication.

($\Leftarrow$) Next we show that if S satisfies the three enumerated conditions then it is a subring of R, that is, S is a ring in itself with the operations on S being defined as the operations on R.

By i. S is non-empty.

Since S is non-empty, let $a \in S$. By ii., $a - a \in S$ and so $0_R \in S$. We claim that 0_R is an additive identity for S. For any $s \in S$, we have $0_R + s = s$, since $s \in R$ and since 0_R is the additive identity in R. Thus 0_R is an additive identity for S.

Let $a \in S$. Then, by ii. we have $0_S - a \in S$. But $0_S - a = 0_S + (-a)$, where $-a$ is the additive inverse of a in R. So $-a \in S$ and $-a$ is an additive inverse for a in S.

Let $a, b \in S$. Then $-b \in S$ and $-(-b) = b$, since if $-b$ is an additive inverse for b, then b is an additive inverse for $-b$. Thus, $a + b = a - (-b) \in S$, by ii., so S is closed under addition.

Let $a, b \in S$. Then $a + b \in S$ as S is closed under addition and, since $a, b \in R$, we have $a + b = b + a$ by commutativity of addition in R.

Let $a, b, c \in S$. Then, since $a, b, c \in R$, we have that $a + (b + c) = (a + b) + c$ and closure ensures that these sums are in S.

Let $a, b, c \in S$. Since $a, b, c \in R$ then $a(bc) = (ab)c$ in R and since S is closed under multiplication then $a(bc) = (ab)c$ in S.

By assumption S has a multiplicative identity 1_S. □

Note that this theorem ensures that in any ring R, both $\{0_R\}$ and R itself are subrings of R.

> **Caution**
>
> Let R be a ring and S be a subring of R. Then it is not necessarily the case that $1_S = 1_R$.
>
> For example Let $R = \mathbb{Z}$. Then $S = \{0\}$ is a subring of R however $1_S = 0 \neq 1 = 1_R$.

Let R be a ring. The *centre* of R is denoted and defined by

$$Z(R) = \{a \in R \mid ab = ba \forall\, b \in R\}.$$

Prove that $Z(R)$ is a subring of R.

Solution:

First observe that $Z(R)$ is non-empty since it contains 1_R. Note that 1_R is therefore also the identity element of $Z(R)$.

Let $a, b \in Z(R)$ and $r \in R$. Then,

$$(a - b)r = ar - br = ra - rb = r(a - b)$$

and

$$(abr) = a(br) = (ar)b = r(ab).$$

Therefore $(a - b), ab \in Z(R)$ as well. We conclude that $Z(R)$ is a subring of R.

It is important to be careful when considering the identity element in a subring given that there are two binary operations to take into account. Recall that the identity element in a ring is the *multiplicative* identity; the definition of a ring takes care of the additive identity 0_R. We know that $S = (\{0_R\}, +, \times)$ is a subring of R, but does it have a multiplicative identity?

Unlike groups, the identity in a subring does not have to be the same as the identity in the ring itself.

Let $R = \mathbb{Z}_6$. The identity element in 1 since for all $a \in \mathbb{Z}_6$, $1a = a1 = 1$.

Now take $S = \{0, 2, 4\}$. Then S is a subring of R (this is an exercise). However, the identity element is 4 since

$$\begin{aligned} 4 \times 0 &= 0 \\ 4 \times 2 &= 2 \\ 4 \times 4 &= 4. \end{aligned}$$

9.1.3 Ring Homomorphisms

Definition 9.2 (Ring Homomorphism)**.** Let R_1 and R_2 be rings and let $\theta : R_1 \to R_2$ be a mapping. Then θ is a *ring homomorphism* if, for all $a, b \in R_1$

$$\theta(a + b) = \theta(a) + \theta(b)$$

and

$$\theta(ab) = \theta(a)\theta(b).$$

So, the definition is analogous to that for groups save that we have to consider both binary operations. Note that the first condition is simply the statement that θ is a homomorphism mapping from the abelian group $(R_1, +)$ to the abelian group $(R_2, +)$. The second condition requires that θ relates the multiplicative structures in the same way.

Let R_1 and R_2 be rings and let $\theta : R_1 \to R_2$ be a ring homomorphism. Then,

i. $\theta(0_{R_1}) = 0_{R_2}$,
ii. $\theta(-x) = -\theta(x)$ for all $x \in R_1$.

Proof.

i. We have

$$\theta(0_{R_1}) = \theta(0_{R_1} + 0_{R_1}) = \theta(0_{R_1}) + \theta(0_{R_1}).$$

Subtracting $\theta(0_{R_1})$ from both sides, we have:

$$\theta_{0_{R_1}} = 0_{R_2}.$$

ii. We have

$$0_{R_2} = \theta(0_{R_1}) = \theta(x + (-x)) = \theta(x) + \theta(-x).$$

Using the fact that $(R_2, +)$ is a group (and so inverses are unique) we conclude that $\theta(-x) = -\theta(x)$ as required.

□

Consider the mapping $\theta : \mathbb{Z} \to \mathbb{Z}_n$ where θ is defined by $\theta(a)$ is the principal remainder on dividing a by n for all $a \in \mathbb{Z}$. This is a ring homomorphism.

Let $a, b \in \mathbb{Z}$. Let $0 \leq r_1, r_2 \leq n$ and $q_1, q_2 \in \mathbb{Z}$ such that $a = q_1 n + r_1$ and $a_2 = q_2 n + r_2$. Notice that r_1 and r_2 are the principal remainders of a and b (respectively) upon dividing by n.

Observe that

$$a + b = (q_1 + q_2)n + (r_1 + r_2)$$

and

$$ab = (q_1 q_2 n + q_1 r_2 + q_2 r_1)n + r_1 r_2.$$

We can find $s, t \in \{0, 1, \ldots, n-1\}$ and $u, v \in \mathbb{Z}$ such that $r_1 + r_2 = un + s$ and $r_1 r_2 = vn + t$. Notice that the principal remainders of $a+b$ and ab upon dividing by n are s and t respectively. Furthermore, in $\mathbb{Z}_n$ we have $r_1 + r_2 = s$ and $r_1 r_2 = t$. Therefore,

$$\theta(a + b) = s = \theta(a) + \theta(b)$$

and

$$\theta(ab) = t = \theta(a)\theta(b).$$

As we did for group homomorphisms, we can define the *kernel* of a ring homomorphism:

Definition 9.3 (Kernel)**.** Let R_1 and R_2 be rings and let $\theta : R_1 \to R_2$ be a ring homomorphism. The *kernel* of θ is the set denoted and defined by

$$\ker(\theta) = \{x \in R_1 \mid \theta(x) = 0_{R_2}\}.$$

Note here that it is the set of elements of R_1 that map to the *additive identity* in R_2. As with groups, an *isomorphism* is a bijective homomorphism. Where the ring isomorphism maps from a set to itself we refer to this as an *automorphism*.

9.2 Integral Domains

Definition 9.4 (Divisor of Zero)**.** Let R be a ring with a one and let $x \in R$ be non-zero. Then x is a *divisor of zero* in R if there exists $y \in R \backslash \{0_R\}$ such that $xy = 0_R$.

- $\mathbb{R}$ is a ring with no zero divisors.

- $R = \mathbb{R}_{2\times 2}$ is a ring with zero divisors. For example let $x, y \in \mathbb{R}\backslash\{0\}$. Then

$$A = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix}$$

  are nonzero elements of $\mathbb{R}_{2\times 2}$. However

$$AB = 0_R = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

We now make the following definition:

Definition 9.5 (Integral Domain)**.** An *integral domain* is a nonzero commutative ring with a one in which there are no divisors of zero.

It follows from this definition that in an integral domain R we have

$$xy = 0_R \Rightarrow x = 0_R \text{ or } y = 0_R.$$

- $\mathbb{Z}_{12}$ is a ring but it is not an integral domain For instance

$$2 \times 6 = 0$$

  but $2 \neq 0 \neq 6$.
- Notice that $\mathbb{Z}_p$ is an integral domain for any prime p.

Theorem 9.2. *In the ring $\mathbb{Z}_n$ the divisors of zero are precisely those non-zero elements that are not relatively prime to n.*

Proof.

Let $r \in \mathbb{Z}_n$ be a nonzero element and suppose that $d = \gcd(m, n) \neq 1$. Let $k, l \in \mathbb{Z}$ be such that $m = dk$ and $n = dl$. Thus, $lm = ldk = nk$. It follows that $lm \equiv 0 \pmod{n}$. Notice that $0 < l < n$ (since $1 < d$) and so m is a divisor of 0 in $\mathbb{Z}_n$.

On the other hand, suppose that $r \in \mathbb{Z}_n$ is a zero divisor. By assumption $r \neq 0$ and there exist some $s \neq 0$ such that $sr \equiv 0 \pmod{n}$. This means there is a $q \in \mathbb{Z}$ such that $sr = qn$. If r and n are relatively prime, then $n|s$ since $n|sr$ by Corollary 8.3. It follows that $s = 0$ which is a contradiction. We conclude that n and r are not relatively prime.

□

Corollary 9.1. *If p is prime then $\mathbb{Z}_p$ has no divisors of zero.*

Proof. This follows directly from Theorem 9.2. □

9.3 Division Rings

In a ring there is no requirement for any element to have a multiplicative inverse, so if a ring does have multiplicative inverses this makes the ring special. Recall from group theory that when we considered $\mathbb{Z}_n$ under multiplication we were unable to form a group unless we ejected all of the elements not relatively prime to n. This is tantamount to discarding all of the elements that do not have a multiplicative inverse in the set

Definition 9.6 (Unit)**.** Let R be a ring. If $a \in R$ has a multiplicative inverse in R, then a is said to be a *unit* in R.

We can collect together such units from a given ring, place them in a set and we obtain a group under multiplication.

- The units of $\mathbb{Z}$ are $\{-1, 1\}$ — this forms a group isomorphic to $\mathbb{Z}_2$.
- The units of $\mathbb{R}_{2\times 2}$ is precisely the group $GL(2, \mathbb{R})$.

Definition 9.7 (Division Ring)**.** A *division ring* is a (not necessarily commutative) ring in which every non-zero element is a unit.

Hence, for all $a \in R$, $a \neq 0$, there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1_R$.

Let R be a division ring. Then $(R\backslash\{0_R\}, \times)$ is a group.

Let $\mathbb{H} \subseteq \mathbb{C}_{2\times 2}$ be the set

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : z, w \in \mathbb{C} \right\}.$$

We show that $\mathbb{H}$ is a subring of $\mathbb{C}_{2\times 2}$.

Note that $\mathbb{H}$ is non-empty, in particular it contains the identity matrix I_2 (take $z = 1$ and $w = 0$).

Let

$$A = \begin{pmatrix} z_1 & w_1 \\ -\overline{w}_1 & \overline{z}_1 \end{pmatrix}, B = \begin{pmatrix} z_2 & w_2 \\ -\overline{w}_2 & \overline{z}_2 \end{pmatrix} \in \mathbb{H}.$$

Then,

$$\begin{aligned} A - B &= \begin{pmatrix} z_1 - z_2 & w_1 - w_2 \\ -\overline{w}_1 + \overline{w}_2 & \overline{z}_1 - \overline{z}_2 \end{pmatrix} \\ &= \begin{pmatrix} z_1 - z_2 & w_1 - w_2 \\ -(\overline{w_1 - w_2}) & \overline{z_1 - z_2} \end{pmatrix} \in \mathbb{H} \end{aligned}$$

and

$$\begin{aligned} AB &= \begin{pmatrix} z_1 z_2 - w_1 \overline{w}_2 & z_1 w_2 + w_1 \overline{z}_2 \\ -(\overline{w}_1 z_2 + \overline{z}_1 \overline{w_2}) & -\overline{w}_1 w_2 + \overline{z}_1 \overline{z}_2 \end{pmatrix} \\ &= \begin{pmatrix} z_1 z_2 - w_1 \overline{w}_2 & z_1 w_2 + w_1 \overline{z}_2 \\ -(\overline{z_1 w_2 + w_1 \overline{z}_2}) & \overline{z_1 z_2 - w_1 \overline{w}_2} \end{pmatrix} \in \mathbb{H}. \end{aligned}$$

We now show that $\mathbb{H}$ is a division ring. Let

$$A = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \in \mathbb{H}$$

be a non-zero element. Note that A^{-1} must be precisely the inverse of $A \in \mathbb{C}_{2\times 2}$ since I_2 is the identity element of H. Therefore, to show that H is a division ring, it suffices to show that $A^{-1} \in H$. First we determine if A is invertible in $\mathbb{C}_{2\times 2}$. We compute

$$\det A = z\overline{z} + w\overline{w} = |z|^2 + |w|^2.$$

Since A is nonzero, then one of z or w is nonzero and so $|z|^2 + |w|^2 \neq 0$. Therefore A has a multiplicative inverse $A^{-1} \in \mathbb{C}_{2\times 2}$ given by

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \overline{z} & -w \\ \overline{w} & z \end{pmatrix}.$$

Since $\det(A) \in \mathbb{R}$, it follows that $\left(\overline{\frac{1}{\det A}}\right) = \frac{1}{\det A}$ and so $A^{-1} \in \mathbb{H}$.

Every non-zero element of $\mathbb{H}$ is a unit and so $\mathbb{H}$ is a division ring.

Where have we seen something similar to this in our study of groups? Recall that we were able to represent complex numbers as matrices in the following way:

Let

$$M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 \neq 0 \right\}.$$

We found that $(\mathbb{C}\backslash\{0\}, \times) \cong (M, \times)$ with an isomorphism $\theta : M \to \mathbb{C}\backslash\{0\}$ by

$$\theta\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + ib.$$

In a similar way we can represent quaternions as matrices. Quaternions were developed by the Irish mathematician Hamilton to solve problems in mechanics in three-dimensional space. They are an 'extension' of the complex numbers in the following way:

Let i, j, k satisfy the rules $i^2 = j^2 = k^2 = ijk = -1$, thus:

$$ij = k = -ji \tag{9.1}$$

$$jk = i = -kj \tag{9.2}$$

$$ki = j = -ik. \tag{9.3}$$

Set $\widehat{\mathbb{H}} := \{a + bi + cj + dk : a, b, c, d, \in \mathbb{R}\}$. Then $\widehat{\mathbb{H}}$ is a division ring.

The quaternions form a ring $\widehat{\mathbb{H}}$ and the group Q_8 lives inside that ring. In a similar way to our representation of complex numbers as matrices with real entries, we can represent quaternions as matrices with complex entries:

The ring $\widehat{\mathbb{H}}$ is isomorphic to the ring

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : w, z \in \mathbb{C} \right\}.$$

An isomorphism is the map $\theta : \widehat{\mathbb{H}} \to \mathbb{H}$ where

$$\theta(a + bi + cj + dk) = \begin{pmatrix} a + bi & c + di \\ -(c - di) & a - bi \end{pmatrix}.$$

Notice that

$$\begin{aligned}
\theta(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -\theta(-1) \\
\theta(i) &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = -\theta(-i) \\
\theta(j) &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -\theta(-j) \\
\theta(k) &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = -\theta(-k)
\end{aligned}$$

Thus we have a representation of the quarternion group Q_8 as a subgroup of $GL(2, \mathbb{C})$ (invertible 2-by-2 matrices over the complex numbers).

Then, as we have seen, the set of all such matrices forms a subring of the ring of all 2×2 matrices with entries from $\mathbb{C}$. In fact, it forms a division ring.

9.4 Fields

Consider the previous example. Note that, for example

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \in \mathbb{H}.$$

Now

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$

But

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

So, $\mathbb{H}$ is not commutative under multiplication. We are, though, interested in cases where we do have commutativity; this leads to the following definition:

Definition 9.8 (Field)**.** A field is a commutative division ring.

The rings $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all fields; $\mathbb{Z}$ is not a fields (it is not a division ring).

Let F be a field. Then $(F\backslash\{0_R\}, \times)$ is an abelian group. Thus a ring R is a field if $(R, +)$ and $(R\backslash 0_R, \times)$ are both abelian groups.

9.4.1 Properties of Fields

Every field is an integral domain.

Proof.

Let F be a field. To show that F is a field it suffices to show that it has no zero divisors. Let $x \in F\backslash\{0_F\}$ and suppose there is a $y \in F$ such that that $xy = 0_F$. Since F is a field, and x is nonzero x has a multiplicative inverse $x^{-1} \in F$. Then,

$$y = 1_F y = (x^{-1}x)y = (x^{-1})0_F = 0_F.$$

Thus F has no zero divisors: if a product $xy = 0$, one of x or y must be zero.

□

Definition 9.9 (Characteristic)**.** Let R be an integral domain. The *characteristic* of R, denoted $\text{char}\,(R)$, is the period of 1_R in the group $(R, +)$. If 1_R has infinite period in the group $(R, +)$ then we define $\text{char}\,(R) = 0$.

- $\text{char}\,(\mathbb{R}) = 0$;
- $\text{char}\,(\mathbb{Z}_n) = n$;
- $\text{char}\,(\mathbb{Q}) = 0$.

Let R be an integral domain. Then $\text{char}\,(R)$ is either zero or a prime.

Proof.

Suppose $\text{char}\,(R) = m \neq 0$. Let $k, l \in \mathbb{N}$ such that $kl = m$. For a positive integer a write $a1_R$ for the sum $\sum_{i=1}^{a} 1_R$. Then

$$m1 = kl(1_R) = (k1_r)(l1_r) = 0_R.$$

Since R is an integral domain, it must be that either $k1_R = 0_R$ or $l1_r = 0_R$. Since $m = \text{char}\ R$ and $1 \leq k, l \leq m$, we conclude that either $k = m$ or $l = m$. Thus m is divisible only by itself and 1 — m is prime.

□

This leads to the conclusion that any field has a subfield that is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$. We find that any field with characteristic p has a copy of $\mathbb{Z}_p$ 'inside it', whilst any field with characteristic 0 has a copy of $\mathbb{Q}$ 'inside it'.

9.4.2 Field Extensions

Consider the polynomial $x^2 - 2$ in $\mathbb{Q}$. What happens if we try to factorise it?

$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$. However, $\sqrt{2} \notin \mathbb{Q}$ so $x^2 - 2$ is not factorisable in $\mathbb{Q}$. One potential way to resolve this is to extend $\mathbb{Q}$ to include all the irrational numbers.

This 'field extension' gives us the set of real numbers, $\mathbb{R}$. In a similar way, consider the polynomial $x^2 + 1$ in $\mathbb{R}$.

$x^2 + 1 = (x + i)(x - i)$. However, $i \notin \mathbb{R}$ so $x^2 + 1$ is not factorisable in $\mathbb{R}$. One potential way to resolve this is to extend $\mathbb{R}$ to include all numbers of the form $a + ib$ where $a, b \in \mathbb{R}$.

Returning to the first example, one obvious question to ask is whether the extension of $\mathbb{Q}$ to the whole of $\mathbb{R}$ is the 'smallest' possible extension that makes $x^2 - 2$ factorisable. The answer is 'no'.

Define a field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. Clearly $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and so $x^2 - 2$ can be

factorised in $\mathbb{Q}(\sqrt{2})$. Notationally we write $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ to indicate that this is an extension of $\mathbb{Q}$.

We can similarly extend $\mathbb{Q}$ in order to factorise say $x^2 - 6$.

> **Aside**
>
> The field $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is a vector space over $\mathbb{Q}$ with basis $(1, \sqrt{2})$.

Note that this extension is a field in its own right (see Problem Set 7) and sits inside $\mathbb{R}$. In fact it is a subfield of $\mathbb{R}$, but it is clearly not all of $\mathbb{R}$.

Such extensions of $\mathbb{Q}$ are known as *algebraic number fields*. We say that $\sqrt{2}$ is an algebraic element in $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$ (and, indeed, in $\mathbb{R} \mid \mathbb{Q}$) as it is a root of the equation $x^2 = 2$. In a similar way, i is an algebraic element in $\mathbb{C} \mid \mathbb{R}$ as it is a root of the equation $x^2 = -1$. On the other hand, e is not an algebraic element in $\mathbb{R} \mid \mathbb{Q}$ since there is no polynomial with rational coefficients that has e as a root.

We are now beginning to stray into the beginnings of Galois theory, a beautiful area of mathematics that explores the connection between group theory and field theory. This tells us why there are general formulae for solving quadratics, cubics and quartics, but not for polynomials of degree five or greater. It also gives us a characterisation of the ratios of lengths that can be constructed using only straightedge and compasses, thus leading to an elegant insight into the theory of constructible regular polygons. In fact it can be argued that the work of Galois, all completed before the age of 21 when he died, saw the birth of Abstract Algebra as a coherent mathematical discipline.

9.5 Problem Sheet 9

Covers Chapter 9.

Question 9.1

a. An element a of a ring R is said to be *idempotent* if $a^2 = a$. Show that a division ring contains exactly two idempotent elements.

b. If every element in a ring R is idempotent, show that any non-zero element $x \in R$ has period 2 in the group $(R, +)$.

c. Show that any ring in which every element is idempotent is necessarily commutative.

Show Solution 9.1 on P232

Question 9.2

Let

$$S = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R} \right\}.$$

Prove that S is a subring of $M_2(\mathbb{R})$.

[Note that the S and $M_2(\mathbb{R})$ each have identity elements but they are not the same]

Show Solution 9.2 on P234

Question 9.3

In the lectures we said that $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$. Prove that $\mathbb{Q}(\sqrt{2})$ is a field.

Show Solution 9.3 on P235

Appendix A

All Solutions

A.1 Chapter 1 solutions

Solution 1.1

Let A be the set $\{x, \{1, x\}, \{3\}, \{\{1, 3\}\}, 3\}$.

- $x \in A$.

  This is true as there is an element of the set A which is x.

- $\{x\} \notin A$.

  This is true. $\{x\}$ is not in A. There is a set in A that does contain x, but it also contains 1. So the *actual* object $\{x\}$ is not in the set A.

- $\{1, x\} \subseteq A$.

  This is false. The object $\{1, x\}$ is an *element* of A , so cannot be a subset of A. However, if we put that object into a set then we do have a subset of A, i.e. $\{\{1, x\}\} \subseteq A$.

- $\{3, \{3\}\} \subseteq A$.

  This is true since this is a set with two elements, namely 3 and $\{3\}$, both of

which are also in A.

- $\{1,3\} \in A$.

  This is false. $\{1,3\}$ is not found in A. Note that $\{\{1,3\}\}$ is not the same thing as $\{1,3\}$.

- $\{\{1,3\}\} \subseteq A$.

  This is false, it is an element of A and not a subset of A.

- $\{\{1,x\}\} \subseteq A$.

  This is true, and that should now be clear from what has gone before.

- $\{1,x\} \notin A$.

  This is false as we have already said that $\{1,x\}$ is in A.

- $\emptyset \subseteq A$.

  This is true since the empty set is always a subset of *any* set.

Return to Question 1.1 on P17

Solution 1.2

Let $J = \{1,2,5,6\}, K = \{3,6,7,8\}, L = \{4,5,7\}, M = \{1,4,6,8\}$ ***and*** $N = \{6,\{8\}\}$.

- $J \cap K = \{6\}$.
- $(K \cap M) \cup L = \{6,8\} \cup L = \{4,5,6,7,8\}$.
- $\mathcal{P}(L) = \{\emptyset,\{4\},\{5\},\{7\},\{4,5\},\{4,7\},\{5,7\},\{4,5,7\}\}$.
- $L \times N = \{(4,6),(4,\{8\}),(5,6),(5,\{8\}),(7,6),(7,\{8\})\}$.
- $\{x+y \mid x \in J, y \in L\} = \{5,6,9,10,7,11,8,12.13\}$.
- $\{x \mid x \in L \times J, x \notin L \times M\} = \{(4,2),(4,5),(5,2),(5,5),(7,2),(7,5)\}$.

Return to Question 1.2 on P18

Solution 1.3

Show that, for any integers a, b and c,

$$a \mid b \text{ and } b \mid c \;\Rightarrow\; a \mid (b+c).$$

$a \mid b \Rightarrow b = ma,\ m \in \mathbb{Z}$ and $b \mid c \Rightarrow c = nb,\ n \in \mathbb{Z}$. Then:

$$\begin{aligned} b + c &= ma + nb \\ &= ma + nma \\ &= a(m + nm) \end{aligned}$$

So, as $(m + nm) \in \mathbb{Z}$, we have that $a \mid (b + c)$.

Is the converse true? No, it is not and it is easy to find a counter-example. Let $a = 3$, $b = 4, c = 2$; then $3 \mid (4 + 2)$ but $3 \nmid 4$ and $3 \nmid 2$.

Return to Question 1.3 on P18

Solution 1.4

Let $m > 0$ be a fixed integer and a, b and c be any integers. Prove that

$$a \equiv b \pmod{m} \;\Rightarrow\; ac \equiv bc \pmod{m}.$$

Is the converse true?

$a \equiv b \pmod{m} \Rightarrow m \mid a - b$. So $m \mid c(a - b) \Rightarrow m \mid ca - cb$ and, hence, $ca \equiv cb \pmod{m}$.

Is the converse true? No, it is not. For example, $20 \equiv 10 \pmod{10}$ but $10 \not\equiv$

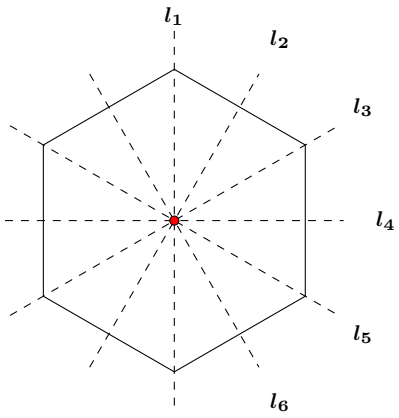
$5 \pmod{10}$.}

Return to Question 1.4 on P19

A.2 Chapter 2 solutions

Solution 2.1

Develop suitable notation and construct an operation table for the symmetries of a regular hexagon, as shown below. For consistency with examples in the lecture notes, let the vertical line of symmetry be denoted l_1 and number the others in a clockwise direction.



For $1 \leq i \leq 5$ we take r_i to be rotation anticlockwise by $\frac{2\pi}{6}$; let s_i be reflection the line l_i. We can draw up a multiplication table as follows:

$\circ$	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
e	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
r_1	r_1	r_2	r_3	r_4	r_5	e	s_6	s_1	s_2	s_3	s_4	s_5
r_2	r_2	r_3	r_4	r_5	e	r_1	s_5	s_6	s_1	s_2	s_3	s_4
r_3	r_3	r_4	r_5	e	r_1	r_2	s_4	s_5	s_6	s_1	s_2	s_3
r_4	r_4	r_5	e	r_1	r_2	r_3	s_3	s_4	s_5	s_6	s_1	s_2
r_5	r_5	e	r_1	r_2	r_3	r_4	s_2	s_3	s_4	s_5	s_6	s_1
s_1	s_1	s_2	s_3	s_4	s_5	s_6	e	r_1	r_2	r_3	r_4	r_5
s_2	s_2	s_3	s_4	s_5	s_6	s_1	r_5	e	r_1	r_2	r_3	r_4
s_3	s_3	s_4	s_5	s_6	s_1	s_2	r_4	r_5	e	r_1	r_2	r_3
s_4	s_4	s_5	s_6	s_1	s_2	s_3	r_3	r_4	r_5	e	r_1	r_2
s_5	s_5	s_6	s_1	s_2	s_3	s_4	r_2	r_3	r_4	r_5	e	r_1
s_6	s_6	s_1	s_2	s_3	s_4	s_5	r_1	r_2	r_3	r_4	r_5	e

Return to Question 2.1 on P37

Solution 2.2

Lemma 2.3 states that if S is a set closed under an associative binary operation, $*$, with identity, e, and if x^{-1} and y^{-1} exist, then $(x*y)^{-1} = y^{-1}*x^{-1}$. Use mathematical induction to prove that this lemma extends to any finite product, that is

$$(x_1 * x_2 * \ldots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \ldots * x_2^{-1} * x_1^{-1}$$

for all natural numbers, n.

Let $P(n)$ be the proposition that $(x_1*x_2*\ldots*x_{n-1}*x_n)^{-1} = x_n^{-1}*x_{n-1}^{-1}*\ldots*x_2^{-1}*x_1^{-1}$.

Base case is $n = 2$ and, by Lemma 2.3, we know that $(x_1 * x_2)^{-1} = x_2^{-1} * x_1^{-1}$. Hence $P(1)$ is true.

We now assume the proposition is true for some $n = k$, say, that is

$$(x_1 * x_2 * \ldots * x_{k-1} * x_k)^{-1} = x_k^{-1} * x_{k-1}^{-1} * \ldots * x_2^{-1} * x_1^{-1}.$$

This is our induction hypothesis.

Then, for $n = k + 1$ we have

$$\begin{aligned}
(x_1 * x_2 * \ldots * x_k * x_{k+1})^{-1} &= ((x_1 * x_2 * \ldots * x_{k-1} * x_k) * x_{k+1})^{-1} && \text{associativity} \\
&= x_{k+1}^{-1} * (x_1 * x_2 * \ldots * x_{k-1} * x_k)^{-1} && \text{Lemma 2.3} \\
&= x_{k+1}^{-1} * x_k^{-1} * \ldots * x_2^{-1} * x_1^{-1} && \text{I.H.}
\end{aligned}$$

So, $P(1)$ is true and if $P(k)$ is true then $P(k+1)$ is true. Hence, by induction, the statement is true for all $n \in \mathbb{N}$.

Return to Question 2.2 on P37

Solution 2.3

A binary operation $*$ is defined on $\mathbb{R}$ by $x * y = xy - 2x - 2y + 6$.

i. Is $\mathbb{R}$ closed under $*$?

ii. Is $*$ associative on $\mathbb{R}$?

iii. Does $\mathbb{R}$ have an identity element w.r.t. $*$?

iv. Does every element of $\mathbb{R}$ have an inverse under $*$?

i. For closure we will need to show that $\forall\, x, y \in \mathbb{R}$, then $x * y \in \mathbb{R}$. We need to use the following facts

- if $a, b \in \mathbb{R}$, then $a + b \in \mathbb{R}$
- if $a, b \in \mathbb{R}$, then $ab \in \mathbb{R}$

- $a \in \mathbb{R}$, then $-a \in \mathbb{R}$

So, $x * y = xy + (-2x) + (-2y) + 6 \in \mathbb{R}$ by the above.

ii. For associativity we need to show that $\forall\, x, y, z \in \mathbb{R}$, then $x * (y * z) = (x * y) * z$. Now

$$\begin{aligned} x * (y * z) &= x * (yz - 2y - 2z + 6) \\ &= x(yz - 2y - 2z + 6) - 2x - 2(yz - 2y - 2z + 6) + 6 \\ &= xyz - 2xy - 2xz + 6x - 2x - 2yz + 4y + 4z - 12 + 6 \\ &= xyz - 2xy - 2xz - 2yz + 4x + 4y + 6z - 2z - 12 + 6 \\ &= xyz - 2xz - 2yz + 6z - 2xy + 4x + 4y - 12 - 2z + 6 \\ &= (xy - 2x - 2y + 6) * z \\ &= (x * y) * z. \end{aligned}$$

The other way to approach this is to compute $x * (y * z)$ and $(x * y) * z$ and show that they produce the same result.

iii. Identity: we need to show that $\exists\, e \in \mathbb{R}$ such that $\forall\, x \in \mathbb{R}$,; $x * e = e * x = x$. Now, $x * e = xe - 2x - 2e + 6$ and

$$\begin{aligned} xe - 2x - 2e + 6 = x \quad &\Leftrightarrow \quad xe - 2e = 3x - 6 \\ &\Leftrightarrow \quad e(x - 2) = 3(x - 2) \end{aligned}$$

and similarly for $e * x = x$. Notice that this is satisfied when $e = 3$ or when $x = 2$. If $x = 2$ then we have $2 * 3 = (2 \times 3) - 4 - 6 + 6 = 2$ (and, similarly, $3 * 2 = 2$). Hence, for this binary operation, $\mathbb{R}$ does have an identity element which is 3.

iv. Inverse: we need to show that $\forall\, x \in \mathbb{R}$,$\exists\, x^{-1} \in \mathbb{R}$ such that $x * x^{-1} =$

$x^{-1} * x = 3$, where, from the above, $e = 3$.

So, consider $x * x^{-1} = 3$. Now

$$\begin{aligned} x * x^{-1} = 3 &\Leftrightarrow xx^{-1} - 2x - 2x^{-1} + 6 = 3 \\ &\Leftrightarrow x^{-1}(x-2) = 2x - 3 \end{aligned}$$

and similarly for $x^{-1} * x = 3$. Clearly this is satisfied whenever x does not equal 2. Then, for $x \neq 2$ we have that $x^{-1} = \frac{2x-3}{x-2}$. Note that if $x = 2$ then this gives $0 = 1$, hence 2^{-1} does not exist. So, all elements of $\mathbb{R}$ **except** 2 have an inverse.

There is an important point to be made here in regard to binary operations. **Do not**, in the above, be fooled into putting e in place of xx^{-1}. The binary operation there was normal multiplication in $\mathbb{R}$ and not $*$.

Return to Question 2.3 on P37

Solution 2.4

A binary operation $*$ is defined on $\mathbb{R}\backslash\{2\}$ by $x * y = xy - 2x - 2y + 6$.

i. Is $\mathbb{R}\backslash\{2\}$ closed under $*$?

ii. Is $*$ associative on $\mathbb{R}\backslash\{2\}$?

iii. Does $\mathbb{R}$ have an identity element w.r.t. $*$?

iv. Does $\mathbb{R}\backslash\{2\}$ have an identity element w.r.t. $*$?

We know from Question 2.3 that ii. iii. and iv. are true. We therefore only need to show i. We prove this by contradiction.

Assume that there exist $x, y \in \mathbb{R}\backslash\{2\}$ such that $x * y = 2$. Then,

$$\begin{aligned} & x * y &&= 2 \\ \Leftrightarrow \quad & xy - 2x - 2y + 6 &&= 2 \\ \Leftrightarrow \quad & x(y-2) &&= 2y - 4 \\ \Leftrightarrow \quad & x &&= \frac{2(y-2)}{y-2}, \quad y \neq 2 \\ \Leftrightarrow \quad & x &&= 2 \end{aligned}$$

But $x \neq 2$ (and, similarly, neither does y) and so closure is not violated.

Hence, $(\mathbb{R}\backslash\{2\}, *)$ forms a group.

Return to Question 2.4 on P38

A.3 Chapter 3 solutions

Solution 3.1

Decide whether or not the following are groups:

i. the set $S = \{1, 2, 3, 4, 5\}$ with operation $*$ defined by the following operation table

$*$	1	2	3	4	5
1	2	1	5	3	4
2	1	2	3	4	5
3	4	3	2	5	1
4	5	4	1	2	3
5	3	5	4	1	2

ii. the power set of a non-empty set A, with respect to set intersection;

iii. the set $S = \{a, b, c, d, e, f\}$ consisting of the six functions defined by

$$a(x) = x,\ b(x) = 1 - x,\ c(x) = \frac{1}{x},\ d(x) = \frac{x-1}{x},\ e(x) = \frac{x}{x-1},\ f(x) = \frac{1}{1-x},$$

together with the binary operation of function composition. Draw up an operation table.

i. Clearly S is closed under $*$ as only elements of S appear in the body of the table. 2 is the identity, since row 2 and column 2 are the same as the index row and column. Furthermore, every element must have an inverse in the set since the identity (i.e. 2) appears exactly once in each row and each column. So, is the binary operation associative? Consider, for example, the following:

$$\begin{aligned}(3*4)*1 &= 5*1 = 3\\ 3*(4*1) &= 3*5 = 1\end{aligned}$$

Hence the binary operation is not associative, so $(S,*)$ is not a group.

ii. Recall that the power set of a non-empty set, A say, is the *set of all subsets* of A. So, for example, the power set of S in the question above is

$$\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \ldots, \{1,2\}, \ldots, \{2,3,4,5\}, S\}$$

We now need to examine each of the group axioms in turn.

a. **Closure**:

quite clearly, each of the subsets of A can only contain elements of A. As the intersection of any two subsets of A must result in another subset of A and since $\mathcal{P}(A)$ contains *all* of the subsets of A, then A must be closed under set intersection.

b. **Associativity:**

set intersection is an associative operation (see Algebra).

c. **Identity:**

We need a subset of A (that is, an element of $\mathcal{P}(A)$), let's call it I such

that, for *any* subset of A, say X,

$$X \cap I = I \cap X = X.$$

The only subset of A (and, hence, element of $\mathcal{P}(A)$) that satisfies this condition is A itself, so A is the identity with respect to set intersection. For an example of how this works, consider the set S in part (i) above. Consider an element of $\mathcal{P}(S)$, lets say $\{1, 3, 4\}$. Clearly, if we intersect this with S itself we get

$$\{1, 3, 4\} \cap \{1, 2, 3, 4, 5\} = \{1, 2, 3, 4, 5\} \cap \{1, 3, 4\} = \{1, 3, 4\}.$$

d. **Inverse:** given that the identity, I, is the set A itself, we need to ask whether or not every subset of A, that is $X \in \mathcal{P}(A)$ has an inverse, X^{-1} such that

$$X \cap X^{-1} = X^{-1} \cap X = I = A$$

A moments thought should tell you that the only element of $\mathcal{P}(A)$ that satisfies this condition is A itself and, hence, not every element of $\mathcal{P}(A)$ has an inverse in $\mathcal{P}(A)$.

So, this does not form a group.

iii. Here we have a set of real-valued functions under function composition. It is important to remember how we compose functions. If f and g are functions then we denote f acting on g as $f \circ g$ (a function in itself), taking special note of the fact that, when applied to an argument, g acts before x. So, $(f \circ g)(x) = f(g(x))$. The easiest way, in this case, to check for closure is to draw up an operation table. here are a few worked examples:

- $(a \circ c)(x) = a(c(x)) = a\left(\frac{1}{x}\right) = \frac{1}{x} = c(x)$. This should come as no

surprise as a is clearly the identity function. So, the first stage of completing the table is easy:

$\circ$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b					
c	c					
d	d					
e	e					
f	f					

- $(b \circ b)(x) = b(b(x)) = b(1-x) = 1-(1-x) = x = a(x)$. So, b is self-inverse.
- $(d \circ e)(x) = d(e(x)) = d\left(\dfrac{x}{x-1}\right) = \dfrac{\frac{x}{x-1} - 1}{\frac{x}{x-1}} = \dfrac{\frac{1}{x-1}}{\frac{x}{x-1}} = \dfrac{1}{x} = c(x)$.

Carrying on in a similar manner we can complete the table as follows:

$\circ$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	d	c	f	e
c	c	f	a	e	d	b
d	d	e	b	f	c	a
e	e	d	f	b	a	c
f	f	c	e	a	b	d

(You should try some more examples yourselves until you are confident with how to combine the functions). It is now clear that the set is closed under function composition since the body of the table contains no elements that are not in the set S. We know that function composition is an associative operation and it has already been said that there is clearly an identity element, namely a. Finally, as the identity appears exactly once in each row and column, we know that each

element of the set has an inverse. Hence we can conclude that $(S, \circ)$ is a group. It may not have escaped your notice that the 'structure' of the table is the same as the 'structure' of the operation table for D_3, the symmetries of an equilateral triangle (what do we mean by that?). This is no coincidence, as we shall see later.

Return to Question 3.1 on P60

Solution 3.2

Let G be the symmetry group of a regular hexagon. Using the Cayley table below

$\circ$	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
e	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
r_1	r_1	r_2	r_3	r_4	r_5	e	s_6	s_1	s_2	s_3	s_4	s_5
r_2	r_2	r_3	r_4	r_5	e	r_1	s_5	s_6	s_1	s_2	s_3	s_4
r_3	r_3	r_4	r_5	e	r_1	r_2	s_4	s_5	s_6	s_1	s_2	s_3
r_4	r_4	r_5	e	r_1	r_2	r_3	s_3	s_4	s_5	s_6	s_1	s_2
r_5	r_5	e	r_1	r_2	r_3	r_4	s_2	s_3	s_4	s_5	s_6	s_1
s_1	s_1	s_2	s_3	s_4	s_5	s_6	e	r_1	r_2	r_3	r_4	r_5
s_2	s_2	s_3	s_4	s_5	s_6	s_1	r_5	e	r_1	r_2	r_3	r_4
s_3	s_3	s_4	s_5	s_6	s_1	s_2	r_4	r_5	e	r_1	r_2	r_3
s_4	s_4	s_5	s_6	s_1	s_2	s_3	r_3	r_4	r_5	e	r_1	r_2
s_5	s_5	s_6	s_1	s_2	s_3	s_4	r_2	r_3	r_4	r_5	e	r_1
s_6	s_6	s_1	s_2	s_3	s_4	s_5	r_1	r_2	r_3	r_4	r_5	e

i. find (a) a subgroup of order 2, (b) a subgroup of order 3, (c) a subgroup of order 4, and (d) a subgroup of order 6.

ii. Does G contain any subgroups which are not of order 2, 3, 4 or 6?

The subgroups are given, in Cayley table form, below. Be sure that you are satisfied that each one is, in itself, a group (which it *has to be* to be a subgroup).

i. (a) one subgroup of order 2 is

$\circ$	e	s_2
e	e	s_2
s_2	s_2	e

Note that the identity with one reflection will always form a subgroup of order 2. There is one more; make sure you can spot it.

(b) there is only one subgroup of order 3 which is

$\circ$	e	r_2	r_4
e	e	r_2	r_4
r_2	r_2	r_4	e
r_4	r_4	e	r_2

(c) one subgroup of order 4 is

$\circ$	e	r_3	s_2	s_5
e	e	r_3	s_2	s_5
r_3	r_3	e	s_5	s_2
s_2	s_2	s_5	e	r_3
s_5	s_5	s_2	r_3	e

Any more? Note that this is an abelian subgroup of an non-abelian group.

(d) the obvious subgroup of order 6 is

$\circ$	e	r_1	r_2	r_3	r_4	r_5
e	e	r_1	r_2	r_3	r_4	r_5
r_1	r_1	r_2	r_3	r_4	r_5	e
r_2	r_2	r_3	r_4	r_5	e	r_1
r_3	r_3	r_4	r_5	e	r_1	r_2
r_4	r_4	r_5	e	r_1	r_2	r_3
r_5	r_5	e	r_1	r_2	r_3	r_4

ii. The answer is 'Yes'. The trivial subgroup $(\{e\}), \circ)$ has order 1 and the improper subgroup, that is the group itself, has order 12.

Return to Question 3.2 on P61

Solution 3.3

For the sets $\{0, 1, 2, 3, 4\}$ and $\{0, 1, 2, 3, 4, 5\}$ construct operation tables under multiplication modulo 5 and multiplication modulo 6, respectively. Do either of these form groups? Make a general conjecture concerning $\{0, 1, 2, \ldots, n-1\}$ under multiplication modulo n

Now repeat the process with 0 removed from each set. How does this affect the result. Make a further general conjecture concerning $\{1, 2, \ldots, n-1\}$ under multiplication modulo n (you may need to try a few more examples to back up your idea - it's not immediately obvious what is going on).

For those instances that still do not form groups, can you generate a group by removing further elements from the set. If so, which ones? Is there a pattern? Try different examples of your own until you can make a further general conjecture.

The tables are

$\otimes_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

and

$\otimes_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

A cursory glance at the tables reveals that these systems cannot be groups since in neither case does zero have an inverse in the set (but we know this generally where we have 0 in a set and the operation is multiplication of numbers). So what happens if we remove 0 from the set? The operation tables then become:

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

and

$\otimes_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

.

In the first case the set $\{1, 2, 3, 4\}$ now forms a group under multiplication modulo 5 (check it). In the second case, though, we still do not have a group since the set is clearly not closed under the operation. So, can we make a general conjecture about the set $\{1, 2, \ldots, n-1\}$ under multiplication modulo n? If you try a few more cases it soon becomes obvious that when n is prime the removal of 0 from the set is sufficient for the system to then form a group. But what about the case where n is not prime? Well, notice that in removing the 0 from the set where n is prime is equivalent to removing the only element that does not have an inverse in the set. Now, in the second case, none of 0, 2, 3, 4 have inverses in the set, so what happens if we remove these elements? We get the following:

$\otimes_6$	1	5
1	1	5
5	5	1

.

This is now a group.

We now conjecture that removing from the set $\{1, 2, \ldots, n-1\}$ all of the elements which do not have inverses in the set, under multiplication modulo n, yields a group. In fact this is true for all n (you may wish to try this for $\{1, 2, \ldots, 7\}$ under multiplication modulo 8). So, what is the relationship between the elements removed and the value of n? From the examples so far it seems clear that we always have to remove 0, but

never 1. Why should this be? The answer (if you haven't figured it out) will come in Chapter 8.

Return to Question 3.3 on P61

Solution 3.4

Giving a suitable notation, draw up the operation table for the symmetries of a rectangle. Do these form a group under function composition? If so, is the group abelian? Is it cyclic?

First, we need to decide what are the symmetries of a rectangle. Playing around with that sheet of A4 paper on your desk should convince you that, apart from the identity, the only symmetries are a 180 degree rotation and the reflections in the horizontal and vertical axes. Using our usual notation, where we measure angles in radians and let the vertical line of reflection be l_1 and the horizontal line be l_2, the set of symmetries is $S = \{e, r_\pi, s_1, s_2\}$. The operation table is:

$\circ$	e	r_π	s_1	s_2
e	e	r_π	s_1	s_2
r_π	r_π	e	s_2	s_1
s_1	s_1	s_2	e	r_π
s_2	s_2	s_1	r_π	e

Clearly the table demonstrates that the group axioms hold:

- the set is *closed* under function composition as the body of the table contains only elements in the set;
- we know that function composition is associative;
- the *identity* is e as the e row and column repeat the index row and column;
- every element has an *inverse* in the set as the identity appears exactly once in each row and column.

It is also clear from the table that the group is abelian since the table is symmetric about the lead diagonal. This means that for all $x, y \in S, x \circ y = y \circ x$.

Is the group cyclic? To be cyclic the group must have a generator and we know that a generator must have period equal to the order of the group. So, in this case, we are looking for an element of period 4. However, all non-identity elements have period 2 (we can see this directly from the table as the identity appears in all places on the lead diagonal) and hence the group cannot be cyclic.

It follows from this observation that the group cannot be isomorphic to $\mathbb{Z}_4$ (which is order 4, but cyclic). However, we know the group is abelian so it must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, the only other isomorphically distinct group of order 4 (see later).

Return to Question 3.4 on P62

A.4 Chapter 4 solutions

Solution 4.1

Let G be the symmetry group of a regular hexagon. The Cayley table is below.

$\circ$	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
e	e	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	s_6
r_1	r_1	r_2	r_3	r_4	r_5	e	s_6	s_1	s_2	s_3	s_4	s_5
r_2	r_2	r_3	r_4	r_5	e	r_1	s_5	s_6	s_1	s_2	s_3	s_4
r_3	r_3	r_4	r_5	e	r_1	r_2	s_4	s_5	s_6	s_1	s_2	s_3
r_4	r_4	r_5	e	r_1	r_2	r_3	s_3	s_4	s_5	s_6	s_1	s_2
r_5	r_5	e	r_1	r_2	r_3	r_4	s_2	s_3	s_4	s_5	s_6	s_1
s_1	s_1	s_2	s_3	s_4	s_5	s_6	e	r_1	r_2	r_3	r_4	r_5
s_2	s_2	s_3	s_4	s_5	s_6	s_1	r_5	e	r_1	r_2	r_3	r_4
s_3	s_3	s_4	s_5	s_6	s_1	s_2	r_4	r_5	e	r_1	r_2	r_3
s_4	s_4	s_5	s_6	s_1	s_2	s_3	r_3	r_4	r_5	e	r_1	r_2
s_5	s_5	s_6	s_1	s_2	s_3	s_4	r_2	r_3	r_4	r_5	e	r_1
s_6	s_6	s_1	s_2	s_3	s_4	s_5	r_1	r_2	r_3	r_4	r_5	e

For* the *subgroup of order 3, find its left cosets in G.

Let H be our subgroup of order 3. So, $H = \{e, r_2, r_4\}$. Then the left cosets of H in G are $eH = \{e \circ e, e \circ r_2, e \circ r_4\} = \{e, r_2, r_4\}$

$r_1H = \{r_1 \circ e, r_1 \circ r_2, r_1 \circ r_4\} = \{r_1, r_3, r_5\}$

$r_2H = \{r_2 \circ e, r_2 \circ r_2, r_2 \circ r_4\} = \{r_2, r_4, e\}$

$r_3H = \{r_3 \circ e, r_3 \circ r_2, r_3 \circ r_4\} = \{r_3, r_5, r_1\}$

$r_4H = \{r_4 \circ e, r_4 \circ r_2, r_4 \circ r_4\} = \{r_4, e, r_2\}$

$r_5H = \{r_5 \circ e, r_5 \circ r_2, r_5 \circ r_4\} = \{r_5, r_1, r_3\}$

$s_1H = \{s_1 \circ e, s_1 \circ r_2, s_1 \circ r_4\} = \{s_1, s_3, s_5\}$

$s_2H = \{s_2 \circ e, s_2 \circ r_2, s_2 \circ r_4\} = \{s_2, s_4, s_6\}$

$s_3H = \{s_3 \circ e, s_3 \circ r_2, s_3 \circ r_4\} = \{s_3, s_5, s_1\}$

$s_4H = \{s_4 \circ e, s_4 \circ r_2, s_4 \circ r_4\} = \{s_4, s_6, s_2\}$

$s_5H = \{s_5 \circ e, s_5 \circ r_2, s_5 \circ r_4\} = \{s_5, s_1, s_3\}$

$s_6H = \{s_6 \circ e, s_6 \circ r_2, s_6 \circ r_4\} = \{s_6, s_2, s_4\}.$

Note that

$eH = r_2H = r_4H,$

$r_1H = r_3H = r_5H,$

$s_1H = s_3H = s_5H,$

$s_2H = s_4H = s_6H.$

So, there are just the four *distinct* left cosets which are:

$$\{e, r_2, r_4\}, \qquad \{r_1, r_3, r_5\}, \qquad \{s_1, s_3, s_5\}, \qquad \{s_2, s_4, s_6\}.$$

Return to Question 4.1 on P70

Solution 4.2

Let G be the symmetry group of a regular octagon. Using the Cayley below find all of the subgroups of orders 2 and 4. For each of those subgroups find the distinct left cosets.

$\circ$	e	r_1	r_2	r_3	r_4	r_5	r_6	r_7	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
e	e	r_1	r_2	r_3	r_4	r_5	r_6	r_7	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
r_1	r_1	r_2	r_3	r_4	r_5	r_6	r_7	e	s_8	s_1	s_2	s_3	s_4	s_5	s_6	s_7
r_2	r_2	r_3	r_4	r_5	r_6	r_7	e	r_1	s_7	s_8	s_1	s_2	s_3	s_4	s_5	s_6
r_3	r_3	r_4	r_5	r_6	r_7	e	r_1	r_2	s_6	s_7	s_8	s_1	s_2	s_3	s_4	s_5
r_4	r_4	r_5	r_6	r_7	e	r_1	r_2	r_3	s_5	s_6	s_7	s_8	s_1	s_2	s_3	s_4
r_5	r_5	r_6	r_7	e	r_1	r_2	r_3	r_4	s_4	s_5	s_6	s_7	s_8	s_1	s_2	s_3
r_6	r_6	r_7	e	r_1	r_2	r_3	r_4	r_5	s_3	s_4	s_5	s_6	s_7	s_8	s_1	s_2
r_7	r_7	e	r_1	r_2	r_3	r_4	r_5	r_6	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_1
s_1	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	e	r_1	r_2	r_3	r_4	r_5	r_6	r_7
s_2	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_1	r_7	e	r_1	r_2	r_3	r_4	r_5	r_6
s_3	s_3	s_4	s_5	s_6	s_7	s_8	s_1	s_2	r_6	r_7	e	r_1	r_2	r_3	r_4	r_5
s_4	s_4	s_5	s_6	s_7	s_8	s_1	s_2	s_3	r_5	r_6	r_7	e	r_1	r_2	r_3	r_4
s_5	s_5	s_6	s_7	s_8	s_1	s_2	s_3	s_4	r_4	r_5	r_6	r_7	e	r_1	r_2	r_3
s_6	s_6	s_7	s_8	s_1	s_2	s_3	s_4	s_5	r_3	r_4	r_5	r_6	r_7	e	r_1	r_2
s_7	s_7	s_8	s_1	s_2	s_3	s_4	s_5	s_6	r_2	r_3	r_4	r_5	r_6	r_7	e	r_1
s_8	s_8	s_1	s_2	s_3	s_4	s_5	s_6	s_7	r_1	r_2	r_3	r_4	r_5	r_6	r_7	e

The subgroups of order 2 in D_8 are $\{e, r_4\}$ and $\{e, s_i\}$ for all $i = 1, 2, \ldots, 8$ (there are eight lines of reflection).

The subgroups of order 4 are $\{e, r_2, r_4, r_6\}$, $\{e, r_4, s_1, s_5\}$, $\{e, r_4, s_2, s_6\}$, $\{e, r_4, s_3, s_7\}$, $\{e, r_4, s_4, s_8\}$. There is a pattern in those last four that we saw similarly in the subgroups of order 4 in D_6.

You need to remind yourselves of the method for forming left cosets. Let's consider first one of the subgroups of order 2, namely $H = \{e, r_4\}$. We form the left cosets by pre-multiplying the elements of H by each element in the group. Since there are 16 group elements this gives 16 cosets, but we know that this process partitions the set

into equal-sized, distinct left cosets which are all the same size as H, so we should expect to end up with eight distinct left cosets.

$eH = \{e \circ e, e \circ r_4\} = \{e, r_4\}$

$r_1H = \{r_1 \circ e, r_1 \circ r_4\} = \{r_1, r_5\}$

$r_2H = \{r_2 \circ e, r_2 \circ r_4\} = \{r_2, r_6\}$

$r_3H = \{r_3 \circ e, r_3, \circ r_4\} = \{r_3, r_7\}$

$r_4H = \{r_4 \circ e, r_4 \circ r_4\} = \{r_4, e\} = eH$

$r_5H = \{r_5 \circ e, r_5 \circ r_4\} = \{r_5, r_1\} = r_1H$

$r_6H = \{r_6 \circ e, r_6 \circ r_4\} = \{r_6, r_2\} = r_2H$

$r_7H = \{r_7 \circ e, r_7 \circ r_4\} = \{r_7, r_3\} = r_3H$

$s_1H = \{s_1 \circ e, s_1 \circ r_4\} = \{s_1, s_5\}$

$s_2H = \{s_2 \circ e, s_2 \circ r_4\} = \{s_2, s_6\}$

$s_3H = \{s_3 \circ e, s_3 \circ r_4\} = \{s_3, s_7\}$

$s_4H = \{s_4 \circ e, s_4 \circ r_4\} = \{s_4, s_8\}$

$s_5H = \{s_5 \circ e, s_5 \circ r_4\} = \{s_5, s_1\} = s_1H$

$s_6H = \{s_6 \circ e, s_6 \circ r_4\} = \{s_6, s_2\} = s_2H$

$s_7H = \{s_7 \circ e, s_7 \circ r_4\} = \{s_7, s_3\} = s_3H$

$s_8H = \{s_8 \circ e, s_8 \circ r_4\} = \{s_8, s_4\} = s_4H$

Hence the distinct left cosets are $\{e, r_4\}$, $\{r_1, r_5\}$, $\{r_2, r_6\}$, $\{r_3, r_7\}$, $\{s_1, s_5\}$, $\{s_2, s_6\}$, $\{s_3, s_7\}$, $\{s_4, s_8\}$.

The distinct left cosets for the other subgroups are as follows (make sure you know how to obtain them):

$H = \{e, s_1\}: \ \{e, s_1\}, \{r_1, s_8\}, \{r_2, s_7\}, \{r_3, s_6\}, \{r_4, s_5\}, \{r_5, s_4\}, \{r_6, s_3\}, \{r_7, s_2\}$

$H = \{e, s_2\}: \ \{e, s_2\}, \{r_1, s_1\}, \{r_2, s_8\}, \{r_3, s_7\}, \{r_4, s_6\}, \{r_5, s_5\}, \{r_6, s_4\}, \{r_7, s_3\}$

$H = \{e, s_3\}: \ \{e, s_3\}, \{r_1, s_2\}, \{r_2, s_1\}, \{r_3, s_8\}, \{r_4, s_7\}, \{r_5, s_6\}, \{r_6, s_5\}, \{r_7, s_4\}$

$H = \{e, s_4\}: \ \{e, s_4\}, \{r_1, s_3\}, \{r_2, s_2\}, \{r_3, s_1\}, \{r_4, s_8\}, \{r_5, s_7\}, \{r_6, s_6\}, \{r_7, s_5\}$

$H = \{e, s_5\}: \ \{e, s_5\}, \{r_1, s_4\}, \{r_2, s_3\}, \{r_3, s_2\}, \{r_4, s_1\}, \{r_5, s_8\}, \{r_6, s_7\}, \{r_7, s_6\}$

$H = \{e, s_6\}: \ \{e, s_6\}, \{r_1, s_5\}, \{r_2, s_4\}, \{r_3, s_3\}, \{r_4, s_2\}, \{r_5, s_1\}, \{r_6, s_8\}, \{r_7, s_7\}$

$H = \{e, s_7\}: \ \{e, s_7\}, \{r_1, s_6\}, \{r_2, s_5\}, \{r_3, s_4\}, \{r_4, s_3\}, \{r_5, s_2\}, \{r_6, s_1\}, \{r_7, s_8\}$

$H = \{e, s_8\}: \ \{e, s_8\}, \{r_1, s_7\}, \{r_2, s_6\}, \{r_3, s_5\}, \{r_4, s_4\}, \{r_5, s_3\}, \{r_6, s_2\}, \{r_7, s_1\}$

$H = \{e, r_4, s_1, s_5\}: \ \{e, r_4, s_1, s_5\}, \{r_1, r_5, s_8, s_4\}, \{r_2, r_6, s_7, s_3\}, \{r_3, r_7, s_6, s_2\}$

$H = \{e, r_4, s_2, s_6\}: \ \{e, r_4, s_2, s_6\}, \{r_1, r_5, s_1, s_5\}, \{r_2, r_6, s_8, s_4\}, \{r_3, r_7, s_7, s_3\}$

$H = \{e, r_4, s_3, s_7\}: \ \{e, r_4, s_3, s_7\}, \{r_1, r_5, s_2, s_6\}, \{r_2, r_6, s_1, s_5\}, \{r_3, r_7, s_8, s_4\}$

$H = \{e, r_4, s_4.s_8\}: \ \{e, r_4, s_4, s_8\}, \{r_1, r_5, s_3, s_7\}, \{r_2, r_6, s_2, s_6\}, \{r_3, r_7, s_1, s_5\}.$

Return to Question 4.2 on P70

A.5 Chapter 5 solutions

Solution 5.1

Show that the group of real numbers under addition is isomorphic to the group of matrices representing shears parallel to the x-axis.

(Recall that this is a type of linear transformation and you studied these in Algebra II. It involves moving a point a fixed distance parallel to the x-axis, that distance being dependent on the y-coordinate of the point. Such transformations can be represented by 2×2 matrices of the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, where a is any real number.)

First we need to remind ourselves of the matrix representation of a shear and how it

acts on a point (it's a function). It involves moving a point a fixed distance parallel to the x-axis, that distance being dependent on the y-coordinate of the point.

So, given any point (x, y) in the plane, the transformation produces the shear as follows:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + ay \\ y \end{pmatrix}.$$

Let $G = (\mathbb{R}, +)$ and $H = \left(\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\}, \times \right)$.

Define $f : G \to H$ by $f(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Then, clearly, this is a bijective function. Now we just need to show that $\forall a, b \in G,\ f(a + b) = f(a)f(b)$.

$$\begin{aligned} f(a+b) &= \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \\ f(a)f(b) &= \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix} \end{aligned}$$

So, $f(a + b) = f(a)f(b)$ and, hence, f is an isomorphism from G to H.

Return to Question 5.1 on P93

Solution 5.2

Consider the set $G = \{1, 2, 3, 4, 5, 6\}$. This set forms a group under multiplication modulo 7.

- ***a. Draw and complete the operation table for the group $(G, \otimes_7)$.***
- ***b. Find the period of each element in the group.***
- ***c. Find an isomorphism between this group and $\mathbb{Z}_6$.***

a. The table is as follows:

$\otimes_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

b. The periods of the elements are (together with those for $\mathbb{Z}_6$)

element	period	$\mathbb{Z}_6$
1	1	0
2	3	2
3	6	1
4	3	4
5	6	5
6	2	3

c. Let $\theta : G \to \mathbb{Z}_6$. We know that identity maps to identity so $\theta(1) = 0$. We also know that the period of an element $g \in G$ must be the same as the period of $\theta(g)$ in $\mathbb{Z}_6$. Since each group has only one element of period 2 we must also have that $\theta(6) = 3$. Note that there are two elements of period 6 in each group (the cyclic generators of those groups). Suppose, therefore, that we chose $\theta(3) = 1$. This then fixes $\theta(5) = 5$.

We now consider $\theta(2)$. Remember that the operation in G is multiplication modulo 7 whereas the operation in $\mathbb{Z}_6$ is addition modulo 6. In G we have $3 \times 3 = 9 \equiv 2 \pmod 7$. Hence $\theta(2) = \theta(3 \times 3) = \theta(3) + \theta(3) = 1 + 1 = 2$. So

$\theta(2) = 2$ and then $\theta(4) = 4$ is fixed.

Hence an isomorphism is

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 2 & 1 & 4 & 5 & 3 \end{pmatrix}.$$

Return to Question 5.2 on P93

A.6 Chapter 6 solutions

Solution 6.1

Let $(G_1, \circ)$ ***and*** $(G_2, *)$ ***be groups and*** $\theta : G_1 \to G_2$ ***be an injective homomorphism. For each of the following statements, either prove that it is true or provide a counter-example:***

a. If $(G_1, \circ)$ ***is abelian, then*** $(G_2, *)$ ***is abelian.***

b. If $(G_2, *)$ ***is abelian, then*** $(G_1, \circ)$ ***abelian.***

Beware spurious 'proofs'!

a. This statement is false, but it is easy to give what appears to be a 'proof' that it is true. Consider the following 'proof':

$$\begin{array}{lrll} \text{Let } x, y \in G_1. \text{ Then, } \theta(x) * \theta(y) & = & \theta(x \circ y) & \theta \text{ is a homomorphism} \\ & = & \theta(y \circ x) & G_1 \text{ is abelian} \\ & = & \theta(y) * \theta(x) & \theta \text{ is a homomorphism} \end{array}$$

Hence, G_2 is abelian.

The problem with this proof is that it only proves that the **image of** G_1 **in** G_2 is abelian. If G_1 does not map onto the whole of G_2 then we can say nothing about the commutativity, or otherwise, of those elements of G_2 that are not

mapped onto from G_1, and in this case we are not told that θ is *surjective*.

As stated, this statement is false. For a counterexample let G_1 be the subgroup of D_3 consisting of the identity and the rotations and let G_2 be the whole of D_3. Let θ be the identity mapping from G_1 to G_2, that is $\theta : \{e, r_1, r_2\} \to D_3$ defined by $\theta(e) = e$, $\theta(r_1) = r_1$, and $\theta(r_2) = r_2$. Clearly θ is injective and a homomorphism, but whilst $(\{e, r_1, r_2\}, \circ)$ is abelian D_3 is not abelian.

b. This statement is true and the proof is as follows:

$$\begin{aligned} \text{Let } x, y \in G_1. \text{ Then, } \theta(x \circ y) &= \theta(x) * \theta(y) && \theta \text{ is a homomorphism} \\ &= \theta(y) * \theta(x) && G_2 \text{ is abelian} \\ &= \theta(y \circ x) && \theta \text{ is a homomorphism} \end{aligned}$$

Hence, G_1 is abelian (since θ is injective).

Return to Question 6.1 on P116

Solution 6.2

Recall that the kernel of the homomorphism is a subgroup of the domain. Recall, also, that we said in lectures that the size of the image of a homomorphism equals the size of the domain divided by the size of its kernel. That, of course, related to examples where both the domain and the image were finite. What happens if we now consider examples where infinity plays a part? So, investigate the kernels of the following homomorphisms in light of the above relationship:

a. $\theta : (\mathbb{Z}, +) \to \mathbb{Z}_n$ ***defined by*** $\forall a \in \mathbb{Z},\ \theta(a) = a \pmod n$,

b. $\phi : GL(2, \mathbb{R}) \to \mathbb{R}\backslash\{0\}$ ***defined by*** $\forall A \in GL(2, \mathbb{R}),\ \phi(A) = |A|$.

First we need to be reminded of the definition of the kernel of a homomorphism. In simple terms, if there is a homomorphism from a group G_1 into a group G_2 then the kernel of that homomorphism is the subset of elements of G_1 that map, under the homomorphism, to the identity element in G_2. Formally:

Let ϕ be a group homomorphism from a group G_1 to a group G_2 and let e_2 be the identity in G_2. Then, the kernel of ϕ is denoted and defined by

$$\text{ker } (\phi) = \{x \in G \mid \phi(x) = e_2\}.$$

Recall that the kernel of the homomorphism is a subgroup of the domain. Recall, a,so, that we said in lectures that the size of the image of a homomorphism equals the size of the domain divided by the size of its kernel. That, of course, related to examples where both the domain and the image were finite. What happens if we now consider examples where infinity plays a part?

a. Note that the function is mapping into $\mathbb{Z}_n$ and so the identity element is 0 $(\text{mod } n)$ (since the operation in $\mathbb{Z}_n$ is addition modulo n). Clearly the domain is infinite. In addition, the kernel of θ must be infinite since, for any $n \in \mathbb{Z}$, there is an infinite number of integers congruent to 0 modulo n for any given n (these will be of the form kn where $k \in \mathbb{Z}$). On the other hand, the image of θ is finite as $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and so contains n elements.
So, here, we have
$$n = \frac{\infty}{\infty}.$$

b. In this instance ϕ is mapping into $\mathbb{R}\backslash\{0\}$. It is implicit that the binary operation is multiplication and that the identity is 1. Therefore, the kernel of this homomorphism is the set of all 2×2 matrices that have determinant 1. Obviously the domain of the homomorphism, that is $GL(2, \mathbb{R})$, is infinite, as is the image $\mathbb{R}\backslash\{0\}$. But what about the kernel? A little thought should reveal that this is also infinite since every matrix of the form $\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$, where $k \in \mathbb{R}$, has determinant 1.

So, here, we have

$$\infty = \frac{\infty}{\infty}.$$

Return to Question 6.2 on P117

Solution 6.3

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$ ***and*** $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$***. Calculate*** $g \circ f$***,*** $f \circ g$***,*** f^2***, and*** g^2***.***

$g \circ f$:

Remember that the operation here is function composition, so we apply the second function, f, first. Consider the number 1. Permutation \$ f\$ takes 1 to 2 and then permutation g takes 2 to 3. Hence, the composite function $g \circ f$ takes 1 to 3. Now consider the number 2. Permutation f takes 2 to 3 and then g takes 3 to 2, so $g \circ f$ takes 2 to 2. Similarly we have

$$f(3) = 5 \quad \text{and} \quad g(5) = 5 \quad \text{so} \quad (g \circ f)(3) = 5$$
$$f(4) = 1 \quad \text{and} \quad g(1) = 4 \quad \text{so} \quad (g \circ f)(4) = 4$$
$$f(5) = 4 \quad \text{and} \quad g(4) = 1 \quad \text{so} \quad (g \circ f)(5) = 1$$

This gives the composite permutation

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

$f \circ g$:

In this case we apply g first and then f. Consider the number 1. Permutation g takes 1 to 4 and then permutation f takes 4 to 1. Hence, the composite function $f \circ g$

takes 1 to 1. Now consider the number 2. Permutation g takes 2 to 3 and then f takes 3 to 5, so $f \circ g$ takes 2 to 5. Similarly we have

$$\begin{aligned} g(3) = 2 \quad &\text{and} \quad f(2) = 3 \quad \text{so} \quad (f \circ g)(3) = 3 \\ g(4) = 1 \quad &\text{and} \quad f(1) = 2 \quad \text{so} \quad (f \circ g)(4) = 2 \\ g(5) = 5 \quad &\text{and} \quad f(5) = 4 \quad \text{so} \quad (f \circ g)(5) = 4 \end{aligned}$$

This gives the composite permutation

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$$

f^2:

Note that $f^2 = f \circ f$. Now, f maps 1 to 2 and then 2 to 3, so f^2 maps 1 to 3. Similarly, $f^2(2) = 5$, $f^2(3) = 4$, $f^2(4) = 2$, and $f^2(5) = 1$, so

$$f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

g^2:

Note that $g^2 = g \circ g$. Now, g maps 1 to 4 and then 4 to 1, so g^2 maps 1 to 1. Similarly, $g^2(2) = 2$, $g^2(3) = 3$, $g^2(4) = 4$, and $g^2(5) = 5$, so

$$g^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Notice that this is the identity permutation, so if $g^2 = \text{id}$ we must have that g is self-inverse, that is $g = g^{-1}$. This is easy to see from the two-row representation of g (turn it upside-down and you get the same permutation).

We could have performed all of the above calculations by first expressing f and g as disjoint cycles. It is good practise to do this.

As disjoint cycles we have that $f = (1\ 2\ 3\ 5\ 4)$ and $g = (1\ 4)(2\ 3)$. Then:

- $g \circ f = (1\ 4)(2\ 3)(1\ 2\ 3\ 5\ 4) = (1\ 3\ 5)(2)(4) = (1\ 3\ 5)$;
- $f \circ g = (1\ 2\ 3\ 5\ 4)(1\ 4)(2\ 3) = (1)(2\ 5\ 4)(3) = (2\ 5\ 4)$;
- $f^2 = (1\ 2\ 3\ 5\ 4)(1\ 2\ 3\ 5\ 4) = (1\ 3\ 4\ 2\ 5)$;
- $g^2 = (1\ 4)(2\ 3)(1\ 4)(2\ 3) = (1)(2)(3)(4)(5) = \mathrm{id}$.

Return to Question 6.3 on P117

Solution 6.4

For each of the following permutations

- ***write the permutation as a product of disjoint cycles,***
- ***state the number of orbits of the permutation,***
- ***find the inverse permutation,***
- ***write the permutation as a product of transpositions in two different ways,***
- ***state whether the permutation is even or odd,***
- ***find the period of the permutation.***

a. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 12 & 8 & 6 & 9 & 11 & 3 & 1 & 2 & 10 & 4 & 5 \end{pmatrix} \in S_{12}$.

b. $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 12 & 10 & 9 & 3 & 11 & 7 & 5 & 1 & 8 & 4 & 2 \end{pmatrix} \in S_{12}$.

c. $\gamma = (1\ 3\ 8\ 5)(2\ 9\ 3)(1\ 4\ 3\ 7)(4\ 5\ 8\ 9) \in S_9$.

d. $\delta = (1\ 5\ 3\ 6)(6\ 3\ 2\ 1)(1\ 2\ 5)(3\ 5\ 7\ 1)(4\ 6\ 1\ 5) \in S_8$.

e. $\epsilon = (1\ 3\ 4)(3\ 2\ 1)(4\ 3\ 1)(5\ 4\ 3)(2\ 5\ 1) \in S_5$.

a. $\alpha = (1\ 7\ 3\ 8)(2\ 12\ 5\ 9)(4\ 6\ 11)(10) = (1\ 7\ 3\ 8)(2\ 12\ 5\ 9)(4\ 6\ 11)$. α has four orbits (we count singletons).

To find the inverse permutation we simply reverse the cyclic order of the elements in *each* of the orbits, so $\alpha^{-1} = (8\ 3\ 7\ 1)(9\ 5\ 12\ 2)(11,\ 6\ 4)$.

We use the two different rules for writing permutations as transpositions (see lecture notes), remembering that we apply the rule to each individual cycle in turn. This gives

$$\alpha = (1\ 7)(7\ 3)(3\ 8)(2\ 12)(12\ 5)(5\ 9)(4\ 6)(6\ 11)$$

or

$$\alpha = (1\ 8)(1\ 3)(1\ 7)(2\ 9)(2\ 5)(2\ 12)(4\ 11)(4\ 6).$$

As the permutation can be expressed as the product of eight transpositions it is an even permutation. [Note we could have deduced that from the fact that it has an even number of orbits of even length.]

We find the period of a permutation from the lowest common multiple of the lengths of the disjoint cycles (orbits). Here we have cycle lengths of 4, 4, 3, and 1. Hence the period of α is lcm(4, 3) = 12.

b. $\beta = (1\ 6\ 11\ 4\ 9)(2\ 12)(3\ 10\ 8\ 5)(7) = (1\ 6\ 11\ 4\ 9)(2\ 12)(3\ 10\ 8\ 5)$.

β has four orbits.

$\beta^{-1} = (9\ 4\ 11\ 6\ 1)(12\ 2)(5\ 8\ 10\ 3)$.

As a product of transpositions we have

$$\beta = (1\ 6)(6\ 11)(11\ 4)(4\ 9)(2\ 12)(3\ 10)(10\ 8)(8\ 5)$$

or

$$\beta = (1\ 9)(1\ 4)(1\ 11)(1\ 6)(2\ 12)(3\ 5)(3\ 8)(3\ 10).$$

This is an even permutation.

The period of β is lcm(5, 2, 4) $= 20$.

c. $\gamma = (1\ 4)(2\ 9)(3\ 7)(5)(6)(8) = (1\ 4)(2\ 9)(3\ 7)$. γ has six orbits.

The disjoint cycles are already a product of transpositions, so there is only one way of writing these, namely $(1\ 4)(2\ 9)(3\ 7)$. This is an odd permutation.

The period of β is lcm(2, 2, 2) $= 2$. So this permutation must be self-inverse.

d. $\delta = (1\ 7\ 5\ 4\ 6\ 2\ 3)(8) = (1\ 7\ 5\ 4\ 6\ 2\ 3)$.

δ has two orbits.

$\delta^{-1} = (3\ 2\ 6\ 4\ 5\ 7\ 1)$.

As a product of transpositions we have

$$\delta = (1\ 7)(7\ 5)(5\ 4)(4\ 6)(6\ 2)(2\ 3)$$

or

$$\delta = (1\ 3)(1\ 2)(1\ 6)(1\ 4)(1\ 5)(1\ 7).$$

This is an even permutation. The period of δ is lcm(7, 1) $= 7$.

e. $\epsilon = (1\ 3\ 5)(2)(4) = (1\ 3\ 5)$.

ϵ has three orbits.

$\epsilon^{-1} = (5\ 3\ 1)$.

As a product of transpositions we have

$$\epsilon = (1\ 3)(3\ 5)$$

or

$$\epsilon = (1\ 5)(1\ 3).$$

This is an even permutation.

The period of ϵ is lcm(3, 1) = 3.

Return to Question 6.4 on P117

Solution 6.5

Find the maximum period of a permutation in S_{15} and give an example of such a permutation.

Recall that the period of a permutation is the lowest common multiple of the lengths of the disjoint cycles. Also, for a permutation in S_n the disjoint cycles (including singletons) must contain precisely the n elements upon which the permutation acts. So in S_{15} we need to maximise the lowest common multiple of numbers from 1 to 15 that add up to 15. For example, if we have cycle lengths of 2, 3 and 10 (total 15) this permutation has a period of lcm(2, 3, 5) = 30. We can beat this with cycle lengths of, say, 7 and 8 since lcm(7, 8) = 56. The maximum period occurs when the cycle lengths add up to 15 but each is pairwise co-prime with the others. So $3 + 5 + 7 = 15$ and lcm(3, 5, 7) = 105. An example of a permutation in S_{15} with period 105 is $(1\ 2\ 3)(4\ 5\ 6\ 7\ 8)(9\ 10\ 11\ 12\ 13\ 14\ 15)$.

Return to Question 6.5 on P118

A.7 Chapter 7 solutions

Solution 7.1

List the generators in each of the following cyclic groups:

i. $\mathbb{Z}_{10}$***;***

ii. $\mathbb{Z}_{24}$***;***

iii. $\mathbb{Z}_3 \times \mathbb{Z}_4$***.***

i. The generators of $\mathbb{Z}_{10}$ are all numbers less than 10 that are relatively prime to 10, that is 1, 3, 7, 9.

ii. Similarly, the generators of $\mathbb{Z}_{24}$ are 1, 5, 7, 11, 13, 17, 19, 23.

iii. The group has order 12 so we need elements of period 12. It therefore follows from Lemma 5.1 that we need ordered pairs where the first element has period 3 in $\mathbb{Z}_3$ and the second element has period 4 in $\mathbb{Z}_4$. Hence, the generators of $\mathbb{Z}_3 \times \mathbb{Z}_4$ are (1, 1), (2, 1), (1, 3) and (2, 3).

Return to Question 7.1 on P137

Solution 7.2

In each of the following cases find the period of the given element of the direct product group:

i. (1, 3) in $\mathbb{Z}_4 \times \mathbb{Z}_9$***;***

ii. (4, 12) in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$***;***

iii. (3, 4, 2) in $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_9$***.***

Recall, again, Lemma 5.1. This says (if extended to more than two groups) that the period of $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \ldots \times G_n$ is the lowest common multiple of the periods of the individual a_i in their respective groups.

i. It is easy to see that 1 has period 4 in $\mathbb{Z}_4$ and, since 3 divides 9 exactly 3 times, that 3 has period 3 in $\mathbb{Z}_9$. Hence the period of (1, 3) in $\mathbb{Z}_4 \times \mathbb{Z}_9 = \text{lcm}(4, 3) = 12$.

ii. We need to find the period of 4 in $\mathbb{Z}_6$ and the period of 12 in $\mathbb{Z}_{15}$.

Now, gcd(4, 6) = 2, so 4 has period $\frac{6}{2} = 3$ in $\mathbb{Z}_6$. Further gcd(12, 15) = 3, so 12 has period $\frac{15}{3} = 5$ in $\mathbb{Z}_{15}$. Thus the period of (4, 12) in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ = lcm(3, 5) = 15.

iii. We need to find the period of 3 in $\mathbb{Z}_4$, the period of 4 in $\mathbb{Z}_5$, and the period of 2 in $\mathbb{Z}_9$.

Note that in each case the element and the order of the group are relatively prime, so each of the given elements is a generator of its group. Hence the period of each of them must be the order of the group.

So, the period of (3, 4, 2) in $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_9$ = lcm(4, 5, 9) = 180.

Return to Question 7.2 on P137

Solution 7.3

i. ***Classify, according to the Fundamental Theorem of Finite Abelian Groups all of the abelian groups of order 100. Which of the groups is cyclic? Which is isomorphic to*** $\mathbb{Z}_5 \times \mathbb{Z}_{20}$***?***

ii. ***Classify, according to the Fundamental Theorem of Finite Abelian Groups all of the abelian groups of order 504. Which of the groups is cyclic? Which is isomorphic to*** $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{21}$***?***

iii. ***How many isomorphically distinct abelian groups are there of order 104,544?***

i. $100 = 2^2 \times 5^2$. Hence, the isomorphically distinct abelian groups are:

$$\mathbb{Z}_4 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

Of these, $\mathbb{Z}_4 \times \mathbb{Z}_{25}$ is cyclic as 4 and 25 are relatively prime.

$\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_{20}$ since 4 and 5 are relatively prime (so $\mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20}$).

ii. $504 = 2^3 \times 3^2 \times 7$. Hence, the isomorphically distinct abelian groups are:

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_7$$
$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_7$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_7$$
$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$$
$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$$

Of these, $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_7$ is cyclic as 8, 9 and 7 are pairwise relatively prime.

$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{21}$ since 3 and 4 are relatively prime (so $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$) and 3 and 7 are relatively prime (so $\mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$).

iii. $104,544 = 2^5 \times 3^3 \times 11^2$. Now, there are seven ways of expressing 2^5 as a product of powers of 2 (which we require for the FT). That is, $2^5 = 2 \times 2^4 = 2^2 \times 2^3 = 2 \times 2 \times 2^3 = 2 \times 2^2 \times 2^2 = 2 \times 2 \times 2 \times 2^2 = 2 \times 2 \times 2 \times 2 \times 2$. In addition there are three ways of expressing 3^3 as products of powers of 3 ($3^3 = 3 \times 3^2 = 3 \times 3 \times 3$) and two ways of expressing 11^2 as a product of powers of 11 ($11^2 = 11 \times 11$). Hence there are $7 \times 3 \times 2 = 42$ isomorphically distinct abelian groups of order 104,544.

Return to Question 7.3 on P137

Solution 7.4

i. Find a subgroup of $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ of order 9.

ii. Find a subgroup of $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{35}$ of order 252.

i. Note that $9 = 3 \times 3$ and that 3 divides both 6 and 15. So we need a subgroup of order 3 from $\mathbb{Z}_6$ and a subgroup of order 3 from $\mathbb{Z}_{15}$. Clearly $\langle 2 \rangle$ satisfies the former and $\langle 5 \rangle$ satisfies the latter. So a subgroup of $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ of order 9 is

$$\{(x, y) \mid x \in \{0, 2, 4\},\ y \in \{0, 5, 10, \}\}.$$

ii. Note that $252 = 4 \times 9 \times 7$ So, using the argument above a subgroup of $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{35}$ of order 252 is

$$\{(x, y, z) \mid x \in \mathbb{Z}_4,\ y \in \{0, 2, 4, 6, 8, 10, 12, 14, 16\},\ z \in \{0, 5, 10, 15, 20, 25, 30\}\}.$$

Return to Question 7.4 on P137

Solution 7.5

Show, by exhibiting a counter-example, that the following converse of Theorem 7.3 is false.

If a group G is such that every proper subgroup is cyclic, then G is cyclic.

Can you find infinitely many counter-examples?

Note that D_3 is non-cyclic. It has order 6. Its proper subgroups are $\{e, r_1, r_2\}$, $\{e, s_1\}$, $\{e, s_2\}$, $\{e, s_3\}$ and $\{e\}$. All of these are cyclic.

In general, let p, q be prime. Then *any* group of order pq does not have non-cyclic subgroups since, by Lagrange's Theorem, the proper subgroup orders can only be 1, p or q and we know that a group of prime order must be cyclic (obviously $\{e\}$ is cyclic).

For infinitely many counter-examples, consider

i. D_p : this has order $2p$ and, of course, 2 and p are prime. Apart from $\{e\}$, the only subgroups are $\{e, r_1, r_2, \ldots, r_{p-1}\}$ and $\{e, s_i\}$, where $i = 1, 2, \ldots, p$.

ii. $\mathbb{Z}_p \times \mathbb{Z}_p$: this cannot be cyclic since p and p cannot be relatively prime ($\gcd(p, p) = p$, not 1). However, by the Fundamental Theorem, the subgroups must be of order p, a prime, and hence cyclic.

Note that $\mathbb{Z}_p \times \mathbb{Z}_q$ does not work because p and q must be relatively prime, so the group itself is cyclic.

Return to Question 7.5 on P138

A.8 Chapter 8 solutions

Solution 8.1

a. ***Use Euclid's algorithm to find the greatest common divisor of 440 and 189. Then find integers s and t such that gcd$(440, 189) = 189s + 440t$.***

b. ***Use Euclid's algorithm to find the greatest common divisor of 1343 and 391. Then find integers s and t such that gcd$(1343, 391) = 1343s + 391t$.***

c. ***Use Euclid's algorithm to find the greatest common divisor of 975 and 121. Then find integers s and t such that gcd$(975, 121) = 121s + 975t$.***

First recall the general principle:

$$\text{if } a = qb + r \text{ then } \gcd(a, b) = \gcd(b, r).$$

a. In what follows we repeat that procedure at each step.

$$440 = 2 \times 189 + 62 \quad (1)$$

$$189 = 3 \times 62 + 3 \quad (2)$$

$$62 = 20 \times 3 + 2 \quad (3)$$

$$3 = 1 \times 2 + 1 \quad (4)$$

$$2 = 2 \times 1 \quad (5)$$

So, gcd $(440, 189) = 1$.

We can now work backwards from the gcd as follows:

$$\begin{aligned}
1 &= 3 - (1 \times 2) \\
&= 3 - (62 - (20 \times 3)) && \text{using } (3) \\
&= (21 \times 3) - (1 \times 62) \\
&= (21 \times (189 - (3 \times 62))) - (1 \times 62) && \text{using } (2) \\
&= (21 \times 189) - (64 \times 62) \\
&= (21 \times 189) - (64 \times (440 - (2 \times 189))) && \text{using } (1) \\
&= (-64 \times 440) + (149 \times 189).
\end{aligned}$$

So $s = 149$ and $t = -64$.

b. We compute $\gcd(1343, 391)$:

$$1343 = 3 \times 391 + 170 \tag{6}$$

$$391 = 2 \times 170 + 51 \tag{7}$$

$$170 = 3 \times 51 + 17 \tag{8}$$

$$51 = 3 \times 17 \tag{9}$$

So, gcd $(1343, 391) = 17$.

We can now work backwards from the gcd as follows:

$$\begin{aligned}
17 &= 170 - (3 \times 51) \\
&= 170 - (3 \times (391 - (2 \times 170))) && \text{using} \quad (7) \\
&= (7 \times 170) - (3 \times 391) \\
&= (7 \times (1343 - (3 \times 391))) - (3 \times 391) && \text{using} \quad (6) \\
&= (7 \times 1343) - (24 \times 391).
\end{aligned}$$

So $s = 7$ and $t = -24$.

c. We compute $\gcd(-419, 52)$:

$$975 = 8 \times 121 + 7 \tag{10}$$

$$121 = 17 \times 7 + 2 \tag{11}$$

$$7 = 3 \times 2 + 1 \tag{12}$$

$$2 = 2 \times 1 \tag{13}$$

So, gcd $(975, 121) = 1$.

We can now work backwards from the gcd as follows:

$$\begin{aligned} 1 &= 7-(3\times 2) \\ &= 7-(3\times(121-(17\times 7))) && \text{using } (11) \\ &= (52\times 7)-(3\times 121) \\ &= (52\times(975-(8\times 121)))-(3\times 121) && \text{using } (10) \\ &= (52\times 975)-(419\times 121). \end{aligned}$$

So $s=-419$ and $t=52$.

Return to Question 8.1 on P163

Solution 8.2

Use your result from Question 8.1 c. to find the inverse of $[121]_{975}$ ***in*** $\mathbb{Z}_{975}^{\times}$.

Note that, by Euclid, $\gcd(a,b)=ma+nb$ for some $m,n\in\mathbb{Z}$. So, if $\gcd(a,b)=1$ we have that $ma=1-nb$ and so a divides $1-nb$. It then follows, by definition, that $nb\equiv 1 \pmod{a}$. Consequently we must have that $[n]_a=[b]_a^{-1}$.

We found in 1(c) above that $(52\times 975)-(419\times 121)=1$. Hence $[121]_{975}^{-1}=[-419]_{975}=[556]_{975}$.

Return to Question 8.2 on P163

Solution 8.3

Show that $\mathbb{Z}_{12}^{\times}$ ***is isomorphic to*** $\mathbb{Z}_2\times\mathbb{Z}_2$ ***and write down an isomorphism between the two groups.***

$\mathbb{Z}_{12}^{\times}=\{1,5,7,11\}$, a group of order 4.

We know that there are only two isomorphically distinct groups of order 4, namely $\mathbb{Z}_4$

and $\mathbb{Z}_2 \times \mathbb{Z}_2$. We also know that $\mathbb{Z}_4$ is cyclic , whereas $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not. So, in order to show that $\mathbb{Z}_{12}^{\times}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, we simply need to demonstrate that it is not cyclic. The easiest way to do this is to show that $\mathbb{Z}_{12}^{\times}$ does not contain any element of period 4 (if the group is cyclic it must have a generator which must have a period equal to the order of the group). Note that

$$\begin{aligned} 5^2 &= 25 \equiv 1 \pmod{12} \\ 7^2 &= 49 \equiv 1 \pmod{12} \\ 11^2 &= 121 \equiv 1 \pmod{12}. \end{aligned}$$

Hence every element has period 2, except for the identity which has period 1. So $\mathbb{Z}_{12}^{\times}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and not $\mathbb{Z}_4$.

As every element of each of those two groups (identity excepted) has period 2, an isomorphism is not difficult to find. For example

$$\theta = \begin{pmatrix} (0,0) & (0,1) & (1,0) & (1,1) \\ 1 & 5 & 7 & 11 \end{pmatrix}.$$

Return to Question 8.3 on P164

Solution 8.4

Use Fermat's Little theorem to find the principal remainder on dividing:

a. $\mathbf{5^{25}}$ ***by 13;***

b. $\mathbf{17^{44}}$ ***by 7;***

c. $\mathbf{19^{53}}$ ***by 11.***

Recall Fermat's Little Theorem (FLT):

If p is prime and a is an integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

a. In the notation of FLT let $p = 13$ and $a = 5$. Now, $13 \nmid 5$, so by FLT we have that $5^{12} \equiv 1 \pmod{13}$. Then,

$$\begin{aligned} 5^{25} &= 5 \times 5^{24} \\ &= 5 \times (5^{12})^2 \\ &\equiv 5 \times 1^2 \pmod{13} && \text{since } 5^{12} \equiv 1 \pmod{13} \\ &\equiv 5 \pmod{13} \end{aligned}$$

So, the principal remainder on dividing 5^{25} by 13 is 5.

b. In the notation of FLT let $p = 7$ and $a = 17$. Now, $7 \nmid 17$, so by FLT we have that $17^6 \equiv 1 \pmod{7}$. Then,

$$\begin{aligned} 17^{44} &= 17^2 \times 17^{42} \\ &= 17^2 \times (17^6)^7 \\ &\equiv 17^2 \times 1^7 \pmod{7} && \text{since } 17^6 \equiv 1 \pmod{7} \\ &\equiv 3^2 \pmod{7} && \text{since } 17 \equiv 3 \pmod{7} \\ &\equiv 9 \pmod{7} \\ &\equiv 2 \pmod{7} \end{aligned}$$

So, the principal remainder on dividing 17^{44} by 7 is 2.

c. In the notation of FLT let $p = 11$ and $a = 19$. Now, $11 \nmid 19$, so by FLT we have

that $19^{10} \equiv 1 \pmod{11}$. Then,

$$\begin{aligned}
19^{53} &= 19^3 \times 19^{50} \\
&= 19^3 \times (19^{10})^5 \\
&\equiv 19^3 \times 1^5 \pmod{11} && \text{since } 19^{10} \equiv 1 \pmod{11} \\
&\equiv 8^3 \pmod{11} && \text{since } 19 \equiv 8 \pmod{11} \\
&\equiv (-3)^3 \pmod{11} && \text{since } 8 \equiv -3 \pmod{11} \\
&\equiv -27 \pmod{11} \\
&\equiv 6 \pmod{11}
\end{aligned}$$

So, the principal remainder on dividing 19^{53} by 11 is 6.

Return to Question 8.4 on P164

Solution 8.5

Show that $2^{11,213} - 1$ is not divisible by 11.

We can use Fermat' Little Theorem to solve this. Recall what the theorem says:

If p is prime, $a \in \mathbb{Z}$ and p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.

Let $p = 11$ and $a = 2$. Now 11 does not divide 2, so we can use FLT and

$$2^{11-1} = 2^{10} \equiv 1 \pmod{11}.$$

Now

$$\begin{aligned} 2^{11,213}-1 &= 2^3(2^{11,210})-1 \\ &= 8(2^{10})^{1121}-1 \\ &\equiv 8(1)^{1121}-1 \pmod{11} \\ &\equiv 8-1 \pmod{11} \\ &\equiv 7 \pmod{11}. \end{aligned}$$

So, $2^{11,213}-1$ leaves principal remainder 7 on division by 11.

Note that 11,213 is prime and it can be shown that $2^{11,213}-1$ is prime. Primes of the form 2^p-1 are called Mersenne primes. The largest known prime is a Mersenne prime; discovered in 2017 it is $2^{77,232,917}-1$ and has 23,249,425 digits.

Return to Question 8.5 on P164

Solution 8.6

Find the inverses of 16, 17 and 18 in $\mathbb{Z}_{19}^{\times}$. Use those results, together with Wilson's Theorem, to find the remainder when 15! is divided by 19.

$\mathbb{Z}_{19}^{\times}=\{1,2,3,\ldots,16,17,18\}$. We know from the proof of Wilson's Theorem that in $\mathbb{Z}_p^{\times}$, where p is prime, the self-inverse elements are 1 and $p-1$. So, the inverse of 18 in $\mathbb{Z}_{19}^{\times}$ is 18 (which, of course, is equivalent to $-1 \pmod{19}$).

Now, $17^{-1}=9$ since $17\times 9=153$ and $153\equiv 1 \pmod{19}$.

Similarly, $16^{-1}=6$.

Recall that Wilson's Theorem states that if p is prime then $(p-1)!\equiv -1 \pmod{p}$.

So, with $p = 19$ we have $18! \equiv -1 \pmod{19}$.\\ Now, using the above results,

$$\begin{aligned} 15! &= 18! \times 18^{-1} \times 17^{-1} \times 16^{-1} \\ &\equiv (-1) \times (-1) \times 9 \times 6 \pmod{19} \\ &\equiv 54 \pmod{19} \\ &\equiv 16 \pmod{19} \end{aligned}$$

Hence, the principal remainder is 16.

Return to Question 8.6 on P164

Solution 8.7

Let p be a prime except 2 and 5. Deduce from Fermat's Little Theorem that there is a multiple of p, all of whose digits in decimal notation are 9's.

[Example: $\mathbf{142857 \times 7 = 999999}$***.]***

Note that $999\ldots9 = 10^k - 1$ for some $k \in \mathbb{Z}$. So,

$$\begin{aligned} np = 999\ldots9 &\Leftrightarrow 10^k - 1 = np \\ &\Leftrightarrow 10^k \equiv 1 \pmod{p} \end{aligned}$$

Now, $p \neq 2$ and $p \neq 5$, hence 10 is not a multiple of p, that is $p \nmid 10$. Hence, by FLT, $10^{p-1} \equiv 1 \pmod{p}$ with $p \neq 2, 5$. Then, with $p = 7$, say, $10^6 \equiv 1 \pmod{7}$ and so $999,999 = 7n$ for some n.

Return to Question 8.7 on P164

Solution 8.8

Consider the set of Hilbert Numbers, $\mathbb{S} = \{n \in \mathbb{N} \mid n \equiv 1 \pmod 4\}$. ***This is the set of all integers that are of the form*** $4k + 1$, ***where*** $k \in \mathbb{N}$. ***Find the first five 'primes' in this set (called Hilbert Primes). What is the smallest number in*** $\mathbb{S}$ ***that does not have a unique factorisation in Hilbert Primes?***

First, it helps to visualise what numbers are actually in the set. Since we are going to be looking at primes in the set we need only consider members of $\mathbb{S}$ that are positive. So

$$\mathbb{S} = \{1, 5, 9, 13, 17, 21, 25, 29, 33, 37, \ldots\}.$$

We then need a suitable definition of 'prime' within the context of this set. If we use our usual definition for primes in $\mathbb{N}$, we need to be careful that we refer to divisibility *within the set*. So, we define a Hilbert prime as a member of $\mathbb{S}$ greater than 1 that is divisible only by 1 (which is in $\mathbb{S}$) and itself. Then, the first five Hilbert primes are 5, 9, 13, 17 and 21. Note that 9 and 21 are both divisible by 3 in $\mathbb{Z}$, but 3 is not in $\mathbb{S}$.

Like the case of $\mathbb{E}$ in the lectures, the unique factorisation principle in $\mathbb{N}$ breaks down in $\mathbb{S}$. The first number in $\mathbb{S}$ to exhibit multiple prime factorisations is

$$441 = 9 \times 49 = 21 \times 21.$$

Return to Question 8.8 on P165

A.9 Chapter 9 solutions

Solution 9.1

a. ***An element*** a ***of a ring*** R ***is said to be*** idempotent ***if*** $a^2 = a$. ***Show that a division ring contains exactly two idempotent elements.***

b. ***If every element in a ring*** R ***is idempotent, show that any non-zero element*** $x \in R$ ***has period 2 in the group*** $(R, +)$.

c. Show that any ring in which every element is idempotent is necessarily commutative.

a. Clearly, $0_R^2 = 0_R$.

Now let $a \in R,\ a \neq 0_R$. We know that a^{-1} exists (division ring), so

$$\begin{aligned} & a^2 = a \\ \Leftrightarrow \quad & aa = a \\ \Leftrightarrow \quad & aaa^{-1} = aa^{-1} \\ \Leftrightarrow \quad & a = 1_R. \end{aligned}$$

Hence, 0_R and 1_R are the only idempotent elements.

b. We have

$$\begin{aligned} 2x &= x + x \\ &= (x+x)^2 \qquad \text{idempotent} \\ &= x^2 + 2x + x^2 \\ &= x + 2x + x \qquad \text{idempotent} \\ &= 4x \\ &= 2x + 2x \end{aligned}$$

Hence, $2x = 0$ and so $x + x = 0$. Thus, x has period 2 in $(R, +)$.

c. Let $x, y \in R$. Now

$$\begin{aligned} x + y &= (x+y)^2 \qquad \text{idempotent} \\ &= x^2 + xy + yx + y^2 \\ &= x + xy + yx + y \qquad \text{idempotent} \\ &= x + y + (xy + yx) \qquad \text{commutativity of } + \end{aligned}$$

Hence, $xy + yx = 0$ and so $xy = -(yx)$. But in part (b) we showed that any element in $(R, +)$ has period 2, which tells us that $-(yx) = yx$. Therefore, $xy = yx$.

Return to Question 9.1 on P184

Solution 9.2

Let

$$\boldsymbol{S = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R} \right\}.}$$

Prove that S is a subring of $M_2(\mathbb{R})$.

[Note that the S and $M_2(\mathbb{R})$ each have identity elements but they are not the same]

The element $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ acts as an identity element in S as, for all $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in S$ we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}.$$

Now let $A = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix} \in S$. Then

$$A - B = \begin{pmatrix} x - y & 0 \\ 0 & 0 \end{pmatrix} \in S$$

and

$$AB = \begin{pmatrix} xy & 0 \\ 0 & 0 \end{pmatrix} \in S.$$

Hence S is a subring of $M_2(\mathbb{R})$.

Return to Question 9.2 on P184

Solution 9.3

In the lectures we said that $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$. Prove that $\mathbb{Q}(\sqrt{2})$ is a field.

Before tackling a problem like this it is always helpful to have a strategy. Recall that a field is a commutative division ring and that a division ring is a (not necessarily commutative) ring in which every non-zero element is a unit. So, the strategy is to show that $\mathbb{Q}(\sqrt{2})$ is a ring (what's the easy way?) and then demonstrate that it is commutative and that all non-zero elements have multiplicative inverses.

To show that $\mathbb{Q}(\sqrt{2})$ is a ring is straightforward if we note that $\mathbb{Q}(\sqrt{2})$ is a subset of $\mathbb{R}$; all we need to do is show that $\mathbb{Q}(\sqrt{2})$ is a *subring* of $\mathbb{R}$.

i. We have that $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and clearly 1 acts as an identity element in $\mathbb{Q}(\sqrt{2})$.

ii. Let $x = a + b\sqrt{2},\ y = c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2}),\ ;\ a, b, c, d \in \mathbb{Q}$. Then

$$\begin{aligned} x - y &= (a + b\sqrt{2}) - (c + d\sqrt{2}) \\ &= a - c + (b - d)\sqrt{2}\ \in \mathbb{Q}(\sqrt{2}) \qquad \text{as } a - c,\ b - d\ \in \mathbb{Q}. \end{aligned}$$

Hence, $\mathbb{Q}(\sqrt{2})$ is closed under subtraction.

iii. Let $x = a + b\sqrt{2},\ y = c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2}),\ ;\ a, b, c, d \in \mathbb{Q}$. Then

$$\begin{aligned} xy &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ &= (ac + 2bd) + (ad + bc)\sqrt{2}\ \in \mathbb{Q}(\sqrt{2}) \qquad \text{as } ac + 2bd,\ ad + bc\ \in \mathbb{Q}. \end{aligned}$$

Hence, $\mathbb{Q}(\sqrt{2})$ is closed under multiplication.

Thus, by i. to iii. above, $\mathbb{Q}(\sqrt{2})$ is a subring of $\mathbb{R}$ and, hence, a ring.

As mentioned, to now show that $\mathbb{Q}(\sqrt{2})$ is a field, we need to demonstrate that it is commutative and that every non-zero element is a unit.

Clearly commutativity follows from the fact that $\mathbb{Q}(\sqrt{2})$ is a subset of $\mathbb{R}$, and $\mathbb{R}$ is commutative.

Checking that each non-zero element is a unit needs care — we require that all non-zero elements of $\mathbb{Q}(\sqrt{2})$ have an inverse *in* $\mathbb{Q}(\sqrt{2})$.

It is useful, for illustration purposes, to consider a specific, numerical example. Suppose that we consider $1+2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Now consider the conjugate $1-2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Then

$$(1+2\sqrt{2})(1-2\sqrt{2}) = 1^2 - (2\sqrt{2})^2 = 1-8 = -7.$$

Now, it follows that $(1+2\sqrt{2})(1-2\sqrt{2})(-\frac{1}{7}) = 1$ and, hence, we have that

$$(1+2\sqrt{2})^{-1} = \left(-\frac{1}{7}\right)(1-2\sqrt{2}) = \frac{1}{(1^2-(2\sqrt{2})^2)}(1-2\sqrt{2}).$$

Checking:

$$\begin{aligned}(1+2\sqrt{2})\left(-\frac{1}{7}+\frac{2\sqrt{2}}{7}\right) &= -\frac{1}{7}+\frac{2}{7}\sqrt{2}-\frac{2}{7}\sqrt{2}+\frac{4\sqrt{2}}{7}\sqrt{2} \\ &= -\frac{1}{7}+\frac{8}{7} \\ &= \frac{7}{7} \\ &= 1\end{aligned}$$

We now consider the general case. Let $0 \neq x = a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Consider the conjugate $y = a-b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Then $(a+b\sqrt{2})(a-b\sqrt{2}) = a^2-2b^2 \in \mathbb{Q}$. So, in

order to get the identity, 1, from x, we simply need to multiply x by

$$\frac{1}{a^2-2b^2}(a-b\sqrt{2}) \in \mathbb{Q}(\sqrt{2}).$$

But, could $a^2-2b^2=0$?

It is easy to see that the only solution to the equation $a^2-2b^2=0$, with $a,b\in\mathbb{Q}$ is $a=b=0$. Hence, for all $0\neq x=a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$ then $a^2=2b^2\neq 0$ and we have

$$x^{-1}=\frac{1}{a^2-2b^2}(a-b\sqrt{2})\in\mathbb{Q}(\sqrt{2}), \quad \forall\, x\in\mathbb{Q}(\sqrt{2}).$$

So, $\mathbb{Q}(\sqrt{2})$ is a field.

Return to Question 9.3 on P184