Keele UNIVERSITY

MAT-30013: Group Theory

F. Olukoya

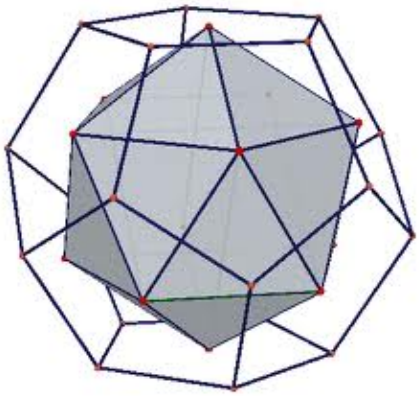


Table of contents

Module Handbook

Welcome to *MAT-30013: Group theory*. This module is an option for Single and combined honours BSc and MMAth and is a pre-requisite for MAT-40018: Topics in Group Theory. A key idea from *MAT-20025: Abstract Algebra* is that groups are an abstraction of symmetry.

This module picks up where MAT-20025 left-off. We go over the essential definitions, introduce canonical examples and continue on to develop a structural understanding of finite groups. The main aim of the course is to give a proof of the seminal Sylow Theorems.

Structure

The module is comprised of the following parts:

1. Equivalence relations;
2. Permutation groups, conjugates and Cayley's Theorem;
3. Group Actions;
4. Normal subgroups and quotient groups;
5. Group homomorphisms and the First Isomorphism Theorem;
6. The Sylow Theorems.

Intended Learning Outcomes (ILO's)

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

- demonstrate knowledge of basic concepts such as abelian groups, normal subgroups,

quotient groups and group actions;

- derive Burnside's Lemma and use it in counting configurations;
- demonstrate knowledge of group homomorphisms and the role of homomorphism as a unifying principle in Group Theory;
- derive and apply the First Isomorphism Theorem;
- demonstrate knowledge of conjugates, centralisers, the Class Equation and Sylow's theorems;
- derive and apply Sylow's First Theorem.

Prerequisites

MAT-20025

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).
- 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.

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

Logistics

Lectures

The lecture material will be delivered by way of 2.5 standard, face-to-face lectures each week (3 in even weeks and 2 in odd). 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 3, 5, 7, 9, and 11 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:

Example Class	Problem Sheet
Week 3	Sheet 1
Week 5	Sheets 2
Week 7	Sheets 3
Week 9	Sheet 4
Week 11	Sheet 5

Table 1: Example classes

Note that there will be no example class covering Problem Sheet 6. Solutions for this problem sheet will be revealed at the appropriate time. Do ensure you attempt the problems and understand the solutions as the content will be examinable. See Table **?@tbl-Exschedule**.

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 3 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.

[ht]

Week Number	Day	Chapter	Material
1	M		
	T	1	Introduction & Equivalence relations
	Thu	1	Equivalence relations & finitely generated groups
2	M	1	Finitely generated groups & Group presentations
	T	2	Permutations & Cayley's Theorem
	Thu	2	Cycle structure & Conjugates
3	M		**Example Class 1**
	T	2	Conjugacy & The 15 puzzle
	Thu	3	An introduction to group actions
4	M	3	Groups acting on sets
	T	3	Orbits and Stabilizers
	Thu	3	Orbit-stabilizer Theorem
5	M		**Example Class 2**
	T	3	Burnside's Lemma and Colouring problems
	Thu	3	Cauchy's Theorem and p-groups
6			
			Reading Week
7	M		**Example Class 3**
	T	4	Normal subgroups, quotient groups and Centres ***(Assignment)***
	Thu	4	Normal subgroups and quotients II
8	M	4	Normal subgroups and quotients III
	T	4	Correspondence Thoerem I ***(Assignment due)***
	Thu	4	Correspondence Theorem II
9	M		**Example Class 4**
	T	4	Normalisers
	Thu	5	Group Homomorphisms
10	M	5	Kernels
	T	5	First Isomorphism Theorem
	Thu	5	Homomorphisms and group actions
11	M		**Example Class 5**
	T	6	The Sylow Theorems: introduction ***(Coursework)***
	Thu	6	Finite p-groups
12	M	6	Centralisers and Sylow's First Theorem
	T	6	Sylow p-subgroups ***(Coursework due)***
	Thu	6	Sylow's Second and Third Theorems
13			***Christmas Vacation***

Table 2: Timetable

Table 3: Timetable

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.

Chapter 1

Introduction and Overview

In this module, we continue the study of groups that we started in second-year Abstract Algebra. We will, as then, concentrate on finite groups. Following a short introduction and reminder of the essential concepts from Abstract Algebra, we will begin by revisiting permutation groups and use these to introduce the concept of a conjugate. Next we study what happens when groups *act* on sets, and follow this with a study of the concepts of normal subgroups and quotient groups. Further exploration of group homomorphisms will bring us to one of the major structural theorems for groups, namely the Isomorphism Theorems, which we will be in a position to prove. Finally, we study the three Sylow theorems, proving the first and considering applications of the second and third.

1.1 Basic ideas

In the second year Abstract Algebra module we gave the formal definition of a group:

Definition 1.1 (Groups)**.** A **group** is a pair $(G, *)$, where G is a non-empty set and $*$ is a binary operation defined on G such that:

i. G is *closed* under $*$, that is

$$\forall\, x, y \in G,\ x * y \in G;$$

ii. $*$ is *associative* on G, that is

$$\forall\, x, y, z \in G,\ x * (y * z) = (x * y) * z;$$

iii. G has an *identity* with respect to $*$, denoted e, that is

$$\exists\, e \in G \text{ such that } \forall\, x \in G e * x = x * e = x;$$

iv. every $x \in G$ has an *inverse* in G, denoted x^{-1}, that is

$$\forall\, x \in G\ \exists\, x^{-1} \in G \text{ such that} x * x^{-1} = x^{-1} * x = e.$$

A group with the additional property that

$$\forall x, y \in G, x * y = y * x$$

is called *abelian*. You were given lots of examples of structures which satisfy the group axioms. Some of these were infinite and abelian (for example $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}\backslash\{0\}, \times)$, and $(\mathbb{C}\backslash\{0\}, \times)$), some were infinite and non-abelian (for example, $GL(n, \mathbb{R})$ under matrix multiplication), some were finite and abelian (for example, $\mathbb{Z}_n$ and $\mathbb{Z}_m^{\times}$), and some were finite and non-abelian (for example, D_n, the group of symmetries of a regular n-gon).

Initially, we would write groups in the form $(G, *)$ to emphasise the fact that a group is a *pair*, namely a set of objects and a binary operation defined on that set. In this module we shall, largely, relax that formality and refer to groups simply by the name of the set where there is no ambiguity with regard to the binary operation.

Definition 1.2 (Subgroup)**.** Let $(G, \times)$ be a group, $H \subseteq G$ (i.e. H is a subset of the elements of G). Then H is a *subgroup* of G if and only if $(H, \times)$ is a group.

In this module we shall use the notation $H \leq G$ to denote that H is a subgroup of G.

To check whether a subset of group elements forms a subgroup we need, in the case of infinite groups, to check that the subset is closed under the group binary operation and that every element of H has an inverse in H. For finite groups we need only check closure.

Lagrange's Theorem states that the order of any subgroup must divide the order of the group. The converse is not true for groups in general, but is true for abelian groups.

Recall that for any group element, the set formed by taking all integer powers of that element forms a subgroup. Notationally, if $(G, \times)$ is a group and $a \in G$, then the set $\{a^n \mid n \in \mathbb{Z}\}$ forms a subgroup of $(G, \times)$ called the cyclic subgroup generated by a and denoted $\langle a \rangle$.

Definition 1.3 (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 1.1.

The group $(\mathbb{Z}, +)$ is cyclic and 1 is a generator.

The group $(\mathbb{R}, +)$ is *not* cyclic.

The subgroup $\{e, s_1\}$ of D_n for any n is cyclic and generated by s_1.

Note that if $(G, \times)$ is a cyclic group with generator a, then the order of G is the same as the *period* of a in G. In addition, note that the order of a cyclic subgroup generated by $a \in G$ is the same as the *period* of a in G. For this reason we shall not refer to the *period* of an element in a group, but, more naturally, to its *order* (though they mean the same thing). Recall, also, that if $(G, \times)$ is a finite group of prime order, then it must be cyclic.

Definition 1.4 (Order of an element)**.** Let $(G, \times)$ be a group with identity element e and consider $a \in G$. If, for all positive integers n, $a^n \neq e$, then a has infinite order. Otherwise,

the *order* of a is the smallest positive integer k such that $a^k = e$.

Example 1.2.

In D_4, r_1 has order 4 since

$$r_1 \circ r_1 \circ r_1 \circ r_1 = r_1^4 = e.$$

In $(\mathbb{Z}, +)$, 1 has infinite order.

An important consequence of Lagrange's theorem is that the order of any element in a group must divide the order of the group.

You were then told that any finite group could be completely described by its operation, or Cayley, table.

	0
0	0

	0	1
0	0	1
1	1	0

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\mathbb{Z}_1$ $\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_4$ $\mathbb{Z}_2 \times \mathbb{Z}_2$

	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

	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

	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

$\mathbb{Z}_5$ $\mathbb{Z}_6$ $S_3 \cong D_3$

Here we have chosen to use the set $\{0, 1, \ldots, n-1\}$ to denote the group elements. This is a natural choice when representing the cyclic group of order n because the Cayley table corresponds to the operation table for addition modulo n, but for the non-cyclic groups, $\mathbb{Z}_2 \times \mathbb{Z}_2$ and S_3, no particular meaning should be ascribed to these symbols. Indeed, we may take any of these groups and replace the symbols with $a, b, c, \ldots$ or Cat, Dog, Goldfish, ... to obtain a group which, although formally different to the original group (because the underlying set is different) is 'essentially the same'. This concept of two structures being 'essentially the same' is called *isomorphism*.

Definition 1.5 (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

a. θ is bijective, and
b. $\forall\, x, y \in G_1$, $\theta(x * y) = \theta(x) \odot \theta(y)$.

An important skill in pure mathematics is to see through the formalism of statements and definitions and understand what is being said. If you do this then concepts will become natural (maybe even obvious) and you will not need to remember very much. Isomorphism is a case in point. If we want to capture the idea that the elements of the Cayley table of one group can be relabelled so as to obtain the Cayley table of another group (subject to some possible rearrangement of the rows and/or columns), then we need to replace each symbol of the first group with a symbol from the second group. This relabelling is exactly what a bijection achieves (make sure you understand why it needs to be both injective and surjective) and, if the resulting Cayley tables are going to be the same, we require the additional property that

$*$	y
	$\vdots$
x	$\cdots \quad z$

$\longmapsto$

$\odot$	$\theta(y)$
	$\vdots$
$\theta(x)$	$\cdots \quad \theta(z)$

Or, in other words, $\theta(x * y) = \theta(x) \odot \theta(y)$. Note that if θ is an isomorphism from G_1 to G_2 then θ^{-1} is an isomorphism from G_2 to G_1, so we say that G_1 and G_2 are isomorphic and write $G_1 \cong G_2$. It is important to understand the relationship between *cyclic* and *abelian*; if a group is cyclic then it is abelian, but the converse does not necessarily hold. Consider $\mathbb{Z}_{12}^{\times}$, which has the following operation table:

$\otimes_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Clearly the group is abelian (since the operation involves only the multiplication of integers), but note that all non-identity elements have period 2, so the group cannot be cyclic (since the generator of a cyclic group must have period equal to the order of the group).

If in Definition 1.5, we remove condition a. then the resulting map θ is what is called a *homomorphism*. In particular, homomorphisms preserve the 'multiplicative structure' but not necessarily the size. More formally, we have:

Definition 1.6 (Homomorphism)**.** Let $(G_1, *)$ and $(G_2, \odot)$ be groups. Then a map $\theta : G_1 \to G_2$ such that

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

is called a *homomorphism*.

> **Note**
>
> An isomorphism is a bijective homomorphism.

Definition 1.7 (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 $H = \{h_1, h_2, \dots, h_m\}$ is finite, then $gH = \{g \times h_1, g \times h_2, \dots, g \times h_m\}$.

Left (or right) cosets are an extremely important concept in this module; in fact, much of the material from Chapter 4 onwards is centred around the idea of groups where the elements of the set are themselves cosets (the so-called quotient groups).

1.2 Equivalence Relations

In first-year Algebra, and Abstract Algebra last year, we used the concept of integers being congruent, or equivalent, to each other modulo some given integer. Formally we have the following:

Definition 1.8 (Congruence of Integers)**.** Let a, b, n be integers, $n > 0$. Then a is *congruent* to b modulo n if and only if $n \mid (b - a)$.

Notationally, we write that $a \equiv b \pmod{n}$. Recall, also, that if two integers are equivalent to each other modulo n, that is the same as saying that they both leave the same principal remainder on division by n. In Abstract Algebra we took this one step further and defined a residue class as follows:

Definition 1.9 (Residue Class)**.** Let a, n be integers, n positive. The *residue class* $[a]_n$ of a modulo n is the set of all integers congruent to a modulo n. (Or, the equivalence class containing a under congruence modulo n.). That is,

$$[a]_n = \{m \mid m \in \mathbb{Z}, m \equiv a \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Example 1.3.

$$[5]_6 = \{5 + 6k | k \in \mathbb{Z}\} = \{..., -7, -1, 5, 11, 17, ...\}$$
$$[0]_5 = \{5k | k \in \mathbb{Z}\} = \{..., -10, -5, 0, 5, 10, ...\}$$

We note two things about these residue classes. First, for any integers a, b, c, then a is in the same class as itself; if a is in the same class as b then b is in the same class as a; if a is in the same class as b and b in the same class as c then a is in the same class as c. Second, for any given n, the classes *partition* the set of integers into disjoint sets where every integer is in exactly one of the residue (or equivalence) classes.

Example 1.4.

Consider $[3]_4$

$$[3]_4 = \{3 + 4k | k \in \mathbb{Z}\} = \{..., -9, -5, -1, 3, 7, 11, 15, ...\}$$

It is clear that 7 is contained in its equivalence class. The following are also straightforward

- as 3 is in the same equivalence class as 19, then 19 is in the same equivalence class as 3;
- As -5 is in the same equivalence class as 7, and 7 is in the same equivalence class as 11, then -5 is in the same equivalence class as 11.

The second property is illustrated below:

$$[0]_3 = \{\dots, -6, -3, 0, 3, 6, 9, \dots\}$$
$$[1]_3 = \{\dots, -5, -2, 1, 4, 7, 10, \dots\}$$
$$[2]_3 = \{\dots, -4, -1, 2, 5, 8, 11 \dots\}$$

So 'equivalence modulo' 3 partitions the integers into three disjoint sets — every integer is in one and only one of the 3 sets.

We can formalise these two ideas as follows.

Definition 1.10 (Relation)**.** A *relation*, R, on a non-empty set S is a non-empty subset of the Cartesian product $S \times S$.

Note that, as a consequence of this definition, R is a set of ordered pairs of elements from S, but rather than specifying a subset R of $S \times S$, it is usual to specify a rule for when $(a, b) \in R$, where $a, b \in S$. We write aRb rather than $(a, b) \in R$ and read this as a *is related to* b *(under the relation* R*).*

Example 1.5. The following are examples of relations.

a. Let $S = \{1, 2, 3, 4, 5, 6, 7\}$ and define a relation on S such that for all $a, b \in S$, $aRb \Leftrightarrow \frac{a-b}{2} \in \mathbb{Z}$.

   So $1R1$ as $(1-1)/2 = 0 \in \mathbb{Z}$; $2R6$ as $(2-6)/2 = -2 \in \mathbb{Z}$. However, $3 \not R 4$ since $(3-4)/2 = -1/2 \notin \mathbb{Z}$.

b. Define the relation $R = \{(x, y) \mid x \in \mathbb{Z}^+, y \in \mathbb{Z}^+, x \neq y \text{ and } x^y = y^x\}$. What does R contain?

   In fact R is finite and has only 2 elements:

$$R = \{(2, 4), (4, 2)\}.$$

Definition 1.11 (Equivalence Relation)**.** A relation, R, on a non-empty set S is said to be an *equivalence relation* if and only if, for all $a, b, c \in S$,

i. aRa for all $a \in S$ (the relation is *reflexive*) and
ii. whenever aRb, then bRa (the relation is *symmetric*) and
iii. whenever aRb and bRc, then aRc (the relation is *transitive*).

Definition 1.12 (Partition)**.** A *partition* of a set, S, is a collection, P, of non-empty subsets of S such that every element of S is in exactly one member of P.

Note that each member of P is, in itself, a set.

Theorem 1.1. *Let R be an equivalence relation defined on a set S and define*

$$[a] = \{b \in S \mid bRa\}.$$

Then, $\{[a] \mid a \in S\}$ is a partition of S.

Proof.

We need to show that every element of S belongs to one of these sets and also that any two such sets which have an element in common must in fact be equal.

Let $a \in S$ be arbitrary. Since R is an equivalence relation, it is reflexive and so aRa holds. Therefore, by definition, $a \in [a]$. Since a was arbitrarily chosen, we conclude that for all $a \in S$ $a \in [a]$.

Now let $a, b \in S$ and suppose that $[a]$ and $[b]$ have a point c in common, that is

$$c \in [a] \cap [b].$$

Let $a' \in [a]$ be chosen arbitrarily. Since a' and c' are in $[a]$ it follows that $a'Ra$ and cRa. Since R is a symmetric relation we deduce that aRc is true as well. Since R is transitive, the statements $a'Ra$ and aRc now mean that $a'Rc$. Using the fact that $c \in [b]$ we have cRb.

Applying symmetry again we deduce that bRc is true also. Transitivity, from the statements $a'Rc$ and cRb, now implies that $a'Rb$. By definition it follows that $a' \in [b]$. Since $a' \in [a]$ was arbitrarily chosen we conclude that $[a] \subseteq [b]$.

Swapping the roles of $[a]$ and $[b]$ above, we see that $[b] \subseteq [a]$ as well. Therefore $[a] = [b]$ as required.

□

We will often refer to each of the members of a partition as an *equivalence class*. Note that, as a consequence of the above, residue classes are defined by an equivalence relation on the set of integers and, therefore, partition the set of integers. We now return to the property of isomorphism. It is obvious that any group is isomorphic to itself. Furthermore, if θ is an isomorphism from G_1 to G_2 then we have noted that θ^{-1} is an isomorphism from G_2 to G_1; so if $G_1 \cong G_2$ then $G_2 \cong G_1$. An extension of this argument then leads us to the conclusion that if $G_1 \cong G_2$ and $G_2 \cong G_3$, then $G_1 \cong G_3$. Thus isomorphism is an equivalence relation on the collection of all groups (the collection of all groups is technically not a proper set). Now let us consider left coset formation. You will recall that we used a direct argument in Abstract Algebra to show that left cosets partition the group elements (and, along with two other properties we used this to prove Lagrange's Theorem). This means, therefore, that left coset formation must be an equivalence relation on the set of group elements and if we can define such an equivalence relation we would have an alternative proof to Lagrange's Theorem. So, let G be a finite group and H be a subgroup of G. Consider $a, b \in G$. We need to find a relation that describes the property of a and b lying in the same left coset of H as each other, that is, a is related to b if and only if both a and b are in the same left coset of H in G. Now, since for any subgroup H we have that $e \in H$, it follows that a and b are in the same left coset of H in G if and only if $aH = bH$ and, hence, $ah_1 = bh_2$ for some $h_1, h_2 \in H$. Now,

$$
\begin{aligned}
& ah_1 = bh_2 \\
\iff & a = bh_2h - 1^{-1} \\
\iff & b^{-1}a = h_2h_1^{-1} \\
\iff & b^{-1}a \in H
\end{aligned}
$$

The last step follows from the fact that if $h_1, h_2 \in H$, then since H is itself a group it is closed under product and inverse and, hence, $h_2h_1^{-1} \in H$. Then it follows that $b^{-1}a \in H$ and, hence, we must have that for any two group elements x and y, they are in the same coset if and only if $y^{-1}x \in H$, for the given subgroup H. (This is just a relabelling where $x = a$ and $y = b$). So we can now define our relation that results in coset formation as follows: let H be a subgroup of a finite group G and let $x, y \in G$, then xRy if and only if $y^{-1}x \in H$. We now need to show that this is indeed an equivalence relation.

- **Reflexive**:

$$x^{-1}x = e \in H \implies xRx \forall x \in G$$

- **Symmetric**:

$$y^{-1}x \in H \iff (y^{-1}x)^{-1} \in H \iff x^{-1}y \in H \iff yRx$$

- **Transitive**:

  Suppose xRy and yRx, then $y^{-1}x \in H$ and $z^{-1}y \in H$. This means that $(z^{-1}y)(y^{-1}x) \in H$. Therefore $z^{-1}x \in H$ and xRz.

We have established that left coset formation is an equivalence relation, so we now know that it must partition the group. We also know, from Abstract Algebra, that the size of

every coset is equal to the size of H and, therefore, we can conclude that the size of H must divide the size of G.

The above also gives us a checking lemma to determine whether two left cosets are equal. It uses the fact that two left cosets are either disjoint or identical and that $g \in gH$.

Lemma 1.1. *Let H be a subgroup of G and $g_1, g_2 \in G$. Then*

$$g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H.$$

Proof.

Suppose $g_1H = g_2H$. Note that $g_2 \in g_2H$ since $g_2 = g_2e$ and $e \in H$. Since $g_1H = g_2H$ there is an element $h \in H$ such that $g_1h = g_2$. Therefore $h = g_1^{-1}g_2$ and so $g_1^{-1}g_2 \in H$ as required.

On the other hand, suppose $g_1^{-1}g_2 \in H$. Let $h \in H$, then

$$g_1h = eh = (g_2g_2^{-1})g_1h = g_2(g_2^{-1}g_1)h = g_2((g_2^{-1}g_1)h) \in g_2H$$

since $g_2^{-1}g_1 = (g_1^{-1}g_2)^{-1} \in H$. Similarly,

$$g_2h = g_1(g_1^{-1}g_2)h \in g_1H.$$

Since $h \in H$ was chosen arbitrarily, we conclude that $g_1H = g_2H$.

□

1.3 An Idea of What is to Come

Earlier we presented the Cayley tables of all the isomorphically distinct groups up to order 6, by which we mean that any group of order less than or equal to 6 is isomorphic to exactly one group in that list. The fundamental problem of Group Theory is to produce such a

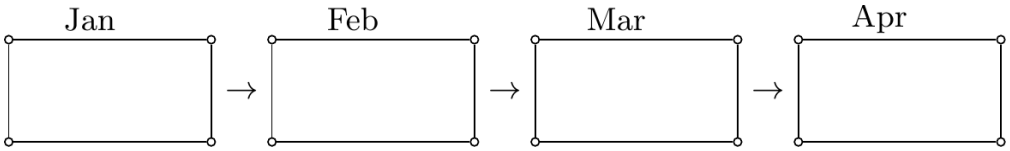
catalogue for all groups, or perhaps just all finite groups. Clearly it is not possible, nor particularly helpful, to produce an infinite list of Cayley tables, but for a given order n can we describe or generate all of the isomorphically distinct groups of that order? We know this is possible for all of the finite abelian groups, by way of the Fundamental Theorem of Finite Abelian Groups, so, it is the non-abelian groups that cause all the trouble in terms of trying to establish a classification. The most celebrated result in Group Theory is the classification of all finite simple groups. Simple groups will be defined later, but are the building blocks of all finite groups in much the same way that the primes are the building blocks of the positive integers. This classification theorem is the result of over 100 years' work by thousands of group theorists and it is estimated that its complete proof (if ever assembled in one place) would require about 20,000 pages! In this module we will prove some classification and structure theorems, but we will also look at how groups arise naturally (albeit in some unexpected places). In doing so we shall be looking at the forms that different groups can take - in particular their actions, presentations and representations. The first unexpected place that group theory arises is in the bedroom….

1.4 Generators

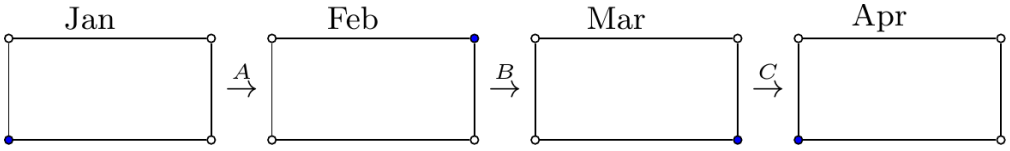
1.4.1 The Mattress Problem

Good mattresses are expensive. Being a frugal individual I wish to maximise the amount of use that I get from my mattress so it is necessary to turn the mattress at regular intervals (say once a month) so as to promote uniform wear. Obviously any turning of the mattress must result in the mattress fitting back onto the bed as intended and, therefore, we can consider this problem in terms of the symmetries of a rectangle (assuming that the mattress is not square!) where the mattress represents the rectangle and the base of the bed represents the two-dimensional plane. Now, we know that the symmetry group of a rectangle is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (there are only two groups, up to isomorphism, of order 4 and the other is cyclic) and hence there are four positions for the mattress, or one per month for a four-month period. The symmetries are a rotation of 180° degrees, a 'flip' about the short axis, and a

'flip' about the long axis. Suppose we designate as A the 180° rotation (where the mattress remains face up), as B the 'flip' in the long axis of symmetry, and as C the 'flip' in the short axis of symmetry. What is the best sequence of moves for the mattress?

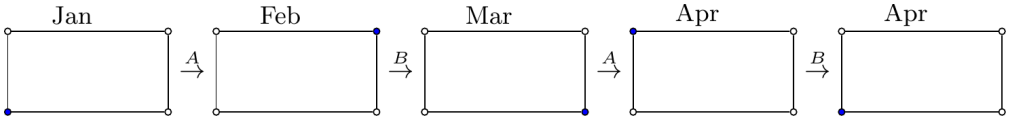


We could try each move in turn:



This is not a good solution since the initial configuration of the mattress is repeated at the end — a configuration is missing,

A better solution, which does not use C, but gives even cover is: $ABABABA\ldots$



1.4.2 Finitely Generated Groups

In the Abstract Algebra module we found that the set of integer powers of an element of a group, G, generates a *cyclic subgroup* of G. If a is an element of G, and has finite period k in G, then this subgroup is

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}.$$

Since this subgroup has order k, the element a has order k (some authors write $|a| = k$). If there is an element $a \in G$ such that $\langle a \rangle = G$, then, as we know, G is a *cyclic group* and a is a *generator* of G. Clearly $\langle a \rangle$ is the smallest subgroup of G containing a in the sense that every subgroup of G which contains a must also contain $\langle a \rangle$. We can generalise this to any subset of elements of G.

We can generalise this to the following:

Definition 1.13. Let G be a group and let $S = \{a_1, a_2, ...\}$ be a subset of the elements of G. The subgroup generated by S is the smallest subgroup of G containing S (we denote this $\langle S \rangle = \langle a_1, a_2, ... \rangle$. If this subgroup is all of G then S generates G and the a_i are generators of G. If there is a finite set, S, which generates G, then G is *finitely generated*.

So, given a group G and a subset of elements S, what does the subgroup generated by S look like? The following theorem answers this question.

Theorem 1.2. *If G is a group and $S = \{a_1, a_2, ...\}$ a subset of the elements of G, then the subgroup $\langle S \rangle$ of G consists of those elements of G that are finite products of integral powers of the a_i (where powers of a given a_i may occur several times in the product).*

Proof.

First observe that a finite product of integral powers of elements of S must be contained in $\langle S \rangle$ since S is contained in $\langle S \rangle$. It therefore suffices to show that the set H of finite produces integral powers of elements of S is a subgroup of G. This is because the set H would then be a subgroup of G containing S that is a subset of $\langle S \rangle$, as $\langle S \rangle$ is the smallest subgroup of G containing S it must therefore be equal to H.

We check the subgroup criteria hold for H.

i. For any $a \in S$, $a^0 = e \in H$, so H is non-empty and contains the identity of G.
ii. By definition H is closed under products.
iii. H is closed under inverses since the inverse of a finite product of integral powers of elements of S is again a finite product of integral powers of elements of S.

□

Example 1.6.

Consider D_4. Note that D_4 is not a cyclic group since it cannot be generated by a single element (the order of D_4 is 8 and the order of an element of D_4 is either 2 or 4). However D_4 can be generated using a proper subset of elements of D_4.

$\circ$	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

Let $S = \{r_1, s_2\}$. Now the set of integral powers of r_1 is precisely $\{e, r_1, r_2, r_3\}$. To obtain the reflections s_1, s_3 and s_4 observe that

$$r_1 s_2 = s_1$$

$$r_1 s_1 = s_4$$

$$r_1 s_4 = s_3$$

We conclude that $\langle r_1, s_2 \rangle = D_4$ and D_4 is finitely generated.

1.5 Presentations

In essence, a group presentation is a notation that describes a group in terms of its generators and relations that hold between them. We begin with a definition.

Definition 1.14 (Presentation)**.** A group can be described concisely by the notation

$$\langle a, b \ldots \mid \text{list of relations between a, b, ... , and their powers} \rangle,$$

where the first part is a list of generators for the group and the second is a list of the relations that generate all the relations that hold between the generators. This notation is called a *presentation* of the group.

Example 1.7. Consider the presentation

$$\langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle.$$

The generators both have order 2 and commute. This means that any finite product integral powers of the generators a, b can be reduced, using the relations, to the form $a^i b^j$ where $i, j \in \{0, 1\}$. Computing the operation table:

$*$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Observe that the group is abelian and is in fact isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 1.8. Consider the presentation

$$\langle a, b \mid a^3 = b^2 = 1, ab = ba^{-1} \rangle.$$

The generator a has order 3 and so has inverse a^2; the generator b has order 2 and is its own inverse. The relation $ab = ba^{-1}$ means we can move b to the left of a at the cost of replacing a with its inverse. Consequently, by repeatedly moving b's to the left of a's any

finite product of integral powers of a and b can be written in the from $b^i a^j$ where $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$.

We can compute the operation table.

$*$	1	a	a^2	b	ba	ba^2
1	1	a	a^2	b	ba	ba^2
a	a	a^2	1	ba^2	b	ba
b	b	ba	ba^2	1	a	a^2
ba	ba	ba^2	a^2	1	a	b
ba^2	ba^2	b	ba	a	a^2	1

Clearly this group is not abelian since $ba \neq ab = ba^2$.

Looking at the above two presentations, we can see that the first is clearly abelian (because there are only two generators a and b and $ab = ba$), whereas the second is clearly non-abelian (because $ab = ba^{-1}$ and $a^{-1} \neq a$). In each case it was also easy to determine the order of each group and write out the group elements in some form. In the next two examples this is not so obvious.

Example 1.9. $\langle a, b \mid a^2 = b^2 = 1, (ab)^3 = 1 \rangle$.

Notice that a and b both have order 2 in this case. Further observe that since $ababab = 1$ then $bab = aba$. Thus $baba = bbab = ab$ and $abab = babb = ba$. Any finite product of integral powers of a and b can be written as a product of a and b's. Moreover, such a product cannot have consecutive a's or consecutive b's. Using the observation $baba = ab$ and $abab = ba$ we notice that such a product cannot exceed length 3. This leaves products of the form a, ab, aba, b, ba. The multiplication table is now

$*$	1	a	b	ab	ba	aba
1	1	a	b	ab	ba	aba
a	a	1	ab	b	ab	ba
b	b	ba	1	aba	a	ab
ba	ba	b	aba	1	ab	a
aba	aba	ab	ba	a	b	1

Note that is group is isomorphic to D_3. The reflections are a, b and aba and the rotations are powers of ab.

Example 1.10. $\langle a, b \mid b^2a = b, ba^2b = a\rangle$.

This group is the trivial group. From $b^2a = b$ we find that $ba = 1$. From $ba^2b = a$ we find that $ab = a$ and so $b = a$. Using $ba = 1$ we see that $a = 1$ as well.

A good presentation provides an efficient description of a group. For example, the dihedral group of order $2n$, which is isomorphic to the symmetry group of a regular n-sided polygon, can be defined by the presentation

$$D_n = \langle a, b \mid a^n = b^2 = 1, ba = a^{-1}b\rangle.$$

It is easy to see that any product must belong to the set $\{1, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$ and any product may be reduced to an element of this set by reducing powers of a modulo n, powers of b modulo 2, and bringing the a's to the left, replacing a with a^{-1} when it 'hops over' a b.

Example 1.11.

For D_6 we have

$$\langle a, b \mid a^6 = b^2 = 1, ba = a^{-1}b\rangle .$$

Given a product, for instance $a^{11}b^3a^2b^{-1}a^{-1}b^4a$, we can apply the relation to reduce it to

the form $a^i b^j$ for $0 \leq i \leq 5$ and $0 \leq j < 2$.

$$\begin{aligned} a^{11}b^3a^2b^{-1}a^{-1}b^4a &= a^5ba^2b \\ &= a^5a^{-2}b^2 \\ &= a^3 \end{aligned}$$

1.6 Free Groups and the Word Problem

Informally the *free group* on a (possibly infinite) set of generators $\{a, b, c, ...\}$ consists of all finite products involving integer powers of the generators where there are no relations to tell us how to reduce products, with the obvious exception that, for example, $ab^2b^{-3}a = ab^{-1}a$ etc. The products formed in this way are called *words*. Fundamentally, all groups can be thought of as consisting of infinitely many words but, using relations, we may be able to reduce each of these to a member of a (possibly finite) set. As we have seen, things are not always this easy. For a given presentation it can be difficult to determine the order of the group or even whether it is finite or infinite. This is summed up by the so called Word Problem for groups. The Word Problem is to find an algorithm which will determine whether two words represent the same element. We have such an algorithm for the dihedral group D_n because we have a way of reducing any given word to one of the $2n$ elements of $\{1, a, a^2, ..., a^{n-1}, b, ab, a^2b, ..., a^{n-1}b\}$. Hence two words are equal if and only if they reduce to the same element. It is hard to imagine that this would not be the case for any group presentation, but remarkably the Word Problem is known to be unsolvable in general.

1.7 Revision Sheet

This is a revision sheet and covers material from Abstract Algebra.

Question R.1

Define $*$ on $\mathbb{R}\backslash\{0\}$ by $a*b = |a|\,b$ (so, for example $2*3 = 6, -2*3 = 6, 2*(-3) = -6$ etc.).

i. Show that $*$ is an associative binary operation on $\mathbb{R}\backslash\{0\}$.

ii. Show that there is an element $e \in \mathbb{R}\backslash\{0\}$ such that $e * x = x,\ \forall\, x \in \mathbb{R}\backslash\{0\}$.

iii. Show that $\forall\, x \in \mathbb{R}\backslash\{0\}$, $\exists\, x^{-1} \in \mathbb{R}\backslash\{0\}$ such that $x * x^{-1} = e$.

iv. Is $(\mathbb{R}\backslash\{0\}, *)$ a group?

Show Solution R.1 on P140

Question R.2

If H is a subgroup of a finite group G then the *right coset* of H by g is denoted and defined by

$$Hg = \{hg \,|\, h \in H\}.$$

Prove Lagrange's Theorem using right cosets (the proof using left cosets was given in the second year Abstract Algebra module). In other words, show that every right coset, Hg, of H is the same size as H, that two right cosets of H are either disjoint or equal, and that every element of G is in a right coset of H. Finally deduce that the order of H divides the order of G.

Show Solution R.2 on P141

Question R.3

Let G be a group and H the subset of G consisting of the identity e and all elements of G of order 2, so $H = \{h \in G | h^2 = e\}$. Show that:

i. if G is abelian, then H is a subgroup of G,

ii. if G is non-abelian, then H is not necessarily a subgroup of G.

Show Solution R.3 on P143

Question R.4

Show that if H and K are subgroups of an abelian group G, then

$$HK = \{hk \,|\, h \in H, k \in K\}$$

is a subgroup of G. Is this true for non-abelian groups?

Show Solution R.4 on P144

Question R.5

Let $(G_1, \times)$ and $(G_2, \circ)$ be groups and $\theta : G_1 \to G_2$ an isomorphism. Prove that H is a subgroup of G_1 if and only if $\theta(H) = \{\theta(h) \,|\, h \in H\}$ is a subgroup of G_2.

Show Solution R.5 on P145

Question R.6

Show that if G is an abelian group then

$$\{g^2 \,|\, g \in G\}$$

is a subgroup of G, but this is not true for groups in general.

Show Solution R.6 on P146

Question R.7

We know that every proper subgroup of a cyclic group is itself cyclic. State the converse and give a counter example to demonstrate that the converse is false.

Show Solution R.7 on P147

Question R.8

In each of the following cases, find the order of the given element in the direct product:

i. $(3, 7)$ in $\mathbb{Z}_9 \times \mathbb{Z}_{14}$;

ii. $(8, 11)$ in $\mathbb{Z}_{10} \times \mathbb{Z}_{15}$;

iii. $(3, 7, 12)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$.

Show Solution R.8 on P148

Question R.9

i. Write down all of the generators of

   a. $\mathbb{Z}_{14}$,

   b. $\mathbb{Z}_{15}$.

ii. Classify, according to the Fundamental Theorem of Finite Abelian Groups, all of the abelian groups of orders

   a. 54,

   b. 600.

iii. In part ii.a. above, state which of the groups of order 54 is cyclic and which is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_9$.

Show Solution R.9 on P148

1.8 Problem Sheet 1

For the example class in Week 3; covers Chapter 1 material. At minimum you should attempt questions 1.4, 1.5 and 1.7.

Question 1.1

Let R be a relation on a non-empty set, S

a. Define a relation on $\mathbb{Z}^+$ by, for $x, y \in \mathbb{Z}^+$, xRy if and only if x and y have the same number of digits in the usual base 10 notation. Show that this is an equivalence relation.

b. Find the equivalence class containing 37.

Show Solution 1.1 on P150

Question 1.2

Define a relation on $\mathbb{R}$ by, for $a, b \in \mathbb{R}$, aRb if and only if $|\,a\,| = |\,b\,|$. Is this an equivalence relation? If so, how does it partition the set?

Show Solution 1.2 on P150

Question 1.3

Define a relation that partitions the plane into the origin and all circles centred at the origin with radius $r \in \mathbb{R}$. Prove that this is an equivalence relation.

Show Solution 1.3 on P151

Question 1.4

In the group

$$\langle A, B, C \,|\, A^7 = B^3 = C^2 = 1, BA = A^3B, CA = AC, CB = B^2C \rangle$$

express each of the following in the form $A^r B^s C^t$:

i. $(BC)^2$;

ii. B^2A^3;

iii. C^3B^{-2};

iv. $(AB)^3$;

v. $(ABC)^{-1}$.

Show Solution 1.4 on P152

Question 1.5

Let $G = \langle a, b, c \,|\, a^4 = b^3 = 1, ab = ba, ac = ca, bc = cb \rangle$. Classify G according to the Fundamental Theorem.

Show Solution 1.5 on P154

Question 1.6

If $G = \langle a, b \,|\, ab = ba, a^4 = b^3 = 1 \rangle$ and H is the cyclic subgroup generated by b, classify G according to the Fundamental Theorem, and find the left and right cosets of H in G.

Show Solution 1.6 on P155

Question 1.7

In the dihedral group $D_5 = \langle a, b \mid a^5 = 1, b^2 = 1, ab = ba^{-1} \rangle$, simplify:

i. $a^7b^3a^{-2}baba^3ba^2a^7b^2a$;

ii. $a^{13}b^5a^2b^{-7}a^2ba$.

Show Solution 1.7 on P155

Question 1.8

In $(\mathbb{Q}, +)$, describe the elements of $\langle \frac{1}{2} \rangle$ and $\langle \frac{1}{2}, \frac{1}{3} \rangle$. Show that $(\mathbb{Q}, +)$ is not finitely generated.

Show Solution 1.8 on P156

Chapter 2

Permutations

You will recall that we studied permutations in Abstract Algebra. A permutation is a bijective mapping from a set to itself. Since permutations are important in the study of finite groups we will start our investigation of group classification by expanding on what we learned about permutations in the Abstract Algebra module. Remember that we were able to represent permutations first as disjoint cycles and then as products of transpositions. The number of transpositions in a product determines whether the permutation is even or odd (it cannot be both). We used cycle (orbit) lengths to calculate the order (period) of a permutation in its group.

Example 2.1. Consider the permutation

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

We can express f as a product of disjoint cycle (recalling that we ignore singletons)

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

We can express f as a product of transpositions as:

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

Thus f is an even as it can be written as a product of an even (6 in this case) number of transpositions.

2.1 Cayley's Theorem

Cayley's Theorem tells us that every finite group is isomorphic to some group of permutations. One way of seeing this is to simply read off the rows of the Cayley table for a group as permutations of the elements themselves.

Example 2.2. Consider the group given by the Cayley table below.

	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

$$0 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \quad 1 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 0 & 5 & 3 & 4 \end{pmatrix} \quad 2 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 0 & 1 & 4 & 5 & 3 \end{pmatrix}$$

$$3 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 0 & 1 & 2 \end{pmatrix} \quad 4 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 0 & 1 \end{pmatrix} \quad 5 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 & 0 \end{pmatrix}$$

We say that we have *represented* the group as a group of permutations. Notice that we can

represent each of the group elements by the permutation of the column border defined by its row. Consider the group element 2 above. If we pre-multiply by 2 each of the elements of the group in their column border order, then we get the elements re-ordered as in row 2. That is,

$$2 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 0 & 1 & 5 & 3 & 4 \end{pmatrix}$$

Of course, the elements of the group do not have to be numbers.

Example 2.3. Consider the group of symmetries of a rectangle:

$\circ$	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

In the same way as in Example 2.2, we can express r_π, for example, as a permutation:

$$r_\pi \mapsto \begin{pmatrix} e & r_\pi & s_1 & s_2 \\ r_\pi & e & s_2 & s_1 \end{pmatrix}.$$

In both of the above examples, and in general, we replace $g \in G = \{g_1, g_2, \dots, g_n\}$ by the permutation

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix}$$

This is called the *left regular representation* of g and is denoted λ_g. So, we have that $\lambda_g(x) = gx, \ \forall x \in G$. It is important to note, at this point, that when we say that every finite group is isomorphic to a group of permutations we do not necessarily mean the full symmetry group itself; it is more likely to be a subgroup of the full symmetry group (for example, D_4 has order 8 but there is no S_n with order 8 for any n and so D_4 will be

isomorphic to some subgroup of S_4 of order 8).

Theorem 2.1 (Cayley's Theorem)**.** *Every finite group is isomorphic to a group of permutations.*

Proof.

For each $a \in G$ define $\lambda_a : G \to G$ by $x \mapsto ax$. Notice that λ_a is a permutation of G since it has an inverse $\lambda_{a^{-1}}$.

Set $G' = \{\lambda_a \mid a \in G\}$. Then G' is a subgroup of the group of permutations of G. This follows as for $a, b \in G$:

$$\begin{aligned} \lambda_a \circ \lambda(b)(x) &= \lambda_a(bx) \\ &= abx \\ &= \lambda_{ab}(x) \end{aligned}$$

for all $x \in G$. Therefore $\lambda_a \circ \lambda_b = \lambda_{ab} \in G$. Further observe that $|G'| = |G|$. This is because for $a, b \in G$ with $a \neq b$, $\lambda_a \neq \lambda_b$. For instance $\lambda_a(e) = a \neq b = \lambda_b(e)$.

Let $\theta : G \to G'$ be the map defined by $\theta(a) = \lambda_a$ for all $a \in G$. Then θ is a bijection. Thus, to see that θ is an isomorphism, we only need show that it is a homomorphism. Let $a, b \in G$,

$$\theta(ab) = \lambda_{ab} = \lambda_a \circ \lambda_b = \theta(a) \circ \theta_b.$$

Therefore θ is a homomorphism and so an isomorphism.

Lastly observe that the group of permutations of G is isomorphic to $S_{|G|}$. We conclude that G is therefore isomorphic to a subgroup of $S_{|G|}$.

□

Notice what we did in that proof. First, we demonstrated that for each $a \in G$ then λ_a is indeed a permutation and we did that by showing that λ_a is a bijective function from G to

itself (because the set is finite it is sufficient to show injectivity). Second, we took the set of all λ_a, for a given $a \in G$, and demonstrated that this set forms a subgroup of S_n (as the set is finite we need only show closure). Third, we defined a function, θ, mapping from our group G to the subgroup of S_n (which we denoted G'), and proved that was an isomorphism in the usual way. A reasonable question to ask at this point is why study abstract groups at all? If every finite group is isomorphic to some group of permutations then why not just study permutation groups? Well, often we do study groups via permutations, but any given finite group can be represented by permutation groups in infinitely many different ways and it is not always obvious which way is the most convenient or appropriate. For example, notice that the group in Example 2.2 is, in fact, isomorphic to S_3, the symmetric group of order 6, and yet the proof of Cayley's Theorem represents the group as a subgroup of S_6. Secondly there are lots of other ways of representing groups and some ways are better than others depending on what we are trying to do or find out. The permutations above have been written in two row notation. We will usually adopt cycle notation and because permutations are functions, and multiplication of permutations is function composition, we will compose (or multiply) permutations from right to left (as you did in the Abstract Algebra module).

Example 2.4.

Returning to Example 2.2 once more. We compute $\lambda_2 \circ \lambda_3$:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 0 & 1 & 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 0 & 1 \end{pmatrix}.$$

Thus $\lambda_2 \circ \lambda_3 = \lambda_4$.

We can express this in cycle notation.

$$(0\ 2\ 1)(3\ 4\ 5)(0\ 3)(1\ 4)(2\ 5) = (0\ 4)(1\ 5)(2\ 3).$$

2.2 Cycle Structure

Recall that the *symmetric group of degree* n is the set of **all** permutations of n things (usually the numbers from 1 up to n). The group is denoted S_n and since there are $n!$ ways to permute or order n objects, then we have that $|S| = n!$. The *cycle structure* of a permutation is its structure as a collection of *disjoint* cycles which can be described by replacing each of the symbols with a $*$. For example, the cycle structure of $(1\ 2)(3\ 4\ 5)(6\ 7)$ is $(* *)(* * *)(* *)$, which we can also write as $(* *)(* *)(* * *)$ or even $(* *)^2(* * *)$, remembering that disjoint cycles commute. Permutations with the same cycle structure have similar properties, for example they have the same order because the order of any permutation is the lowest common multiple of the lengths of its disjoint cycles.

Example 2.5.

The possible cycle structures in S_3 are:

$$I, (* *), (* * *).$$

For a 2-cycle, there are 3 choices for the first element and then 2 for the second giving a total of six 2-cycles:

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

However, a the cycles $(a\ b)$ is the same as the cycle $(b\ a)$. Therefore, we have a total of 3 distinct 2-cycles:

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

In a similar way there are $3!/3 = 2$ distinct 3-cycles. Since the total number of 3-cycles is $3!$, we divide by 3 to get the number of distinct cycles since we have the equalities

$$(a\ b\ c) = (b\ c\ a) = (c\ a\ b)$$

for a cycle $(a\ b\ c)$.

So

$$S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Note that $|S_3| = 3! = 6$.

For S_4 we haven:

Structure	number
I	1
$(* *)$	$6 = \frac{4\times3}{2}$
$(* * *)$	$8 = \frac{4\times3\times2}{3}$
$(* * **)$	$6 = \frac{4\times3\times2}{4}$
$(* *)(* *)$	$3 = \frac{4\times3\times2}{2\times2\times2}$

Notice that

$$|S_4| = 1 + 6 + 8 + 6 + 3 = 24 = 4!.$$

2.3 Conjugates

We begin with a definition.

Definition 2.1 (Conjugate)**.** If a and b are permutations (defined on the same set) then *the conjugate* of a by b is the permutation bab^{-1}.

Later we shall extend the definition of conjugacy, in the obvious way, to group elements in general but for now we concentrate on permutations and hopefully get some idea as to why conjugacy is such a useful concept.

Example 2.6.

Let $a = (1\ 2\ 3)(4\ 5), b = (1\ 6\ 2\ 4\ 3) \in S_6$. The the conjugate of a by b is:

$$bab^{-1} = (1\ 6\ 2\ 4\ 3)(1\ 2\ 3)(4\ 5)(1\ 3\ 4\ 2\ 6) \tag{2.1}$$

$$= (1\ 6\ 4)(3\ 5) \tag{2.2}$$

Note that a and bab^{-1} have the same cycle structure:

$$(*\ *\ *)(*\ *).$$

Less obvious is the fact that bab^{-1} can be obtained from a by replacing each element in each cycle of the disjoint cycle of a by its image under b. That is:

$$a = (1\ 2\ 3)(4\ 5) \tag{2.3}$$

$$bab^{-1} = (b(1)\ b(2)\ b(3))(b(4)\ b(5)) \tag{2.4}$$

$$= (6\ 4\ 1)(3\ 5) \tag{2.5}$$

$$= (1\ 6\ 4)(3\ 5). \tag{2.6}$$

The next theorem demonstrates that the above holds true in general.

Theorem 2.2. *The conjugate of* $a = (x_1\ x_2\ \ldots\ x_r)(y_1\ y_2\ \ldots\ y_s)\ldots(z_1\ z_2\ \ldots\ z_t)$ *by* b *is*

$$c = (b(x_1)\ b(x_2)\ \ldots\ b(x_r))(b(y_1)\ b(y_2)\ \ldots\ b(y_s))\ldots(b(z_1)\ b(z_2)\ \ldots\ b(z_t)),$$

where a *has been expressed as a product of disjoint cycles.*

Proof.

It suffices to show that $ba = cb$ since, post-multiplying by b, this implies that $bab^{-1} = c$.

Let x be an element *not* fixed by a. Without loss of generality we may assume that $x = x_1$.

We then have:

$$ba(x_1) = b(x_2)$$
$$cb(x_1) = b(x_2)$$

If x is fixed by a then:

$$ba(x) = b(x)$$
$$cb(x) = b(x)$$

Hence, $ba = cb$ as required.

□

Definition 2.2 (Conjugacy)**.** Let a, b and c be permutations (defined on the same set). Then a is *conjugate to* c means that there exists a permutation b such that $c = bab^{-1}$.

If c is the conjugate of a by b, then a is the conjugate of c by b^{-1}. This can be seen as follows:

$$c = bab^{-1} \tag{2.7}$$
$$\iff b^{-1}c = ab^{-1} \tag{2.8}$$
$$\iff b^{-1}cb = a. \tag{2.9}$$

This show that the relation R on a group G that relates two elements whenever they are conjugate to to one another is symmetric. One can show that this relation is reflexive and transitive and, consequently, is an equivalence relation.

Corollary 2.1. *Two permutations are conjugate if and only if they have the same cycle structure.*

Proof.

This follows from the proof of Theorem 2.2.

□

Example 2.7.

Let $a = (1\ 5\ 2\ 4)(3\ 7)$ and $c = (1\ 6)(2\ 4\ 3\ 5)$ be elements of S_7. Clearly a and c have the same cycle structure and so must be conjugate. We can find an element in S_7 that conjugates a to c by finding an element b satisfying

$$(b(1)\ b(5)\ b(2)\ b(4)) = (2\ 4\ 3\ 5) \tag{2.10}$$

$$(b(3)\ b(7)) = (1\ 6). \tag{2.11}$$

For example $b = (1\ 2\ 3)(4\ 5)(6\ 7)$ works.

2.4 The 15-Puzzle

The original 15-puzzle is a tray with 15 numbered tiles that are free to slide into a single blank space but may not be removed from the tray.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

After jumbling the pieces thoroughly the object is to bring them back into the above *solved state*. This puzzle was marketed by the American puzzle maker Sam Loyd in the 1890s, the resulting craze was fuelled by Loyd's offer of a $1,000 prize for anyone who could solve the

puzzle starting from the state with 14 and 15 swapped.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

One way to model this problem is to treat the blank space as tile number 16. The solution requires us to express the transposition $(14\ 15)$ as a product of transpositions each involving 16. Of course not all transpositions with 16 are allowed, for example our first move must be either $(12\ 16)$ or $(14\ 16)$ but each move results in tile 16 moving one space vertically or one space horizontally. Since tile 16 must end up in the same position it started we must have that the number of ''up'' moves equals the number of ''down'' moves and the number of ''left moves'' equals the number of ''right moves''. Hence the number of transpositions required for any solution is even but $(14\ 15)$ is clearly an odd permutation so no solution is possible (and Sam Loyd's money was safe). The above analysis, although powerful and elegant, only tells us half the story. If we rearrange the tiles so that the empty space ends up where it started, then only even permutations of the remaining blocks are possible. A similar argument shows that if the empty space is allowed to end up somewhere else, then if the space is an even (odd) distance from its starting point then only even (odd) permutations are possible. But are all such permutations possible? The answer is yes and it follows from the following results about the Alternating Group.

Lemma 2.1. *For $n \geq 3$, A_n is generated by its 3-cycles.*

Proof.

First observe that A_n contains all 3 cycles and so the group generated by all 3 cycles is a subgroup of A_n.

Let $g \in A_n$ then there are transpositions $t_1, t_2, \ldots, t_{2_k}$ such that $g = t_1 t_2 \ldots t_{2k}$. Write $g = (t_1 t_2)(t_3 t_4) \ldots (t_{2k-1} t_{2k})$. For each odd i in the set $\{1, \ldots, 2k\}$ there are three possibilities

for $t_i t_{i+1}$

1. $t_i = t_{i+1}$: in this case $t_i t_{i+1} = I$.
2. t_i and t_{i+1} have a point in common.In this case there are a, b, c such that $t_i = (a\ b)$ and $t_{i+1} = (b\ c)$. Hence, $t_i t_{i+1} = (a\ b\ c)$.
3. t_i and t_{i+1} have no point in common. In this case there are a, b, c, d such that $t_i = (a\ b)$ and $t_{i+1} = (c\ d)$. Observe that the equality

$$t_i t_{i+1} = (a\ b)(c\ d) = (a\ c\ d)(a\ b\ d)$$

holds in this case.

Therefore, whenever $t_i t_{i+1}$ is not trivial we may replace it with a 3-cycle or with a product of 3-cycles. We see that g can therefore be written as a product of 3-cycles. The result now follows.

□

Note the structure of that proof. We were required to show that A_n is generated by its 3-cycles. Let us assume that S is the set of all 3-cycles where, obviously, S will depend on n. In the first part of the proof we demonstrated that $S \subseteq A_n$ and in the second part that $A_n \subseteq S$. Hence we showed that the sets are equal and so the result follows.

Theorem 2.3. *For $n \geq 3$, A_n is generated by its 3-cycles of the form $(1\ 2\ i)$.*

Proof.

It suffices to show, by Lemma 2.1 that any 3-cycle can be written as a product of elements of the form $(1\ 2\ i)$ and their inverses.

Now

$$\begin{aligned}(1\ a\ 2)(1\ 2\ c)(1\ b\ 2)(1\ 2\ a) &= (1\ 2\ a)^{-1}(1\ 2\ c)(1\ b\ 2)(1\ 2\ a)\\ &= (1\ 2\ a)^{-1}(1\ b\ c)(1\ 2\ a)\\ &= (a\ b\ c).\end{aligned}$$

This concludes the proof.

□

Clearly the same result would hold if 1 and 2 were replaced by any other distinct symbols. We want to know which starting positions, with the empty space in the bottom right hand corner, can be rearranged back into the solved state:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Clearly these are precisely the states which can be reached by starting from the solved state. We know that these states (when expressed as permutations of the solved state) form a subgroup of A_{15}, we want to show that it is all of A_{15} (or, equivalently, all the elements of A_{16} which fix 16). We will do this by showing that every 3-cycle of the form $(11\ 12\ i)$ is possible and, since these cycles generate A_{15}, the result will follow. [*The rest of this section is not examinable.*]

We first construct the 3-cycle $(11\ 12\ 15)$ in a particular way. Start by moving the empty

space away from the edge of the board by exchanging it with 12 and then 11:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

$\rightsquigarrow$

1	2	3	4
5	6	7	8
9	10		11
13	14	15	12

Then rotate the tiles in the bottom right quadrant.

1	2	3	4
5	6	7	8
9	10		11
13	14	15	12

$\rightsquigarrow$

1	2	3	4
5	6	7	8
9	10		15
13	14	12	11

Finally, we undo the two moves we started with to get the space back in the corner.

1	2	3	4
5	6	7	8
9	10		15
13	14	12	11

$\rightsquigarrow$

1	2	3	4
5	6	7	8
9	10	15	11
13	14	12	

Representing this state as a permutation of the solved state gives $(11\ 12\ 15)$ as desired. We can construct any 3-cycle of the form $(11\ 12\ i)$ for any piece $i \notin \{11, 12, 15\}$ by first moving the space away from the corner (as we did above), then applying some sequence of moves to place i into the place originally occupied by 15 without moving 11 or 12, and ending with the space in the same position as before. If we then rotate the bottom right corner pieces, as before, and reverse the previous moves we will obtain $(11\ 12\ i)$. For example, to obtain

$(11\ 12\ 4)$:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

$\rightsquigarrow$

1	2	3	4
5	6	7	8
9	10		11
13	14	15	12

Then identify a tour which passes through the space and 15 without hitting 11 or 12 (indicated in bold). Cycle this tour round to obtain place 4 in the position occupied by 15.

1	**2**	**3**	**4**
5	6	**7**	**8**
9	10		11
13	**14**	**15**	12

$\rightsquigarrow$

13	**9**	**5**	**1**
14	6	**3**	**2**
15	10		11
7	**8**	**4**	12

Now cycle the bottom right quadrant so that the 4 moves to where the 11 is now:

13	9	5	1
14	6	3	2
15	10		11
7	8	4	12

$\rightsquigarrow$

13	9	5	1
14	6	3	2
15	10		4
7	8	12	11

Finally undo the bold cycle which carried 4 into the place occupied by 15 and then move the space back to the corner to obtain $(11\ 12\ 4)$.

13	**9**	**5**	**1**
14	6	**3**	**2**
15	10		4
7	**8**	**12**	11

$\rightsquigarrow$

1	**2**	**3**	**12**
5	6	**7**	**8**
9	10		4
13	**14**	**15**	11

$\rightsquigarrow$

1	2	3	12
5	6	7	8
9	10	4	11
13	14	15	

Because every 3-cycle $(11\ 12\ i)$ can be formed in this way and these 3-cycles generate A_{15} we can obtain every even permutation of the solved state. It follows that every even

permutation of the solved state can be solved! There is a subtlety here though - we are permuting positions not tiles. For example, if we want to apply $(11\ 12\ 4)$ again so as to form the permutation $(11\ 12\ 4)^2 = (11\ 4\ 12)$ then we need to repeat the actual moves we did before so that the tile in position 4 (which is now 12) moves into the space occupied by 15.

2.5 Problem Sheet 2

For Week 5; covers Chapter 2 material. At minimum you should attempt questions 2.2, 2.3, 2.9 and 2.10.

Question 2.1

Which of the following permutations is different from the other two:

$$(1\ 4\ 2\ 8)(3\ 7\ 5), \quad (1\ 8\ 2\ 4)(5\ 7\ 3), \quad (7\ 5\ 3)(2\ 8\ 1\ 4).$$

Show Solution 2.1 on P157

Question 2.2

Write down all of the permutations in S_5 with each of the following cycle structures:

i. $(* *)$;

ii. $(* * * *)$;

iii. $(* *)(* *)$.

Show Solution 2.2 on P157

Question 2.3

Write down all of the cycle structures in S_6 together with the number of each. [Do not attempt to list the permutations themselves!]

Show Solution 2.3 on P158

Question 2.4

Write down the elements of A_4.

Show Solution 2.4 on P160

Question 2.5

Let $a = (2\ 5\ 3)(4\ 6)$ and $b = (1\ 2\ 6)$. Calculate:

i. ab;

ii. ba;

iii. $(ab)^{-1}$;

iv. a^{-1};

v. b^{-1};

vi. $b^{-1}a^{-1}$.

Show Solution 2.5 on P160

Question 2.6

Write down the orders of the following permutations:

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

ii. $(1\ 2\ 3\ 4\ 5)(7\ 8)$;

iii. $(1\ 2\ 3\ 4\ 5\ 6)(7\ 8)$;

iv. $(1\ 2)(3\ 4)(5\ 6)(7\ 8)$;

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

Show Solution 2.6 on P161

Question 2.7

In each of the following cases find the order of ab:

i. $a = (1\ 2)$ and $b = (1\ 2\ 3)$;

ii. $a = (4\ 5)$ and $b = (1\ 2\ 3)$;

iii. $a = (1\ 4)$ and $b = (1\ 2\ 3)$;

iv. $a = (1\ 2)(3\ 4)$ and $b = (1\ 2\ 3)$;

v. $a = (3\ 4)(5\ 6)$ and $b = (1\ 2\ 3)(4\ 5\ 6)$;

vi. $a = (3\ 4)(6\ 7)$ and $b = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)$.

Show Solution 2.7 on P161

Question 2.8

Given $N \in \mathbb{N}$, show that there is a number $n \in \mathbb{N}$ and elements $a, b \in S_n$ such that

- $a^2 = I$,
- $b^3 = I$, and,
- the order of ab is greater than N.

Show Solution 2.8 on P162

Question 2.9

Find the largest order for an element of S_{10}.

Show Solution 2.9 on P162

Question 2.10

In each of the following cases find the conjugate of a with b, i.e. compute bab^{-1}:

a. $a = (1\ 2)$ and $b = (2\ 3\ 4\ 5)$;

b. $a = (1\ 3)(2\ 5\ 6)$ and $b = (2\ 3)(4\ 5)$;

c. $a = (1\ 4)(2\ 5)$ and $b = (1\ 3\ 2\ 5)$;

d. $a = (1\ 2)(3\ 4)$ and $b = (1\ 2\ 3)$;

e. $a = (1\ 3\ 2\ 5)$ and $b = (1\ 4)(2\ 5)$;

f. $a = (1\ 5\ 6)$ and $b = (1\ 5\ 6)$.

Show Solution 2.10 on P163

Question 2.11

In each of the following cases find, where possible, permutations $b \in S_6$ and $d \in A_6$ such that $bab^{-1} = c = dad^{-1}$:

a. $a = (1\ 3\ 2)(4\ 5)$, and $c = (1\ 5)(2\ 3\ 4)$;

b. $a = (1\ 4)(2\ 3)$, and $c = (1\ 6)(2\ 4)(3\ 5)$;

c. $a = (1\ 2)(3\ 4)$, and $c = (1\ 3)(2\ 4)$;

d. $a = (1\ 4)$, and $c = I$;

e. $a = (1\ 3)$, and $c = (1\ 3)$.

Show Solution 2.11 on P163

Question 2.12

Let $n \geq 5$. Let $a, c \in A_n$ be 3-cycles. Show that there is an element $b \in A_n$ such that $bab^{-1} = c$.

Does the statement above hold when $n \in \{3, 4\}$?

[Hint: For the first part of the question, find a conjugate in S_n; if it is not an element of A_n how can you make it into an elmement of A_n using the fact that disjoint cycles commute?]

Show Solution 2.12 on P164

Chapter 3

Group Actions

3.1 An Activity in Group Actions

Consider two people who can have one of two states, either standing or seated. We label the standing state as U (for 'up') and the seated state as D (for 'down'). The instruction to 'invert' means to change from one of these states to the other. The instruction 'swap' means that the two people change places and we denote the two places as L (left) and R (right). We now define the operation a as 'swap position then invert L'.

Example 3.1.

$$DD \overset{a}{\to} UD \overset{a}{\to} UU \overset{a}{\to} DU \overset{a}{\to} DD$$

Note the following:

$$DD \overset{a^2}{\longrightarrow} UU$$

$$DD \overset{a^3}{\longrightarrow} DU$$

$$DD \overset{a^4=e}{\longrightarrow} DD$$

We can now form an operation table as follows:

$*$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

So, as is easily discernible from the table, the transformations $\{e, a, a^2, a^3\}$ form a group and as a has order 4 this group is isomorphic to $\mathbb{Z}_4$.

Using the same terminology as the previous example, consider now three people seated and let L be the instruction that the two people on the left invert and R be that the two people on the right invert (so, in each case, the middle person inverts). We have the following:

$$DDD \quad \overset{L}{\rightarrow} \quad UUD \quad \overset{L}{\rightarrow} \quad DDD$$

So, $L^2 = e$ and, similarly, $R^2 = e$. We further have

$$DDD \quad \overset{L}{\rightarrow} \quad UUD \quad \overset{R}{\rightarrow} \quad UDU$$

and

$$DDD \quad \overset{R}{\rightarrow} \quad DUU \quad \overset{L}{\rightarrow} \quad UDU.$$

Hence, $LR = RL$. Since we have that $LR = RL$, the only distinct elements are e, L, R, and LR. We can then construct the operation table:

$*$	e	L	R	LR
e	e	L	R	LR
L	L	e	LR	R
R	R	LR	e	L
LR	LR	R	L	e

For example, $R * LR = R(LR) = R(RL) = R^2L = L$ as $R^2 = e$. In this case, we can see from the table that all of the non-identity elements have order 2 (the identity element appears in every position on the lead diagonal) and so this group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. As a presentation, this group is

$$\langle L, R \mid L^2 = R^2 = e, LR = RL \rangle.$$

Example 3.2. Consider three people seated. Let a : invert L, swap the other two; b : invert R, swap the other two. Find the distinct elements of the group and construct the operation table. What is this group?

Observe that a and b both have order two. Moreover $(ab)^3 = 1$:

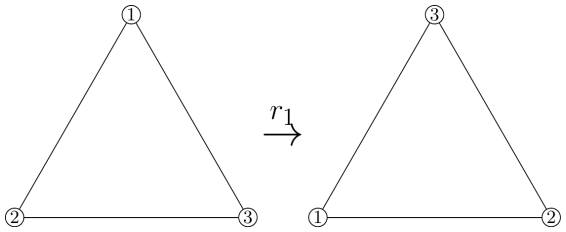
$$D_L D D_R \xrightarrow{ab} D_R U_L U \xrightarrow{ab} U U_R D_L \xrightarrow{ab} D_L D D_R.$$

Thus the group generated by a and b has the same presentation as the group in Example 1.9 and so is isomorphic to D_3.

3.2 Groups Acting on Sets

We have already seen several examples of groups acting on sets but have not introduced the concept formally. Each element of D_3 permutes the vertices of the triangle and we say that the group 'acts' on these vertices.

Consider rotation anticlockwise by $\pi/3$



Then r_1 'acts' on vertex 1 by mapping it to position 2 and so on. We can represent this

action on the set $\{1, 2, 3\}$ of vertices as:

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

A group G acts on a set X when each element of G maps each element of X onto another element of X in a way consistent with the group axioms. Formally we have:

Definition 3.1 (Group Action)**.** A group G *acts on* a (non-empty) set X (or there is an *action* $*$ of G on X) if, for each $g \in G$ and $x \in X$ there is an element $g * x \in X$ and

i. $e * x = x,\ \forall\, x \in X$,

ii. $g * (h * x) = (gh) * x,\ \forall\, g, h \in G$ and $\forall\, x \in X$.

The first property requires that the effect of the identity element in G is the identity permutation on X and the second says that the effect of applying h followed by g to an element of X is the same as applying the single element gh. Groups acting on sets are really just thinly disguised permutation groups in that whenever a group G acts on a set X we can associate with each $g \in G$ the permutation f_g of X defined by $f_g(x) = g * x,\ \forall\, x \in X$. These permutations form a subgroup of $S_{|X|}$, but this group need not be isomorphic to G, and we shall return to this later. First we consider some examples.

Example 3.3.

Consider the symmetric group S_n. This acts on the set $\{1, 2, \ldots, n\}$ by the rule $f * x = f(x)$. For example, for $f = (1\ 2\ 4)$, then

$$f * 1 = 2$$
$$f * 3 = 3.$$

Notice that this extends to any subgroup of S_n, that is any subgroup $H \leq S_n$ acts on the set $\{1, 2, \ldots, n\}$ in the manner just described. By Cayley's Theorem, this means that every

finite group acts on a finite set (recall that in Cayley's theorem this set is just the group elements and so every group acts on itself).

Example 3.4.

Consider the group D_4. This group acts on the set $N = \{1, 2, ..., 9\}$ of nine small squares in a 3x3 array as follows:

1	2	3
4	5	6
7	8	9

Using our notation for the symmetries of a square we have, for example,

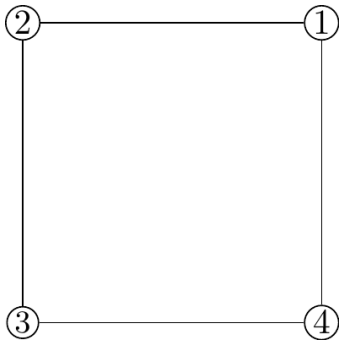
$$r_1 * 7 = 9$$

$$r_2 * 5 = 5$$

$$s_1 * 3 = 1$$

Example 3.5.

Let $V = \{1, 2, 3, 4\}$ be the set of numbered vertices of a square as shown with symmetries defined as usual.



If we let D_4 acts on the vertices of the square, then we are led to the permutation group:

$$\underset{e}{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}}, \underset{r_1}{\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}}, \underset{r_2}{\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}}, \underset{r_3}{\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}},$$
$$\underset{s_1}{\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}}, \underset{s_2}{\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}}, \underset{s_3}{\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}}, \underset{s_4}{\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}}.$$

This permutation group is isomorphic to D_4.

The group D_4 can also act on the diagonals of the square (so ignoring vertices and thinking only of how the diagonals are affected). Writing d_1 for the main diagonal and d_2 for the off diagonal, we see that e, r_2, s_2, s_4 all fix the diagonals while all other elements of D_4 swap the diagonals. We can represent this action by the permutation group:

$$\left\{ \begin{pmatrix} d_1 & d_2 \\ d_1 & d_2 \end{pmatrix}, \begin{pmatrix} d_1 & d_2 \\ d_2 & d_1 \end{pmatrix} \right\}.$$

Example 3.6.

Consider the group $\mathrm{GL}(n, \mathbb{R})$, the group of invertible $n \times n$ matrices with real entries under matrix multiplication. This acts on the $\mathbb{R}^n$ by $A * \mathbf{x} = A\mathbf{x}$ since:

$$I * \mathbf{x} = I\mathbf{x} = \mathbf{x}$$

and

$$B * (A * \mathbf{x}) = B * (A\mathbf{x}) = BA\mathbf{x} = (BA) * \mathbf{x}.$$

Any group of functions G on a set X defines a group action $*$ according to the 'obvious' rule $f * x = f(x), \forall\, x \in X$. By definition of the identity function, e, we have $e * x = x, \forall\, x \in X$ and, since $g * (f * x)$ means apply g to $f(x)$, it follows immediately that $\forall\, g, f \in G$, $g * (f * x) = (gf) * x$ as they are both just $g(f(x))$. However, many deep

theorems of Group Theory have been proved by finding a 'good action'. A good example is the following alternative proof to one of the main results on permutations in the Abstract Algebra module. We give an example first, followed by the proof.

Theorem 3.1. *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.*

Example 3.7. Let S_4 act on the set of polynomials in $\{x_1, x_2, x_3, x_4\}$ by the rule $f : x_i \to x_{f(i)}$. For example,

$$(1\ 2)(3\ 4) * (x_1^3 x_2 - x_3) = x_2^3 x_1 - x_4.$$

Now consider the polynomial

$$P = \prod_{1 \le i < j \le 4} (x_j - x_i) = (x_2 - x_1)(x_3 - x_2)(x_3 - x_1)(x_4 - x_3)(x_4 - x_2)(x_4 - x_1).$$

Then

$$(1\ 2)P = (x_1 - x_2)(x_3 - x_1)(x_3 - x_2)(x_4 - x_3)(x_4 - x_1)(x_4 - x_2) = -P$$

since the only *overall* change is $(x_2 - x_1) \mapsto (x_1 - x_2) = -(x_2 - x_1)$. Also

$$(1\ 3)P = (x_2 - x_3)(x_1 - x_2)(x_1 - x_3)(x_4 - x_1)(x_4 - x_2)(x_4 - x_3) = -P$$

since the first three terms change parity. In fact we have that, for all $(i\ j) \in S_4$, $(i\ j) * P = -P$.

We can now prove the theorem.

Proof. Let S_n act on the set of polynomials $\{x_1, x_2, \ldots, x_n\}$ by the rule $f : x_i \mapsto x_{f(i)}$. Consider the so-called alternating polynomial

$$P = \prod_{1 \le i < j \le n} (x_j - x_i).$$

For all transpositions $(i\ j) \in S_n$, then $(i\ j) * P = -P$. If f can be written as the product of an even number of transpositions, then $f * P = P$. If f can be written as the product of an odd number of transpositions, then $f * P = -P$. Hence, f cannot be expressed as the product of both an even number and an odd number of transpositions. □

3.3 Orbits and Stabilizers

Let G be a group acting on a set X. Given $x \in X$ we define the orbit of x, $\mathrm{orb}\,(x)$ to be the set of elements of X that we can obtain from x by applying some element of G. Formally we have:

Definition 3.2 (Orbit)**.** Let G be a group acting on a set X. Then the *orbit* of x is denoted and defined by

$$\mathrm{orb}\,(x) = \{y \in X \,|\, y = g * x \text{ for some } g \in G\}.$$

Example 3.8.

We apply Definition 3.2 to some groups we have encountered already.

- The orbits of the cyclic subgroup of S_n generated by an element $f \in S_n$ are the cycles of f written as sets. For example the orbit of the group $\langle (1\ 2)(3\ 4\ 5\ 7) \rangle \leq S_7$ are $\{1, 2\}, \{3, 4, 5, 7\}, \{6\}$.
- Consider Example 3.5: D_4 acting on the vertices has only one orbit: $\{1, 2, 3, 4\}$. However in Example 3.4, the orbits of D_4 are $\{1, 3, 7, 9\}, \{2, 4, 6, 8\}, \{5\}$.

It would appear that the orbits partition X and the standard way to prove the existence of a partition is to show that there is an underlying equivalence relation.

Lemma 3.1. *Let G be a group acting on a set X. Define the relation $\sim$ on X by $x \sim y$ if and only if $g * x = y$ for some $g \in G$ (i.e. x is related to y if and only if y is in the orbit of x). Then $\sim$ is an equivalence relation on X.*

Proof.

We verify that the relation is reflexive, symmetric and transitive.

- **Reflexive**: for all $x \in X$, $e * x = x$, therefore $x \in \operatorname{orb}(x)$ and $x \sim x$.
- **Symmetric**: $x \sim y \implies g * x = y$ for some $g \in G$. However this now means that

$$x = e * x = (g^{-1}g) * x = g^{-1} * (g * x) = g^{-1} * y$$

  and so $y \sim x$.
- **Transitive**: $x \sim y$ and $y \sim z$. There are g_1, g_2 such that $g_1 * x = y$ and $g_2 * y = z$. This now means that

$$(g_2 g_1) * x = g_2 * (g_1 * x) = g_2 * y = z$$

  and so $x \sim z$.

□

The stabilizer of x, $\operatorname{stab}(x)$, consists of those elements of G that leave x unchanged. Formally we have:

Definition 3.3 (Stabilizer)**.** Let G be a group acting on a set X. Then the *stabilizer* of $x \in X$ is denoted and defined by

$$\operatorname{stab}(x) = \{g \in G \,|\, g * x = x\}.$$

Example 3.9.

Consider Example 3.4 and Example 3.5:

- In Example 3.4: $\operatorname{stab}(2) = \{e, s_1\}$, $\operatorname{stab}(5) = D_4$

- In Example 3.5:

$$\begin{aligned}\operatorname{stab}(1) &= \{e, s_2\} = \operatorname{stab}(3)\\ \operatorname{stab}(2) &= \{e, s_4\} = \operatorname{stab}(4)\\ \operatorname{stab}(d_1) &= \{e, r_2, s_2, s_4\} = \operatorname{stab}(d_2)\end{aligned}$$

> **Note**
>
> For a group G acting on a set X, the orbits are subsets of X whereas the stabilizers are subsets of G. In fact a stabilizer is rather more than just a subset of G!

Theorem 3.2. *Let G be a group acting on a set X. Then $\operatorname{stab}(x)$ is a subgroup of G.*

Proof.

Note that $e \in \operatorname{stab}(x)$ since $e * x = x$.

Let $g, h \in \operatorname{stab}(x)$, then

$$(gh) * x = g * (h * x) = g * x = x$$

and so $gh \in \operatorname{stab}(x)$. Furthermore,

$$x = e * x = (g^{-1}g) * x = g^{-1} * (g * x) = g^{-1} * x$$

and so $g^{-1} \in \operatorname{stab}(x)$.

This completes the subgroup check.

□

Example 3.10.

Consider Example 3.4 and Example 3.5 again:

- Revisiting Example 3.4:

Orbit	stabilizer
$\operatorname{orb}(1) = \{1, 3, 7, 9\}$	$\operatorname{stab}(1) = \{e, s_4\}$
$\operatorname{orb}(2) = \{2, 4, 6, 8\}$	$\operatorname{stab}(2) = \{e, s_1\}$
$\operatorname{orb}(5) = \{5\}$	$\operatorname{stab}(5) = D_4$

- Revisiting Example 3.5:

Orbit	stabilizer
$\operatorname{orb}(1) = \{1, 2, 3, 4\}$	$\operatorname{stab}(1) = \{e, s_2\}$
$\operatorname{orb}(d_1) = \{d_1, d_2\}$	$\operatorname{stab}(d_1) = \{e, r_2, s_2, s_4\}$

Notice that in each of the cases above:

$$|\operatorname{orb}(x)| \times |\operatorname{stab}(x)| = |D_4|.$$

This fact holds in general.

Theorem 3.3 (Orbit Stabilizer Theorem)**.** *Let G be a finite group acting on a finite set X, and $x \in X$. Then:*

$$|\operatorname{orb}(x)| \times |\operatorname{stab}(x)| = |G|.$$

Proof.

Recalling, by Lagrange's theorem, that the index of $\operatorname{stab}(x)$ in G is precisely $|G|/|\operatorname{stab}(x)|$, it suffices to show that orbit x is in one-to-one correspondence with the left cosets of $\operatorname{stab}(x)$ in G. We do this by showing that $g_1 * x = g_2 * y$, for $g_1, g_2 \in G$ if and only if g_1 and g_2 belong to the same left coset.

Suppose first that g_1 and g_2 belong to the same left coset of $\operatorname{stab}(x)$. This means that

there is an $h \in \mathrm{stab}\,(x)$ such that $g_1 h = g_2$. Consequently:

$$g_2 * x = (g_1 h) * x = g_1 * (h * x) = g_1 * x$$

as required.

Suppose on the other hand that $g_1 * x = g_2 * x$. We then have:

$$x = e * x = (g_1^{-1} g_1) * x = g_1^{-1} * (g_1 * x) = g_1^{-1} * (g_2 * x) = (g_1^{-1} g_2) * x)$$

and we conclude that $g_1^{-1} g_2 \in \mathrm{stab}\,(x)$. Therefore, g_1 and g_2 belong to the same left coset of $\mathrm{stab}\,(x)$.

□

Later we will use this result to prove an important structural property of groups, namely Cauchy's Theorem which states that if p is a prime divisor of the order of a group G, then G contains an element (and hence a subgroup) of order p. This is the first step towards a 'converse' to Lagrange's Theorem. Before we do this, though, we prove a famous result that has many important applications.

3.4 Counting Orbits

Let G be a group acting on a set X. For each $g \in G$, the *fixed set* of g, $\mathrm{fix}\,(g)$, is the subset of X consisting of those elements of X fixed by g. Formally we have:

Definition 3.4 (Fixed Set)**.** Let G be a group acting on a set X. Then, for each $g \in G$, the *fixed set* of g is denoted and defined by

$$\mathrm{fix}\,(g) = \{x \in X \mid g * x = x\}.$$

Example 3.11.

Consider Example 3.4 with D_4 acting on the four vertices of a square. We have:

$$\begin{aligned}
\operatorname{fix}(e) &= \{1,2,3,4\} \\
\operatorname{fix}(r_1) = \operatorname{fix}(r_2) &= \operatorname{fix}(r_3) = \emptyset \\
\operatorname{fix}(s_1) &= \operatorname{fix}(s_3) = \emptyset \\
\operatorname{fix}(s_2) &= \{1,3\} \\
\operatorname{fix}(s_4) &= \{2,4\}.
\end{aligned}$$

Notice that

$$\sum_{g \in D_4} |\operatorname{fix}(g)| = 8$$

and

$$\sum_{x \in V} |\operatorname{stab}(x)| = 8$$

For this example we have $\sum_{g \in G} |\operatorname{fix}(g)| = \sum_{x \in V} |\operatorname{stab}(x)|$.

We prove that this holds in general. The key idea is to consider the set of all pairs (g, x) such that $g * x = x$. We can order this set of pairs in two ways:

$$\{(g,x) \mid x \in \operatorname{fix}(g)\} = \{(g,x) : g \in \operatorname{stab}(x)\}.$$

For instance, returning to Example 3.4 again, we have, under the first ordering,

$$\{(e,1),(e,2),(e,3),(e,4),(s_2,1),(s_2,3),(s_4,2),(s_4,4)\}$$

and under the second,

$$\{(e,1),(s_2,1),(e,2),(s_4,2),(e,3)(s_2,3),(e,4),(s_4,4)\}.$$

As expected the two sets are equal and consequently:

$$\sum_{g \in D_4} |\operatorname{fix}(g)| = \sum_{x \in V} |\operatorname{stab}(x)|$$

since both sums count the number of pairs (g, x) such that $g * x = x$.

Notice that $\operatorname{fix}(g)$ is a subset of X (as is $\operatorname{orb}(x)$ but not $\operatorname{stab}(x)$ which is a subgroup of G). However, $\operatorname{fix}(g)$ and $\operatorname{stab}(x)$ are related.

Lemma 3.2. *Let G be a finite group acting on a finite set X, then*

$$\sum_{g \in G} |\operatorname{fix}(g)| = \sum_{x \in X} |\operatorname{stab}(x)|.$$

Proof.

Let N be the size of the set

$$\{(g, x) : g \in G, x \in X, g * x = x\}.$$

Then,

$$N = |\{(g, x) : g \in G, x \in X, g * x = x\}| = \sum_{g \in G} |\{(g, x) : x \in \operatorname{fix}(g)\}| = \sum_{g \in G} |\operatorname{fix}(g)|$$

and

$$N = |\{(g, x) : g \in G, x \in X, g * x = x\}| = \sum_{x \in X} |\{(g, x) : g \in \operatorname{stab}(x)\}| = \sum_{x \in X} |\operatorname{stab}(x)|.$$

The result now follows.

□

We are now in a position to prove Burnside's Lemma, which should really be called a Theorem (but then it wasn't proved by Burnside either).

Theorem 3.4 (Burnside's Lemma). *Let G be a finite group acting on a finite set X. Then*

$$\textit{the number of orbits in } X \textit{ under } G \ = \frac{1}{|G|}\sum_{g\in G} |\operatorname{fix}(g)|.$$

Proof.

Let $O_1, O_2, \ldots, O_r$ be the r orbits of X under G and consider the

$$\sum_{x\in X} |\operatorname{stab}(x)|.$$

Recalling that the orbits of X form a partition of X, we can organise the above sum as:

$$\sum_{x\in X} |\operatorname{stab}(x)| = \sum_{x\in O_1} |\operatorname{stab}(x)| + \sum_{x\in O_2} |\operatorname{stab}(x)| + \ldots + \sum_{x\in O_r} |\operatorname{stab}(x)|.$$

We next observe that points in the same orbit have stabilizers of equal sizes. This is a consequence of Theorem 3.3 since for x, y belonging to the same orbit O:

$$|\operatorname{stab}(x)| = \frac{|G|}{|O|} = |\operatorname{stab}(y)|.$$

Therefore fixing, for each $1 \leq i \leq r$ a point $x_i \in O_r$,

$$\begin{aligned}\sum_{x\in X} |\operatorname{stab}(x)| &= \sum_{x\in O_1} |\operatorname{stab}(x)| + \sum_{x\in O_2} |\operatorname{stab}(x)| + \ldots + \sum_{x\in O_r} |\operatorname{stab}(x)| \\ &= (|O_1| \times |\operatorname{stab}(x_1)|) + (|O_2| \times |\operatorname{stab}(x_2)|) + \ldots + (|O_r| \times |\operatorname{stab}(x_r)|) \\ &= |G|r\end{aligned}$$

Dividing by $|G|$ yields,

$$\frac{1}{|G|}\sum_{x\in X} |\operatorname{stab}(x)| = r.$$

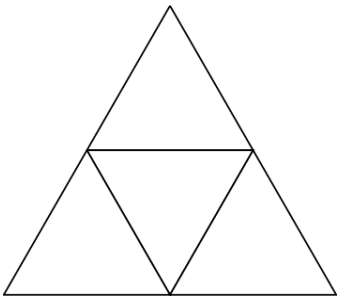
The result is now a consequence of Lemma 3.2.

□

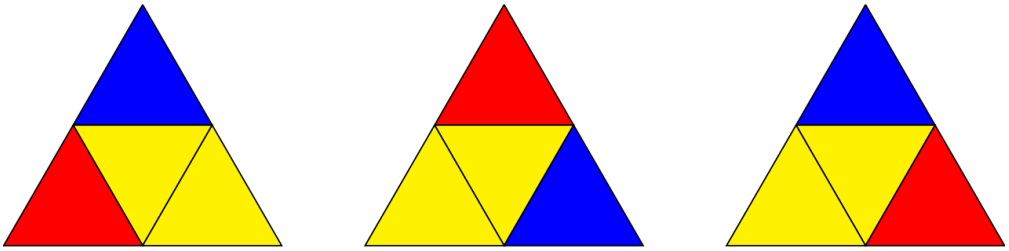
3.5 Colouring Problems

Burnside's lemma can be used to count the number of 'essentially different' configurations in a set. As in Graph Theory, these configurations are usually described in terms of colourings but the applications are much wider than this suggests.

Example 3.12. How many essentially different ways are there of colouring the smaller equilateral triangles red, blue or yellow?



The answer depends on what is meant by 'essentially' different.



1 2 3

We may wish to consider 1 and 2 the same since we may obtain 2 from 1 by applying the symmetry r_2 in D_3 (rotating anticlockwise twice by $2\pi/3$).

If the triangle is equilateral, then we may consider all the labellings to be equivalent, since we may obtain 3 from 1 by reflecting in the vertical axis (that is by applying the element s_2 of D_3).

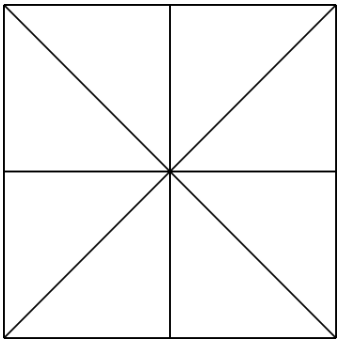
To be precise about what we mean by 'essentially different' we specify a group of symmetries of the figure and say that two colourings are equivalent (i.e. essentially the same) if and

only if one can be transformed into the other by one of these symmetries. In other words, if we consider the action of a group of symmetries on the set of all colourings of the figure, then two colourings are equivalent if and only if they lie in the same orbit. It follows that the number of distinct colourings is just the total number of orbits, which we can find using Burnside's Lemma.

Example 3.13. In how many different ways can the square glass tile shown below, which can be turned over, be coloured

a. using n colours,

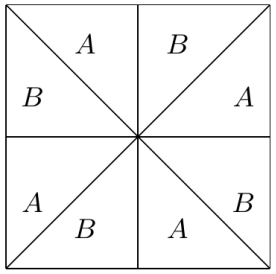
b. so that there are six red and two blue regions?



The group acting is D_4:

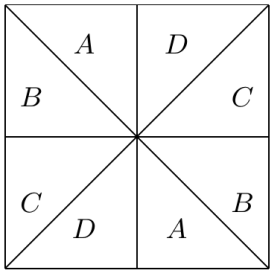
a. The underlying set X is the set of all n^8 colourings of the 8 regions of the tile. Hence $|\operatorname{fix}(e)| = |X| = n^8$.

Colourings
fixed by r_1



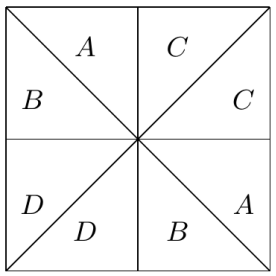
$|\operatorname{fix}(r_1)| = n^2 = |\operatorname{fix}(r_3)|$

Colourings
fixed by r_2



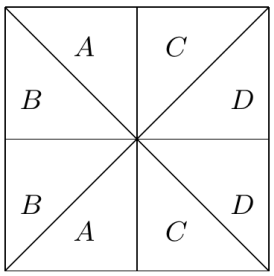
$|\operatorname{fix}(r_2)| = n^4$

Colourings
fixed by s_1



$|\operatorname{fix}(s_2)| = n^4 = |\operatorname{fix}(s_4)|$

Colourings
fixed by s_3



$|\operatorname{fix}(s_3)| = n^4 = |\operatorname{fix}(s_1)|$

By Burnside's Lemma, the number of orbits of X under D_4, that is the total number of distinct colourings, is

$$\frac{1}{8}(n^8 + 5n^4 + 2n^2).$$

b. There are $\binom{8}{2}$ ways of choosing the blue colored regions; the rest are colored red. Therefore the total number of colorings is

$$\binom{8}{2} = 28.$$

This means that $\operatorname{fix}(e) = 28$. Looking at the working for part a., a colouring of the tile with blue and red that is fixed by r_1 or r_3 is either monochromatic or has at least

4 blue regions. Therefore $\text{fix}\,(r_1) = \text{fix}\,(r_3) = \emptyset$ since there are no colourings of the tile with 6 red and 2 blue regions fixed under r_1 or r_3.

Looking at the working for r_2 we need at that exactly one of A, B, C, D is blue (the rest are red). Thus there are 4 such colourings. A similar argument works for the reflections – each fixes 4 colourings.

Hence the number of valid colourings is:

$$\frac{1}{8}(28 + (5 \times 4)) = 6.$$

3.6 Cauchy's Theorem and p-Groups

Up to now this chapter has been concerned with applications of (permutation) groups. The main aim of this course, however, is to examine the structure of finite groups. Lagrange's Theorem is a structure theorem in that for any finite group G it rules out the existence of subgroups of G for any order not dividing $|G|$. We know that the converse of Lagrange's Theorem is true for abelian groups but false in general. This is not the end of the story, as we shall eventually show that if $|G| = p^r m$ for some prime p, then G has a subgroup of order p^r (and in fact of order $p^s \ \forall\, s,\ 0 \leq s \leq r$). Our first step towards this goal is to prove that if p is a prime divisor of the order of a group G, then G contains an element of order p. We will illustrate the proof of this result by way of an example.

Example 3.14. Consider $D_3 = \{e, r_1, r_2, s_1, s_2, s_3\}$, we will use group actions to show that at least one of these elements has order 3. Form the set X consisting of all triples (x, y, z)

where x, y and z are (not necessarily distinct) elements of G such that $xyz = e$. Thus:

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

We see that $|X| = 36$. We should have expected this because for any choice of elements x and y, $(x,y,z) \in X$ if and only if $z = (xy)^{-1}$; there are 6 choices for x and 6 for y giving $6 \times 6 = 36$ triples in total. We now consider the action of the cyclic group $\langle (1\ 2\ 3) \rangle$ on X defined by $(1\ 2\ 3) * (x,y,z) = (z,x,y)$. First we need to show that this is a group action on X, so we need to show that if $(x,y,z) \in X$, then $(z,x,y) \in X$ and $(y,z,x) \in X$. But $xyz = e \Leftrightarrow z = (xy)^{-1}$, so $zxy = (xy)^{-1}xy = e$ and $yzx = y(xy)^{-1}x = yy^{-1}x^{-1}x = e$

as required. What are the orbits of this action on X?

$$\{(e,e,e)\}$$
$$\{(e,r_1,r_2),(r_2,e,r_1),(r_1,r_2,e)\}$$
$$\{(e,r_2,r_1),(r_1,e,r_2),(r_2,r_1,e)\}$$
$$\{(e,s_1,s_1),(s_1,e,s_1),(s_1,s_1,e)\}$$
$$\{(e,s_2,s_2),(s_2,e,s_2),(s_2,s_2,e)\}$$
$$\{(e,s_3,s_3),(s_3,e,s_3),(s_3,s_3,e)\}$$
$$\{(r_1,r_1,r_1)\}$$
$$\{(r_1,s_1,s_3),(s_3,r_1,s_1),(s_1,s_3,r_1)\}$$
$$\{(r_1,s_2,s_1),(s_1,r_1,s_2),(s_2,s_1,r_1)\}$$
$$\{(r_1,s_3,s_2),(s_2,r_1,s_3),(s_3,s_2,r_1)\}$$
$$\{(r_2,r_2,r_2)\}$$
$$\{(r_2,s_1,s_2),(s_2,r_2,s_1),(s_1,s_2,r_2)\}$$
$$\{(r_2,s_2,s_3),(s_3,r_2,s_2),(s_2,s_3,r_2)\}$$
$$\{(r_2,s_3,s_1),(s_1,r_2,s_3),(s_3,s_1,r_2)\}$$

We see that the orbits are all either of size 1 or of size 3, moreover the orbits of size 1 are of the form $\{(g,g,g)\}$ where g is either the identity or an element of order 3. Could we have anticipated this? Under the action described any orbit of size 1 is necessarily of the form $\{(g,g,g)\}$ and hence $g^3 = e$; clearly $\{(e,e,e)\}$ will give us one such orbit and any further orbits of size 1 will correspond to elements of order 3. So D_3 contains an element of order 3 if and only if $\{(e,e,e)\}$ is not the only orbit of size 1 in X under this action. Let there be s orbits of size 1 and t orbits of size 3, so $|X| = s + 3t$, but we know that $|X| = 36$, so $s = 36 - 3t = 3(12 - t)$. It follows that s is at least 1 and also a multiple of 3, so there are at least 3 orbits of size 1 with at least 2 corresponding to elements of order 3.

Theorem 3.5 (Cauchy's Theorem)**.** *Let G be a finite group of order n and let p be a prime*

divisor of n. Then G has an element of order p and, consequently, a subgroup of order p.

Proof. The proof that follows is non-examinable.

Let $n = mp$ and $X = \{(g_1, g_2, ..., g_p) \in G \times G \times ... \times G \mid g_1 g_2 ... g_p = e\}$.

Note that $|X| = n^{p-1}$ since, for any choice of $g_1, g_2, ..., g_{p-1}$ in G (and there are n choices for each of the g_i in the list), we set $g_p = (g_1 g_2 ... g_{p-1})^{-1}$. But $|X| = n^{p-1} = (pm)^{p-1}$ so p divides $|X|$. Consider the group action of $\langle(1\ 2\ ...\ p)\rangle$ on X defined by

$$(1\ 2\ ...\ p) * (g_1, g_2, ..., g_p) = (g_2, ..., g_p, g_1).$$

For this to be an action on X we need to show that

$$(1\ 2\ ...\ p)^r * (g_1, g_2, ..., g_p) = (g_{r+1}, ..., g_p, g_1, ..., g_r) \in X.$$

But $g_{r+1} ... g_{p-1} g_p g_1 ... g_r = g_{r+1} ... g_{p-1} (g_{p-1}^{-1} ... g_{r+1}^{-1} g_r^{-1} ... g_2^{-1} g_1^{-1}) g_1 ... g_r = e \in X$, as required.

Next consider the orbits of X under this action. We know that the size of each orbit divides the order of $\langle(1\ 2\ ...\ p)\rangle$, which is p. Therefore, each orbit has size 1 or p. But an orbit has size 1 if and only if it is of the form $\{(g, g, ..., g)\}$ and hence $g^p = e$, so either $g = e$ or g is an element of order p.

Since $|X|$ is a multiple of p and $|X|$ is the sum of the sizes of the orbits, we have that the number of orbits of size 1 is also a multiple of p (possible zero), but $\{e, e, ..., e\}$ is one such orbit, so there must be at least $p - 1$ further orbits of size 1, and each of these is of the form $\{(g, g, ..., g)\}$ where $g \neq e$ is an element of order p. □

We now introduce an important class of groups.

Definition 3.5 (p-groups and p-subgroups)**.** A group is called a *p-group* if and only if every element in G has order a power of the prime p. A subgroup of a group G is a *p-subgroup* of G if the subgroup is itself a p-group.

It is not immediately obvious that finite p-groups are exactly the groups of order p^n.

Theorem 3.6. *Let G be a finite group. Then G is a p-group if and only if $|G|$ is a power of p.*

Proof.

If $|G|$ is a power of p, then by Lagrange's Theorem, the order of every element of $|G|$ is also a power of p (since it has to divide the order of $|G|$).

Suppose G is a p-group. If q is a prime dividing $|G|$, then by Cauchy's Theorem (Theorem 3.5), there is an element of G of order q. This means that the only prime dividing G must be q and so the order of G must be a power of p.

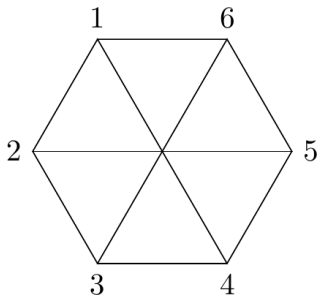
□

3.7 Problem Sheet 3

For Week 7; covers Chapter 3. At minimum you should attempt questions 3.1, 3.4 and 3.5.

Question 3.1

Consider the group D_6 (the group of symmetries of a regular hexagon) acting on the set, X, of vertices of the regular hexagon shown below and numbered sequentially 1 to 6 in an anticlockwise direction with the upper left vertex being number 1.



Using our standard notation for the elements of D_6:

a. find the orbits of X;

b. find the stabiliser of each element of X;

c. show how your results in parts a. and b. above demonstrate the Orbit-Stabiliser Theorem.

Show Solution 3.1 on P165

Question 3.2

In how many ways can the edges of a regular octagon be coloured with four different colours if two colourings are indistinguishable when one can be obtained from the other by

i. a rotation of the octagon.

ii. a rotation or reflection of the octagon.

Show Solution 3.2 on P166

Question 3.3

Use Burnside's Lemma to count the distinguishable colourings of the edges of

i. a square,

ii. a regular pentagon,

using at most three colours under the relevant full dihedral group of symmetries in each case.

Show Solution 3.3 on P169

Question 3.4

Use Burnside's Lemma to count the distinguishable colourings of the edges of a square with four distinct colours when two colourings are indistinguishable if one can be obtained from the other by

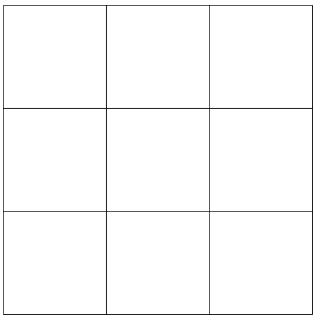
i. a rotation of the square,

ii. a rotation or reflection of the square.

Show Solution 3.4 on P171

Question 3.5

Use Burnside's Lemma to enumerate the distinguishable colourings of the regions of the following square grid using at most two colours:



a. under the group of rotations of the square;

b. under the full dihedral group D_4.

Give an example of two colourings that are distinguishable in part a. but not in part b.

Show Solution 3.5 on P173

Question 3.6

A teacher has a bank of n test questions and wants to assign to each of 3 students, A, B, C, one of the n questions in this bank. The teacher is not concerned if the same question is assigned to more than one student, and is not concerned about the order in which the questions are assigned to the students. Using Burnside's Lemma determine the number of essentially different ways of assigning a question from the bank to each student.

Show Solution 3.7 on P176

Question 3.7

Consider the proof of Cauchy's Theorem with $G = D_5$ and $p = 5$. Describe the set X and the group acting on X. Determine the possible sizes of the orbits in X under this action and write out, in full, two distinct orbits for each of these possible sizes.

Show Solution 3.7 on P177

Chapter 4

Quotient Groups

We start this chapter with three examples that are intended to motivate much of what follows.

Example 4.1. Consider the group $\mathbb{Z}_6$ and one of its subgroups $H = \{0, 3\}$. The distinct left cosets of H in $\mathbb{Z}_6$ are:

$$eH = 0 + \{0, 3\} = \{0, 3\} = 3 + \{0, 3\} = 3H,$$

$$1H = 1 + \{0, 3\} = \{1, 4\} = 4 + \{0, 3\} = 4H,$$

$$2H = 2 + \{0, 3\} = \{2, 5\} = 5 + \{0, 3\} = 5H.$$

We then re-order the row and column of the Cayley table for $\mathbb{Z}_6$ in 'coset order'.

		H		$1+H$		$2+H$	
	$\oplus_6$	0	3	1	4	2	5
H	0	0	3	1	4	2	5
	3	3	0	4	1	5	2
$1+H$	1	1	4	2	5	3	0
	4	4	1	5	2	0	3
$2+H$	2	2	5	3	0	4	1
	5	5	2	0	3	1	4

On replacing 'blocks' by cosets we obtain:

$\circ$	H	$1+H$	$2+H$
H	H	$1+H$	$2+H$
$1+H$	$1+H$	$2+H$	H
$2+H$	$2+H$	H	$1+H$

This looks like a Cayley table for a group of cosets - but note that we do not have a binary operation.

Finally, if we ignore the H's and use the fact that $0+H=H$, we obtain the following:

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

So, it would appear that if H is a subgroup of G, then we can 'divide' G by H to obtain a group of order $|G|/|H|$. Let's see if this works for another group.

Example 4.2. Consider the subgroup $H = \{e, r_1, r_2\}$ of D_3. Here the distinct left cosets of H in D_3 are: $eH = r_1H = r_2H = \{e, r_1, r_2\}$ $s_1H = s_2H = s_3H = \{s_1, s_2, s_3\}$.

		H			s_1H		
	$\circ$	e	r_1	r_2	s_1	s_2	s_3
	e	e	r_1	r_2	s_1	s_2	s_3
H	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_1H	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

Which looks like:

$\circ$	H	s_1H
H	H	s_1H
s_1H	s_1H	H

So far, so good. Now let's try another.

Example 4.3. Consider the subgroup $H = \{e, s_1\}$ of D_3. Here the distinct left cosets of

H in D_3 are:

$$eH = s_1H = \{e, s_1, \}, r_1H = s_3H = \{r_1, s_3\}, r_2H = s_2H = \{r_2, s_2\}.$$

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

This time the Cayley table is not partitioned into coset 'blocks'. We will see that the process of 'factoring' a group G by one of its subgroups H can yield useful information about G, but first we need to examine exactly when the procedure works.

4.1 Normal Subgroups and Quotient Groups

Let H be a subgroup of a group G. Now H has both left and right cosets and, in general, a left coset aH, $a \in G$, need not be the same as the right coset Ha. Suppose we try to define a binary operation on left cosets as follows:

$$(aH)(bH) = (ab)H. \tag{4.1}$$

It is important to realise that this rule does not necessarily define a binary operation on the left cosets of H in G. This is because it is defined in terms of elements a and b but, in general, the cosets will have other representatives and we need to show that it does not matter which representative we choose (this is the same as the situation involving the representatives of the equivalence classes modulo some integer m).

First recall that $a' \in aH$ and $b' \in bH$ if and only if $aH = a'H$ and $bH = b'H$ (cosets are either distinct or equal).

Second, recall that a binary operation gives a unique result. In particular for Equation 4.1 to define a binary operation, we must have that

$$(aH)(bH) = (a'H)(b'H)$$

or, equivalently,

$$(ab)H = (a'b')H.$$

Consider the case where $G = D_3$ and $H = \{e, r_1, r_2\}$. We have:

$$H = r_1H = r_2H = \{e, r_1, r_2\}$$
$$s_1H = s_2H = s_3H = \{s_1, s_2, s_3\}.$$

It then follows, for example, that:

$$(r_1H)(s_1H) = (r_1s_1)H = s_3H$$
$$(r_1H)(s_2H) = (r_1s_2)H = s_1H$$
$$(r_2H)(s_3H) = (r_2s_3)H = s_1H$$

In particular, we see that:

$$(r_1H)(s_1H) = (r_1H)(s_2H) = (r_2H)(s_3H)$$

Note that, although we have changed the representative of the coset, this does not alter the outcome.

But, suppose $G = D_3$, $H = \{e, s_1\}$. The distinct left cosets are,

$$\{e, s_1\} = eH = s_1H;\ \{r_1, s_3\} = r_1H = s_3H;\ \{r_2, s_2\} = r_2H = s_2H.$$

Then,

$$(eH)(r_1H) = (er_1H) = r_1H$$
$$(s_1H)(s_3H) = (s_1s_3H) = r_2H$$

but $r_1H \neq r_2H$. In this example, Equation Equation 4.1 does not define a binary operation.

It is important to realise what this does (and does not) mean.

With $G = D_3$ and $H \in \{e, r_1, r_2\}$, then

$$s_1H = \{s_1e, s_1r_1, s_1r_2\} = \{s_1, s_2, s_3\}$$
$$Hs_1 = \{es_1, r_1s_1, r_2s_2\} = \{s_1, s_2, s_3\}.$$

So $s_1H = Hs_1$ even though $s_1r_1 \neq r_1s_1$ for instance. However, for $H = \{e, s_1\}$

$$r_1H = \{r_1e, r_1s_1\} = \{r_1, s_3\}$$
$$Hr_1 = \{er_1, s_1r_1\} = \{r_1, s_2\}.$$

so $r_1H \neq Hr_1$.‘

Definition 4.1 (Normal Subgroup)**.** A subgroup H of a group G is *normal* if its left and right cosets coincide, that is if $gH = Hg\ \forall\, g \in G$.

We shall often use the notation $H \lhd G$ to denote that H is a normal subgroup of G. The

next Lemma tells us that $(*)$ defines a binary operation provided that, for all elements of the group, the left and right cosets coincide for a given subgroup. The Lemma is, in fact, an 'if and only if' statement; we prove only the forward implication below as the converse does not add anything to what we need.

Lemma 4.1. *Let H be a subgroup of a group G. If $gH = Hg$ for all $g \in G$, then left coset multiplication is well-defined by $(aH)(bH) = (ab)H$.*

(It does not matter which representative we choose in any given coset - in this context that is what we mean by well-defined.)

Proof.

Let $a, a', b, b' \in G$ satisfy $aH = a'H$ and $bH = b'H$. We show that

$$(aH)(bH) = abH = a'b'H = (a'H)(b'H).$$

There are elements $h, k \in H$ such that $a'h = a$ and $b'k = b$. Therefore

$$a'b'H = ahbkH = ahbH$$

since $kH = H$ as $k \in H$.

Observe that hb is an element of the right coset Hb. Since $Hb = bH$, there is an element $j \in H$ such that $hb = bj$ and so

$$a'b'H = ahbH = abjH = abH$$

as required,

□

> **Note**
>
> If G is abelian then every subgroup is normal!

As a convention we will often use N to denote a normal subgroup. The following result is the one towards which we have been building.

Theorem 4.1. *Let N be a normal subgroup of a group G. Then the cosets of N form a group G/N under the binary operation $(aN)(bN) = (ab)N$.*

Proof.

We note that the set G/N is non-empty as it contains the coset $eN = N$.

Since N is a normal subgroup of G then by Lemma 4.1 the binary operation is closed.

For associativity, let $a, b, c \in G$, then

$$\begin{aligned}(aNbN)(cN) &= abNcN \\ &= (ab)cN \\ &= a(bc)N \\ &= aN(bcN) \\ &= aN(bNcN)\end{aligned}$$

The identity element if eN.

lastly, the inverse of aN is $a^{-1}N$.

□

The group G/N in the above theorem is called the *quotient* or *factor* group of G with N. The following Lemma gives the standard way of showing that a subgroup is normal.

Lemma 4.2. *Let G be a group and H a subgroup of G. Then H is normal in G if and only if for all $g \in G$*

$$gHg^{-1} \subseteq H,$$

where $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.

Proof.

First suppose that H is a normal subgroup of G. Let $g \in G$ and $h \in H$. Since $gH = Hg$ there is an element $k \in H$ such that $gh = kg$. Post-multiplying by g^{-1} now yields:

$$ghg^{-1} = kgg^{-1} = ke = k.$$

Therefore $ghg^{-1} \in H$. Since $h \in H$ was arbitrary, we conclude that $gHg^{-1} \subseteq H$.

Now suppose that $gHg^{-1} \subseteq H$ for all $g \in G$. Let $g \in G$. Let $gh \in gH$ be arbitrary. Then,

$$gh = ghe = gh(g^{-1}g) = (ghg^{-1})g = kg$$

where $k \in H$ is equal to ghg^{-1} since by assumption $gHg^{-1} \subseteq H$. Therefore we conclude that $gh \in Hg$. Since $h \in H$ was arbitrary we see that $gH \subseteq Hg$

Similarly, given $k \in H$, then observe that $kg = gg^{-1}kg$. Since $g^{-1} \in G$, then by assumption, $g^{-1}Hg \subseteq H$ and so there is $h \in H$ such that $g^{-1}kg = h$. Therefore,

$$kg = g(g^{-1}kg) = gh \in gH.$$

We conclude that $Hg \subseteq gH$ and so $Hg = gH$.

Since $g \in G$ was arbitrary, we conclude that $gH = Hg$ for all $g \in G$ and H is a normal subgroup.

□

For any non-abelian group an important normal subgroup of G is the *centre* of G. This

consists of all the elements that commute with every other element of the group.

Definition 4.2 (Centre)**.** Let G be a group and $z, g \in G$, then the *centre* of G is denoted and defined by

$$Z(G) = \{z \in G \mid zg = gz, \ \forall\, g \in G\}.$$

Obviously, a group is abelian if and only if $Z(G) = G$, so this concept is only of interest for non-abelian groups. That the centre forms a normal subgroup is the content of the next theorem.

Theorem 4.2. *The centre of a group G forms a normal subgroup of G.*

Proof.

First observe that $Z(G)$ if it is a subgroup must be a normal subgroup. This follows since for $z \in Z(G)$ and $g \in G$

$$gzg^{-1} = gg^{-1}z = z.$$

Therefore $gZ(G)g^{-1} = Z(G)$ for all $g \in G$.

We now show that $Z(G)$ is a subgroup.

First notice that $e \in Z(G)$ since $eg = ge = g$ for all $g \in G$.

Let $y, z \in Z(G)$ and consider yz. Let $g \in G$, then

$$yzg = y(zg) = y(gz) = (yg)z = (gy)z = gyz.$$

Therefore, $yz \in Z(G)$.

Lastly consider $(zg^{-1})^{-1}$, we have

$$gz^{-1} = (zg^{-1})^{-1} = (g^{-1}z)^{-1} = z^{-1}g$$

and so $gz^{-1} = zg^{-1}$ and $z^{-1} \in Z(G)$.

□

Example 4.4.

We consider the centre of various group we have already encountered:

- $Z(D_3) = \{e\}$;
- $Z(D_4) = \{e, r_2\}$;
- $Z(D_5) = \{e\}$;
- $Z(D_6) = \{e, r_3\}$;
- $Z(A_4) = \{e\}$;
- $Z(\mathbb{Z}_2 \times D_4) = \{(0, e), (1, e), (0, r_2), (1, r_2)\}$.

4.2 Further Examples of Normal Subgroups

Example 4.5. For any group G, the trivial subgroup $\{e\}$ is normal and, since $\{e\}$ contains only one element, every coset of $\{e\}$ contains only one element. It is therefore easy to see that

$$G/\{e\} \cong G$$

since all we have done is to rename $g \in G$ by the coset $g\{e\} = \{g\}$.

Example 4.6. At the other extreme, we have that for any group G, G itself is a normal subgroup of G and G/G is the trivial group — the group of order 1.

These two extremes of quotient groups are of little importance because they tell us nothing new about the structure of G. We now consider an example where H is a subgroup of G and has half the size of G. Consider $a \in G\backslash H$ (so $a \notin H$); then aH must be all of $G\backslash H$ (because H and aH are disjoint and of equal size and $a \in aH$) and, similarly, Ha must be all of $G\backslash H$, so $aH = Ha$. Thus it follows that any subgroup that is half the size of the group must be normal in that group and $|G| = 2|N|$.

Example 4.7. Since $|S_n| = 2|A_n|$ we have that A_n is a normal subgroup of S_n and S_n/A_n has order 2. If σ is any odd permutation, for example $(1\ 2) \in S_n$, then $\sigma \in S_n \backslash A_n$, the elements of S_n/A_n are $\{A_n, \sigma A_n\}$ and its Cayley table is:

	A_n	σA_n
A_n	A_n	σA_n
σA_n	σA_n	A_n

Example 4.8. Lagrange's Theorem states that if H is a subgroup of a finite group G, then the order of H divides the order of G. In the Abstract Algebra module we stated that the converse is false; we are now in a position to prove this by showing that A_4, which has order 12, contains no subgroup of order 6.

Proof. Suppose A_4 had a subgroup N of order 6, then N must be a normal subgroup as it has only 2 left cosets N and σN for any $\sigma \in A_4 \backslash N$. Let σ be any element of A_4 that is not an element of N, we can write down the Cayley table of the quotient group A_4/N,

	N	σN
N	N	σN
σN	σN	N

Notice that

$$NN = (eN)(eN) = N = (\sigma\sigma N) = \sigma N \sigma N.$$

From this it follows that for any $\sigma \in A_4$, $(\sigma^2)N = N$. This means that $\sigma^2 \in N$ for any $\sigma \in A_4$. However for any three cycle $(a\ b\ c)$, it square, $(a\ c\ b)$ is also a three cycle. This means that N contains all three cycles. However A_4 has 8 three cycles and so $|N| > 8$ which is a contradiction. □

Example 4.9. Classify the quotient group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle$ according to the Fundamental Theorem of Finitely Generated Abelian Groups.

Let

$$N = \langle (0,1) \rangle = \{(0,0), (0,1), (0,2), (0,3)(0,4), (0,5)\}.$$

Since $\mathbb{Z}_4 \times \mathbb{Z}_6 = 24$, then $(\mathbb{Z}_4 \times \mathbb{Z}_6)/N$ has order 4. By the Fundamental Theorem of Finitely Generated Abelian Groups, $(\mathbb{Z}_4 \times \mathbb{Z}_6)/N$ is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Notice that each of $(1,0), (2,0)$ and $(3,0)$ give rise to distinct cosets since $(a,0)((b,0))^{-1} = (ab^{-1}, 0) \notin N$ for any $a, b \in Z_4$ with a and b not both 0. Therefore the quotient group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/N$ is generated by $(1,0)N$ since $(1,0)^2N = ((1,0)N)^2 = (2,0)N$, $(1,0)^3N = ((1,0)N)^3 = (3,0)N$ and $(1,0)^4N = ((1,0)N)^4 = N$.

The above example is a special case of the following theorem.

Theorem 4.3. *Let $G = H \times K$ be the direct product of groups H and K. Then*

$$\overline{K} = \{(e,k) \mid k \in K\}$$

is a normal subgroup of G isomorphic to K and $G/\overline{K} \cong H$.

Proof.

It is easily verified that $\overline{K}$ is a subgroup of G and the map $(e,k) \mapsto k$ from $\overline{K} \to K$ is an isomorphism.

Let $(h,k) \in G$ be arbitrary, then:

$$\begin{aligned}(h,k)\overline{K} &= \{(h,k)(e,k') : k' \in K\} \\ &= \{(h,kk') : k' \in K\} \\ &= \{(h,k'') : k'' \in K\}.\end{aligned}$$

Therefore, $(h,k)\overline{K} = \{(h,k') : k' \in K\}$. Similarly,

$$\begin{aligned}\overline{K}(h,k) &= \{(h,k'k) : k' \in K\} \\ &= \{(h,k'') : k'' \in K\}.\end{aligned}$$

Therefore,

$$(h,k)\overline{K} = \overline{K}(h,k)$$

and H is a normal subgroup.

Observe that the order of $G/\overline{K}$ is equal to the order of H. Moreover, for all $h_1, h_2 \in H$ with $h_1 \neq h_2$,

$$(h_1,e)K = \{(h_1,k) : k \in K\} \neq \{(h_2,k) : k \in K\} = (h_2,e)K.$$

Therefore, the left cosets of $\overline{K}$ (the elements of $G/\overline{K}$) are

$$\{(h,e)\overline{K} : h \in H\}.$$

It now follows that the map $\phi : G/\overline{K} \to H$ by $(h,e)\overline{K} \mapsto h$ is an isomorphism.

□

The following two examples provide further twists on looking at subgroups of the right-hand factor of the direct product, in the sense that in Example 4.10 and Example 4.9, the cyclic subgroup makes no contribution to the left-hand factor whereas that will not be the case in Example 4.11.

Example 4.10. Classify the quotient group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle$ according to the Fundamental Theorem of Finite Abelian Groups.

	Order	$\theta : G \to \mathbb{Z}_4 \times \mathbb{Z}_2$
$\overline{K} = \langle(0,2)\rangle = \{$ $\}$	1	
$(1,0) + \langle(0,2)\rangle = \{$ $\}$		
$(0,1) + \langle(0,2)\rangle = \{$ $\}$		
$(2,0) + \langle(0,2)\rangle = \{$ $\}$		
$(3,0) + \langle(0,2)\rangle = \{$ $\}$		
$(1,1) + \langle(0,2)\rangle = \{$ $\}$		
$(2,1) + \langle(0,2)\rangle = \{$ $\}$		
$(3,1) + \langle(0,2)\rangle = \{$ $\}$		

The group $G = (\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle$ has order $24/3 = 8$ and isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$. Below we give two isomorphisms. The red terms give the image of the corresponding coset under the first isomorphism and the blue terms under the second. Notice that once we specify the images of the generators $(1,0) + \overline{K}$ and $(0,2) + \overline{K}$ the remaining terms are determined. To work out the order of an element, we are effectively answering the question ''What is the smallest positive integer power of that particular representative of the given coset that lands in the subgroup that is the identity?' '

	Order	$\theta : G \to \mathbb{Z}_4 \times \mathbb{Z}_2$	
$\overline{K} = \langle(0,2)\rangle = \{(0,0),(0,2),(0,4)\}$	1	$(0,0)$	$(0,0)$
$(1,0) + \langle(0,2)\rangle = \{(1,0),(1,2),(1,4)\}$	4	$(1,0)$	$(1,1)$
$(0,1) + \langle(0,2)\rangle = \{(0,1),(0,3),(0,5)\}$	2	$(0,1)$	$(0,1)$
$(2,0) + \langle(0,2)\rangle = \{(2,0),(2,2),(2,4)\}$	2	$(2,0)$	$(2,0)$
$(3,0) + \langle(0,2)\rangle = \{(3,0),(3,2),(3,4)\}$	4	$(3,0)$	$(3,1)$
$(1,1) + \langle(0,2)\rangle = \{(1,1),(1,3),(1,5)\}$	4	$(1,1)$	$(1,0)$
$(2,1) + \langle(0,2)\rangle = \{(2,1),(2,3),(2,5)\}$	2	$(2,1)$	$(2,1)$
$(3,1) + \langle(0,2)\rangle = \{(3,1),(3,3),(3,5)\}$	4	$(3,1)$	$(3,0)$

Example 4.11. Classify the quotient group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2,3)\rangle$ according to the Fundamental Theorem of Finite Abelian Groups.

The subgroup $N = \langle (2,3) \rangle$ has order two and is equal to $\{(0,0),(2,3)\}$. Therefore taking $G = \mathbb{Z}_4 \times \mathbb{Z}_6$, G/N has order 12. Two elements (a,b) and (c,d) belong to the same coset of G if and only if $(a-c, b-d) \in N$ That is $a = c$ and $b = d$ or a and c differ by 2 and b and d differ by 3. This gives left cosets:

$$(0,0)N, (0,1)N, (0,2)N, (0,3)N, (0,4)N, (0,5)N,$$
$$(1,0)N, (1,1)N, (1,2)N, (1,3)N, (1,4)N, (1,5)N.$$

Since $|G/N| = 12$, then by the Fundamental Theorem of Finite Abelian Groups G/N is either isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$ or to $\mathbb{Z}_{12}$. However, we observe that G/N contains an element of order 4, $(1,0)N$. Since $((1,0)N)^2 = (2,0)N = (0,3)N$ and $((0,3)N)^2 = (0,0)N = N$. Therefore, G/N is isomorphic to $\mathbb{Z}_{12}$ and is in fact generated by $(1,2)N$.

4.3 The Correspondence Theorem

In general, a finite quotient group G/N will be smaller than G and we may hope that it has a simpler structure. It would be nice if knowing the structure of G/N helped us to understand the structure of G. Our main result, in this regard, is the following theorem which we state for finite groups (the statement is also true for infinite groups, but the proof is longer and we shall only use the finite case).

Theorem 4.4 (The Correspondence Theorem)**.** *Let N be a normal subgroup of a finite group G. Then H is a subgroup of G containing N if and only if H/N is a subgroup of G/N, and every subgroup of G/N has this form for some H in G.*

What this theorem says is that if N is a normal subgroup of G then, given a subgroup of G containing N, we can produce a unique subgroup of the quotient group G/N and, conversely, given a subgroup of the quotient group we can produce a corresponding subgroup of G that contains N.

We leave the proof until we have studied an illustrative example of how the Correspondence

Theorem works.

First consider the direct product group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$\oplus_2$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

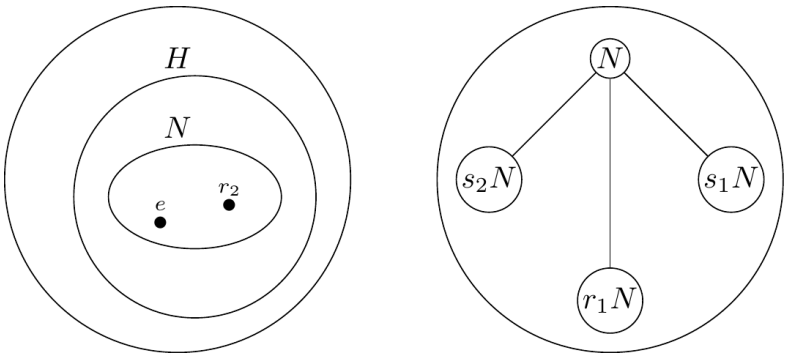
Subgroups of order 2 are:

$$H_1 = \{(0,0),(0,1)\}$$
$$H_2 = \{(0,0),(1,0)\}$$
$$H_3 = \{(0,0),(1,1)\}$$

Excluding the trivial group $\{(0,0)\}$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ itself, these are all the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Now we consider the group $G = D_4$ and its normal subgroup $N = \{e, r_2\}$.

The order of D_4 is 8 and the order of N is 2, therefore the order of D_4/N is 4. Thus, D_4/N is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.



The subgroups of D_4/N are:

$$X_1 = \{N, r_1N\}; N \cup r_1N = \{e, r_1, r_2, r_3\} \leq D_4$$
$$X_2 = \{N, s_1N\}; N \cup s_1N = \{e, r_2, s_1, s_3\} \leq D_4$$
$$X_1 = \{N, s_2N\}; N \cup s_2N = \{e, r_2, s_2, s_4\} \leq D_4.$$

Now we prove the theorem.

Theorem 4.5 (The Correspondence Theorem)**.** *Let N be a normal subgroup of a finite group G. Then H is a subgroup of G containing N if and only if H/N is a subgroup of G/N, and every subgroup of G/N has this form for some H in G.*

proof of the correspondence theorem.

Let H be a subgroup of G that contains N. Notice that since N is normal in G, then N is normal in H. This follows as since $hN = Nh$ for all $h \in G$, then $hN = Nh$ for all $h \in H \leq G$. It therefore follows that H/N is a group, however $H/N \subset G/N$ and so H/N is a subgroup of G/N.

Now suppose X is a subgroup of G/N. Let $\{N, x_1N, x_2N, \ldots, x_rN\} \subseteq G/N$ be the distinct elements of X. Define

$$H := \bigcup_{1 \leq i \leq r} x_iN = \{x_in : 1 \leq i \leq r, n \in N\}.$$

If H is a subgroup of G, then it is a subgroup of G that contains N and H/N is precisely the subgroup X of G/N. Thus we need only show that H is a subgroup of G. Clearly H is non-empty since it contains N. Let $x, z \in H$. There are x_i, x_j, $1 \leq i, j \leq r$ and $n_1, n_2 \in N$ such that $x_in_1 = x$ and $x_jn_2 = y$. Therefore

$$xy = x_in_1x_jn_2 = x_ien_1x_jn_2 = x_ix_jx_j^{-1}n_1x_jn_2 = x_ix_j(x_j^{-1}n_1x_j)n_2.$$

Since N is a normal subgroup of G, $(x_j^{-1}n_1x_j) \in N$ and so there is an $n \in N$ such that $(x_j^{-1}n_1x_j)n_2 = n$. Thus,

$$xy = x_ix_jn.$$

Lastly, as X is a subgroup of G/N, then there is a k between 1 and r such that

$$(x_iN)(x_jN) = (x_ix_j)N = x_kN.$$

Thus, there is an element $m \in N$ such that $xy = x_ix_jn = x_km$ and so $xy \in H$. This means that H is closed under products.

One can similarly show that H is closed under inverses, however, as H/N is finite, it is enough to show closure under products.

□

Note

One can actually demonstrate the uniqueness of the group H above. For if H and H' satisfy $H/N = H'/N$, then for $x \in H$, there is an $x' \in H'$ such that $xN = x'N$. In particular, there is an $m \in N$ such that $x = x'm$ and so, as $N \leq H'$, $x \in H'$. This demonstrates that $H \subseteq H'$; swapping the order of H and H' above, we also have that $H' \subseteq H$. Thus, $H = H'$ as required.

Example 4.12.

Let G be the group D_4. Let N be the normal subgroup of D_4, $N = \{e, r_2\}$. Since $|D_4| = 8$, then D_4/N has order 4. It follows that $D4/N$ is either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. However, we observe that every element of D_4/N has order 2. Indeed we need only check the element r_1N:

$$(r_1N)^2 = r_1^2N = r_2N = N.$$

We conclude that D_4/N is in fact $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Now D_4/N has three subgroups of order two each of which corresponds to a subgroup of order 4 in D_4:

Subgroup of N	Corresponding subgroup of D_4
$\{N, r_1N\}$	$\{e, r_2, r_1, r_3\}$
$\{N, s_1N\}$	$\{e, r_2, s_1, s_3\}$
$\{N, s_2N\}$	$\{e, r_2, s_2, s_4\}$

Thus we have all thee subgroups of G of order 4 each containing N and corresponding to exactly **one** of the subgroups of order 2 in D_4/N.

Example 4.13. Demonstrate the proof of the Correspondence Theorem where the quotient group is

$$(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle.$$

We demonstrated in Example 4.10 that $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Non-trivial (that is not equal to the subgroups $\{(0,0)\}$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$) subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_2$ have order 2 and 4. There are 3 distinct subgroups of order 4

$$\langle(1,0)\rangle, \langle((1,1))\rangle, \text{ and, } \langle(2,0),(0,1)\rangle.$$

Each element of order 2 of $\mathbb{Z}_4 \times \mathbb{Z}_2$ generates a unique subgroup of order 2, there are 3 of them:

$$\langle(2,0)\rangle, \langle((2,1))\rangle, \text{ and, } \langle((0,1)\rangle.$$

Using Example 4.10, and setting $N = \langle(0,2)\rangle$, we can write down the correspondence between the subgroups of $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$

Subgroups of order 4	Corresponding subgroup of $\mathbb{Z}_4 \times \mathbb{Z}_6$
$\{N, (1,0)N, (2,0)N, (3,0)N\}$	$\{e, (0,2), (0,4), (1,0), (1,2), (1,4),$ $(2,0), (2,2), (2,4), (3,0), (3,2), (3,4)\}$
$\{N, (1,1)N, (2,0)N, (3,1)N\}$	$\{e, (0,2), (0,4), (1,1), (1,3), (1,5),$ $(2,0), (2,2), (2,4), (3,1), (3,3), (3,5)\}$
$\{N, (0,1)N, (2,1)N, (2,0)N\}$	$\{e, (0,2), (0,4), (0,1), (0,3), (0,5),$ $(2,1), (2,3), (2,5), (2,0), (2,2), (2,4)\}$

Subgroups of order 2	Corresponding subgroup of $\mathbb{Z}_4 \times \mathbb{Z}_6$
$\{N, (0,1)N\}$	$\{e, (0,2), (0,4), (0,1), (0,3), (0,5)\}$
$\{N, (2,0)N\}$	$\{e, (0,2), (0,4), (2,0), (2,2), (2,4)\}$
$\{N, (2,1)N\}$	$\{e, (0,2), (0,4), (2,1), (2,3), (2,5)\}$

Example 4.14.

Let G be a group of order 44. Suppose G has a normal subgroup N of order 11, so that G/N is a group of order 4. Thus G/N is isomorphic either to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Now both $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ have subgroups of order 2 and so G has a subgroup H containing N such that H/N has order 2. This means that H has order 22 and so must itself be a normal subgroup of G. Thus H is a normal subgroup of G containing N.

4.4 Normalisers

We now consider a question which may seem artificial, but will turn out to be very important.

> Given a subgroup, H, of a group G, what is the largest subgroup of G containing H as a normal subgroup?

Consider the group $H = \{e, r_2\} \lhd D_4$. The largest subgroup of D_4 in which H is normal,

is D_4 itself.

Now $\{e, s_1\}$ is **not** a normal subgroup of D_4, but $\{e, r_2, s_1, s_3\}$ is a subgroup of D_4 in which $\{e, s_1\}$ is normal. Notice that the elements $g \in D_4$ such that $g\{e, s_1\} = \{e, s_1\}g$ are precisely e, r_2, s_1 and s_3.

We had better make sure that this is a sensible question! If H is a normal subgroup of G, then the answer is G. If H is not normal in G can we be certain that there is a subgroup of G that contains H as a normal subgroup? Yes! Any group is a normal subgroup of itself so H is a subgroup of G containing H as a normal subgroup. Having established the existence of such a subgroup it makes sense to ask for the largest such subgroup (except that there may be more than one). Let L be a largest subgroup of G containing H as a normal subgroup. It is certainly the case that any element $l \in L$ has the property that $lH = Hl$. It would be nice if every element $g \in G$ with the property that $gH = Hg$ formed a subgroup of G, then this subgroup would certainly answer our question. We first define this set, then prove that it is a subgroup.

Definition 4.3 (Normaliser)**.** Let H be a subgroup of a group G. The *normaliser* of H in G is denoted and defined by

$$N(H) = \{g \in G | gH = Hg\}.$$

Theorem 4.6. *Let H be a subgroup of a group G, then the normaliser of H in G forms a subgroup of G.*

Proof.

We prove this both directly, in the normal way, and indirectly using a group action.

- **Direct proof**: Clearly $e \in N(H)$ since $eH = H = He$. Let $g_1, g_2 \in N(H)$. Then

$$g_1 g_2 H = g_1(g_2 H) = g_1(Hg_2) = (g_1 H)g_2 = H(g_1 g_2)$$

and so $g_1g_2 \in N(H)$. Let $g \in N(H)$ and consider gh_1 for $h_1 \in H$. There is and $h_2 \in H$ such that $gh_1 = h_2g$. Taking inverses of both sides

$$h_1^{-1}g^{-1} = (gh_1)^{-1} = (h_2g)^{-1} = g^{-1}h_2^{-1}.$$

We conclude that $g^{-1}H = Hg^{-1}$.

- **Indirect proof**:

  We define an action $*$ of G on the set of all of the subsets of G. In terms of the definition of a group action (see Definition 3.1) this set is the set denoted X and we need to demonstrate that all three conditions hold. Clearly for $S \subseteq G$, gSg^{-1} is again a subset of G. Thus $g * S \in X$ for all $S \in X$ and $g \in G$. Moreover,

  - $e * S = eSe^{-1} = eSe = S$ for all $S \in X$;
  - $g_1 * (g_2 * S = g_1 * (g_2Sg_2^{-1}) = g_1g_2Sg_2^{-1}g_1^{-1} = g_1g_2S(g_1g_2)^{-1} = (g_1g_2) * S$. So $*$ is indeed an action of G on the set of all subsets of G. We know that the stabiliser of an element of X under the action is a subgroup of G. However, the stabiliser of a subgroup under this particular action, is just the normaliser of the subgroup yielding the result.

□

4.5 Problem Sheet 4

For Week 9; covers Chapter 4.

Question 4.1

Classify each of the following groups according to the Fundamental Theorem of Finite Abelian Groups and in each case give an isomorphism from the stated group to the group given as your answer.

(a) $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1,0)\rangle$.

(b) $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$.

(c) $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(2,2)\rangle$.

Show Solution 4.1 on P178

Question 4.2

Let H be a subgroup of a group G.

(a) Show that, for all $g \in G$, the set

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

forms a subgroup of G.

(b) Deduce that if G has exactly one subgroup, H, of a given finite order, then H is a normal subgroup of G.

Show Solution 4.2 on P180

Question 4.3

Let H be a subgroup of a group G. Prove that the centre of G is a normal subgroup of the normaliser of H. [Hint: all you really need to show is that $Z(G) \subseteq N(H)$ and the rest is 'obvious'.]

Show Solution 4.3 on P181

Question 4.4

Let $n \geq 3$. Show that the centre of S_n is trivial. What is the centre of S_2?

Show Solution 4.4 on P182

Question 4.5

Let N be a normal subgroup of a finite group G, and H be a further subgroup of G (which need not be normal in G). Show that the set NH, where

$$NH = \{nh \,|\, n \in N, h \in H\}$$

forms a subgroup of G.

Show Solution 4.5 on P182

Question 4.6

In D_4, let e and r_2 denote the identity and π radians rotation respectively. Given that $N = \{e, r_2\}$ is a normal subgroup of D_4, give an example of a surjective homomorphism

$$\phi : D_4 \to D_4/N$$

and classify D_4/N according to the Fundamental Theorem of Finite Abelian Groups.

Show Solution 4.6 on P183

Question 4.7

Consider the quarternion group Q_8 with elements $\{\pm 1, \pm i, \pm j, \pm k\}$ and multiplication defined by the rules:

$$(-1)^2 = 1,$$
$$i^2 = j^2 = k^2 = -1,$$

and

$$ij = k = -(ji), jk = i = -(kj), ki = j = -(ik).$$

The group $N = \{1, -1\}$ is a normal subgroup of Q_8. Find elements $g_1, g_2, \ldots, g_i \in Q_8$ such that $\{g_1N, g_2N \ldots, g_iN\}$ are the distinct left cosets of N in G.

Classify the group Q_8/N according to the Fundamental Theorem of finite abelian groups.

Show Solution 4.7 on P184

Chapter 5

Group Homomorphisms Revisited

We now come to the central topic of Algebra. Homomorphisms have been at work behind the scenes in much of our work in this module as well as in the Abstract Algebra module. Informally, a homomorphism is a structure-preserving mapping from one group into another group, G into G' say. Such mappings are used to provide information about the structure of G' from the known structural properties of G and vice versa. The formal definition is as follows:

Definition 5.1 (Homomorphism)**.** Let G and G' be groups. A mapping $\phi : G \to G'$ is a *homomorphism* if, for all $x, y \in G$

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

> **Note**
>
> An isomorphism is simply a bijective homomorphism.

An easy example of structure preservation is the following lemma.

Lemma 5.1. *Let ϕ be a homomorphism from a group G into 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.

We take each in turn.

i. Notice that

$$\phi(x) = \phi(xe) = \phi(x)\phi(e).$$

Pre-multiplying by $\phi(x)^{-1}$, and writing e' for the identity of G' we have:

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

as required.

ii. We have:

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

Therefore $\phi(x)^{-1} = \phi(x)$ as required.

□

Example 5.1.

The map $\phi : \mathbb{Z} \to \mathbb{Z}_2$ by $\phi(n) = \begin{cases} 0, & n \text{ is even} \\ 1, & n \text{ is odd} \end{cases}$. Then ϕ is a homomorphism. This follows since the sum of two even or two odd numbers is even and the sum of an odd and even number is odd.

Example 5.2.

Two homomorphisms arise naturally in linear algebra:

i. Let V and W be vector spaces and $T : V \to W$ be a linear transformation. Recall that V and W form abelian groups under vector addition $+$. Thus $T : (V, +) \to (W, +)$

is a homomorphism since

$$T(u+v) = T(u) + T(v)$$

for all $u, v \in V$.

ii. The set $\mathrm{GL}(n, \mathbb{R})$ of all invertible $n \times n$ matrices over the real numbers is a group under matrix multiplication. The map $\det : \mathrm{GL}(n, \mathbb{R}) \to (\mathbb{R}\backslash\{0\}, \times)$ by $A \mapsto \det(A)$ is a homomorphism since $\det(AB) = \det(A)\det(B)$.

Example 5.3.

Similarly to Example 5.1 we can define a homomorphism ϕ from the symmetric group S_n to $\mathbb{Z}_2$ by:

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

Example 5.4.

The set $\mathrm{C}[a, b]$ of all continuous functions on the interval $[a, b]$ forms a group under pointwise addition:

$$f + g(x) = f(x) + g(x).$$

The map $\phi : \mathrm{C}[a, b] \to \mathbb{R}$, defined by

$$\phi(f) = \int_a^b f(x)\ \mathrm{d}x$$

is a group homomorphism for

$$\int_a^b (f+g)(x)\ \mathrm{d}x = \int_a^b f(x) + g(x)\ \mathrm{d}x = \int_a^b f(x)\ \mathrm{d}x + \int_a^b g(x)\ \mathrm{d}x.$$

Example 5.5.

Consider the group D_4 and the normal subgroup $N = \{e, r_1, r_2, r_3\}$. Define $\phi : D_4 \to$

D_4/N by $\phi(g) = gN$. Then ϕ is a homomorphism from D_4 to D_4/N, since

$$\phi(hg) = (hg)N = (hN)(gN) = \phi(h)\phi(g).$$

Notice that all elements of N (in D_4) map to the identity element N in the group D_4/N.

Note that if we chose a non-normal subgroup H of D_4 (e.g $H = \{e, s_1\}$), the map ϕ from D_4 to the set of left cosets of H given by $\phi(g) = gH$ is a well-defined map but is **not** a homomorphism since the set of left cosets of H do not form a group (coset multiplication is only well-defined over cosets of a normal subgroup).

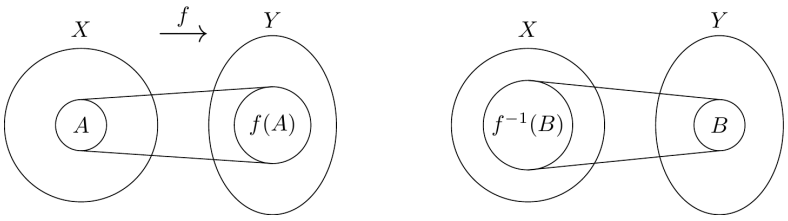
We shall see that there is an intimate connection between homomorphisms and normal subgroups. Before continuing, though, we make the following definition about sets.

Definition 5.2 (Image and Pre-image)**.** 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 in Y under f is denoted and defined by

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

The *pre-image* of B in Y under f is denoted and defined by

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



Our first observation is that the image of a group homomorphism is a group.

Theorem 5.1. *Let ϕ be a group homomorphism from a group G into a group G'. Then, for any subgroup H of G, $\phi(H)$ is a subgroup of G'.*

Proof.

Since $\phi(e)$ is the identity element e' of G', then $\phi(H)$ is non-empty.

Let $g', h' \in \phi(H)$. Then there are elements $g, h \in H$ such that $\phi(g) = g'$ and $\phi(h) = h'$. Thus:

$$g'h' = \phi(g)\phi(h) = \phi(gh) \in \phi(H)$$

and $\phi(H)$ is closed under products.

Moreover,

$$(g')^{-1} = (\phi(g))^{-1} = \phi(g^{-1}) \in \phi(H)$$

and $\phi(H)$ is closed under inverses.

□

5.1 Kernels and the First Isomorphism Theorem

In this section we establish the fundamental connection between homomorphisms and normal subgroups. We begin with a definition.

Definition 5.3 (Kernel)**.** Let ϕ be a group homomorphism from a group G into a group G'. The *kernel* of ϕ is denoted and defined by

$$ker(\phi) = \phi^{-1}(e') = \{x \in G \,|\, \phi(x) = e'\},$$

where e' is the identity in G'.

The kernel of a homomorphism consists, therefore, of all of the elements of G that are mapped onto the identity in G'.

Lemma 5.2. *Let ϕ be a group homomorphism from a group G into a group G'. Then $ker(\phi)$ is a normal subgroup of G.*

Proof.

First we need to demonstrate that $ker(\phi)$ is a subgroup. Clearly, the $ker(\phi)$ is non-empty since it contains the identity of G.

Let $g, h \in ker(\phi)$. Then

$$\phi(gh) = \phi(g)\phi(h) = e'e' = e'$$

for e' the identity element of G'. Therefore, $ker(\phi)$ is closed under products. Moreover,

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

and $ker(\phi)$ is closed under inverses.

These completes the subgroup tests. Now we show that $ker(\phi)$ is a normal subgroup of G.

Let $h \in ker(\phi)$ and $g \in G$. Then

$$\begin{aligned}
\phi(ghg^{-1}) &= \phi(g)\phi(h)\phi(g^{-1}) \\
&= \phi(g)e'\phi(g^{-1}) \\
&= \phi(g)\phi(g^{-1}) \\
&= \phi(gg^{-1}) \\
&= \phi(e) \\
&= e'.
\end{aligned}$$

Therefore, for all $g \in G$, $g\ker(\phi)g^{-1} = \ker(\phi)$ and so $\ker(\phi)$ is a normal subgroup of G.

□

Example 5.6.

The kernel of the map $\phi : \mathbb{Z} \to \mathbb{Z}_2$ is precisely the even integers. (This is clearly a normal subgroup of $\mathbb{Z}$ since $\mathbb{Z}$ is abelian.)

Example 5.7.

Returning to Example 5.2:

i. The kernel of a linear transformation $T : V \to W$ was defined in the linear algebra module as

$$\ker(T) = \{v \in V : T(v) = 0\}.$$

This definition coincides with the definition of the kernel of the group homomorphism $T : (V, +) \to (W, +)$.

ii. The kernel of the homomorphism $\det : \mathrm{GL}(n, \mathbb{R}) \to (\mathbb{R}\backslash\{0\}, \times)$ is the set of all $n \times n$ matrices with determinant 1.

Example 5.8.

The kernel of the homomorphism $\phi : S_n \to \mathbb{Z}_2$ defined by

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

is precisely the normal subgroup A_n of S_n.

Example 5.9.

The kernel of the homomorphism $\phi : \mathrm{C}[a, b] \to \mathbb{R}$ of Example 5.4 is the set of elements of $\mathrm{C}[a, b]$ whose integral over the interval $[a, b]$ is 0. (Note the kernel consists of not just the zero function.)

Example 5.10.

Revisiting Example 5.5, the kernel of the homomorphism ϕ is precisely the normal subgroup N.

Since $ker(\phi)$ is a normal subgroup of G, it follows that we can form the quotient group of G by $ker(\phi)$. The following result tells us that this quotient group is isomorphic to the image

of G under the homomorphism; this is known as the First Isomorphism Theorem (there are two more but we will not need them).

Theorem 5.2 (First Isomorphism Theorem)**.** *Let $\phi : G \to G'$ be a group homomorphism with kernel K. Then*

$$\phi(G) \cong G/K.$$

Proof.

Define a map $\psi : \phi(G) \to G/K$ by $\phi(g) \mapsto gK$ for all $g \in G$. We need to prove that: $+$ that ψ is a well-defined map; $+$ that ψ is a bijection; $+$ that ψ is a homomorphism.

First we prove that ψ is well-defined. Let $g, h \in G$ such that $\phi(g) = \phi(h)$. We need to show that $\psi(\phi(g)) = \psi(\phi(h))$. Since $\phi(g) = \phi(h)$ then $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = e'$, where $'e$ is the identity element of G'. Therefore, $gh^{-1} \in K$. Let $k \in K$ be such that $gh^{-1} = k$. Then, by postmultiplying on both sides by h, we have $g = kh$. We now have,

$$\phi(g) = \phi(kh) = \phi(k)\phi(h) = e'\phi(h) = \phi(h)$$

and $\phi(g) = \phi(h)$ as required.

Clearly the map ψ is surjective since for any $gK \in G/K$ $\psi(\phi(g)) = gK$. Thus it remains only to show that ψ is a injective to conclude that it is bijective.

Suppose $\phi(g), \phi(h) \in \phi(G)$ satisfy $gK = hK$. We want to conclude that $\phi(g) = \phi(h)$. Since $gK = hK$, then $gh^{-1} \in K$. Therefore there is a $k \in K$ such that $g = hk$ (repeating an argument above). Repeating the argument for well-definedness, we conclude that $\phi(g) = \phi(h)$ as required.

The last is the most straightforward. We verify the homomorphism criteria:

$$\psi(\phi(g)\phi(h)) = \psi(\phi(gh)) = ghK = gKhK = \psi(\phi(g))\psi(\phi(h))$$

as required.

□

The converse of the First Isomorphism Theorem is also true, namely if N is a normal subgroup of G then we can easily define a group homomorphism $\phi : G \to G'$ such that $G/N \cong \phi(G)$. The exact nature of the group G' is not important and there are infinitely many groups G' that we could choose to serve our purpose (any group containing a subgroup isomorphic to G/N will do), but the easiest one to choose is $G' = G/N$.

Lemma 5.3. *Let N be a normal subgroup of G. Then $\phi : G \to G/N$ defined by $\phi(x) = xN$, for all $x \in G$, is a homomorphism with kernel N.*

Proof.

The map ϕ is a homomorphism since

$$\phi(xy) = (xy)N = xNyN = \phi(x)\phi(y).$$

Clear $N \subseteq \ker(\phi)$. On the other hand, if $x \in \ker(\phi)$ then $xN = N$ and so $x \in N$. Thus $\ker(\phi) = N$ as required.

□

The map ϕ in the statement of Lemma 5.3 is called the ***natural*** or ***canonical*** homomorphism.

In summary, the image of a homomorphism of G is isomorphic to G/N where N is the kernel of the homomorphism, and for every normal subgroup N of G there is a homomorphism from G to G/N with kernel N (each homomorphism has a different codomain as N changes). Group homomorphisms and quotient groups are really just two different ways of looking at the same thing. Compare the following example and theorem to those in Chapter 4.

Example 5.11. Classify the group $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(0,1)\rangle$ according to the Fundamental Theorem of Finite Abelian Groups.

The map $\phi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ defined by $\phi((x, y)) = x$ is a homomorphism with kernel

$$\{0\} \times \mathbb{Z}_2 = \{(0, 0), (0, 1)\}.$$

Therefore, using the First Isomorphism Theorem, $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(0, 1)\rangle \cong \mathbb{Z}_4$.

In very loose terms the previous example can be represented as follows:

$$(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(0, 1)\rangle = \frac{\mathbb{Z}_4 \times \mathbb{Z}_2}{\{0\} \times \mathbb{Z}_2} = \mathbb{Z}_4.$$

Theorem 5.3. *Let $G = H \times K$ be the direct product of groups H and K. Then $\overline{K} = \{(e, k) \,|\, k \in K\}$ is a normal subgroup of G isomorphic to K and $G/\overline{K} \cong H$.*

Proof.

The map $\phi : H \times K \to H$ by $(h, k) \mapsto h$ is easily verified to be a group homomorphism. The kernel of ϕ is precisely the set

$$\{e_H\} \times K = \{(e_H, k) : K \in K\}$$

where e_H is the identity element of H.

By the First Isomorphism Theorem, we have $\phi(H \times K) = H \cong G/\overline{K}$.

□

5.2 Homomorphisms and Group Actions

When introducing group actions we made the following remark:

> Groups acting on sets are really just thinly disguised permutation groups in that whenever a group G acts on a set X we can associate with each $g \in G$ the permutation f_g of X defined by $f_g(x) = g * x, \ \forall\, x \in X$. These permutations

form a subgroup of $S_{|X|}$, but this group need not be isomorphic to G, and we shall return to this later.

We are now in a position to state precisely what was meant by this, and we begin with the following theorem (note that, as usual, we denote the action of a group element g on an element $x \in X$ by $g * x$):

Theorem 5.4. *Let G be a group acting on a finite set X. Define $\phi : G \to S_{|X|}$ by $\phi(g) = f_g$ where $f_g(x) = g * x$ for all $x \in X$. Then ϕ is a homomorphism.*

Proof.

We need to show that the map ϕ is well-defined. In this context, this means verifying that f_g is in fact a bijection on X. A map is bijective if and only if it is invertible and so it suffices to show that f_g is invertible. We have:

$$(f_g \circ f_{g^{-1}})(x) = f_g(f_{g^{-1}}(x)) = f_g(g^{-1} * x) = g * (g^{-1} * x) = e * x = x.$$

Similarly one has that $f_{g^{-1}} \circ f_g(x) = x$ for all $x \in X$. Therefore f_g is invertible (with inverse $f_{g^{-1}}$) and so it is a bijective map on X.

It now remains to verify that ϕ is a homomorphism. We have

$$\phi(gh)(x) = f_{gh}(x) = (gh) * x = g * (h * x) = f_g(f_h(x)) = \phi(g)(\phi(h)(x))$$

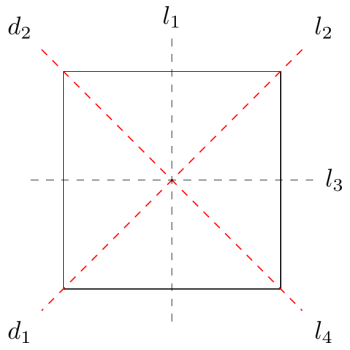
for all $x \in X$. This means that $\phi(gh) = \phi(g)\phi(h)$ and so ϕ is a homomorphism.

□

Remark. The kernel of the homomorphism in Theorem 5.4 is precisely the set of elements $g \in G$ with $\mathrm{fix}\,(g) = X$.

Example 5.12.

Recall that in Chapter 3, Example 3.5 we considered the group D_4 acting on the diagonals d_1 and d_2 of the square.



We demonstrated that the permutation group corresponding to this action is:

$$\left\{ \begin{pmatrix} d_1 & d_2 \\ d_1 & d_2 \end{pmatrix}, \begin{pmatrix} d_1 & d_2 \\ d_2 & d_1 \end{pmatrix} \right\} \cong S_2.$$

By Theorem 5.4, $\phi : D_4 \to S_2$ is defined by:

$$\phi(e) = \phi(r_2) = \phi(s_2) = \phi(s_4) = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

$$\phi(r_1) = \phi(r_3) = \phi(s_1) = \phi(s_3) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

is a homomorphism with kernel $K = \{e, r_2, s_2, s_4\}$. It follows that K is a normal subgroup of D_4 and $D_4/K \cong S_2$.

5.3 Problem Sheet 5

For Week 11; covers Chapter 5.

Question 5.1

Let $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to D_4$ be a homomorphism with kernel $K = \langle (2,2) \rangle$, where D_4 denotes the dihedral group of order 8.

(i) List the elements of K and of $(\mathbb{Z}_4 \times \mathbb{Z}_6)/K$.

(ii) Classify $\phi(\mathbb{Z}_4 \times \mathbb{Z}_6)$ according to the Fundamental Theorem of Finite Abelian Groups.

Show Solution 5.1 on P185

Question 5.2

Let $\phi : G \to G'$ be a group homomorphism. Show that if $|G|$ and $|G'|$ are finite, then:

(a) $|\phi(G)|$ is a divisor of $|G'|$.

(b) $|\phi(G)|$ is a divisor of $|G|$.

(c) $\forall\, g \in G$, the order of $\phi(g)$ divides the order of g.

Show Solution 5.2 on P185

Question 5.3

Let $\phi : G \to G'$ be a group homomorphism. For each of the following statements, show whether it is true or false by providing either a proof or a non-trivial counter-example as appropriate. (The trivial homomorphism from G to G' is defined by $\phi(g) = e',\ \forall\, g \in G$.)

(a) If G is abelian, then G' is abelian.

(b) If G' is abelian, then G is abelian.

(c) If G is abelian, then $\phi(G)$ is abelian.

(d) If $\phi(G)$ is abelian, then G is abelian.

Show Solution 5.3 on P186

Question 5.4

By considering all of the normal subgroups of D_4, determine the number of distinct homomorphisms that exist from D_4 to A_4.

Show Solution 5.4 on P187

Question 5.5

Let G, H, K be groups.

a. If $\phi : G \to H$ is a homomorphism and $\psi : H \to K$ is a homomorphism, show that $\psi\phi : G \to K$.

b. If $\phi : G \to H$ is an isomorphism, show that $\phi^{-1} : H \to G$ is also an isomorphism.

Show Solution 5.5 on P188

Question 5.6

Let G be a group and fix an element $g \in G$. Define a mapping $\kappa_g : G \to G$ by $\kappa_g(h) = ghg^{-1}$ for all $h \in G$. Show that κ_g is an isomorphism from G to G.

Show Solution 5.6 on P189

Question 5.7

Write down a non-trivial homomorphism from A_4 to D_3 and describe its kernel, K. Form the quotient group A_4/K and show directly that this is isomorphic to the image of A_4. (This is a bit tricky; remember that the image of A_4 need not be the whole of D_3, but must be a non-trivial subgroup of D_3.)

Show Solution 5.7 on P190

Chapter 6

The Sylow Theorems

The Sylow Theorems are named after the Norwegian mathematician Ludwig Sylow, who published them in 1872. They are the most important structure theorems of finite group theory after Lagrange's Theorem. Several distinct lines of proof are now known; we shall adopt a blend of the traditional approach, which uses the class equation, and the more modern approach using group actions.

6.1 Conjugates, Centralisers and the Class Equation

We begin with a definition:

Definition 6.1 (Conjugate)**.** Let G be a group and let $x, g \in G$. The *conjugate* of x by g is the element gxg^{-1}.

Example 6.1.

Consider the group D_3 . The conjugates of s_1 are

$$es_1e^{-1} = s_1;\ r_1s_1r_1^{-1} = s_2;\ r_2s_1r_2^{-1} = s_3$$
$$s_1s_1s_1^{-1} = s_1;\ s_2s_1s_2^{-1} = s_3;\ s_3s_1s_3^{-1} = s_2.$$

The set of conjugates of s_1 is therefore $\{s_1, s_2, s_3\}$. These are also the conjugates of s_2 and s_3.

Clearly e is its only conjugate since $geg^{-1} = e$ for all $g \in D_3$. For r_1 we have:

$$er_1e^{-1} = r_1;\ r_1r_1r_1^{-1} = r_1;\ r_2r_1r_2^{-1} = r_1$$
$$s_1r_1s_1^{-1} = r_2;\ s_2r_1s_2^{-1} = r_2;\ s_3r_1s_3^{-1} = r_2.$$

The conjugates of r_1 are therefore r_1 and r_2 — these are also the conjugates of r_2.

At this point the traditional approach would be to show that conjugacy defines an equivalence relation on the elements of G and that the size of each equivalence class divides the order of G. All of this will follow from the Orbit-Stabilizer Theorem once we have established the following:

Lemma 6.1. *Let $(G, \circ)$ be a group and define $*$ on the elements of G by*

$$\forall\, x, g \in G,\ g * x = gxg^{-1}.$$

Then $*$ is a group action of $(G, \circ)$ on G.

Proof.

Clearly $e * x = exe^{-1} = x$ for all $x \in G$. Moreover, for $g_1, g_2 \in G$ we have:

$$\begin{aligned}(g_1g_2) * x &= g_1g_2xg_2^{-1}g_1^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} \\ &= g_1(g_1 * x)g_1^{-1} = g_1 * (g_2 * x).\end{aligned}$$

This complete the verifications. We conclude that $*$ is a group action.

□

If we have established a group action then we know that we must have orbits and stabilisers.

The orbits of the above group action are called the *conjugacy classes* of G, and we denote the conjugacy class containing x by $conj_G(x)$, that is

$$conj_G(x) = \{gxg^{-1} \mid g \in G\}.$$

Example 6.2.

Revisiting Example 6.1 with $G = D_3$, we have:

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

Notice that

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

is a partition of G.

Although the size of the conjugacy classes differ, they all divide the order of G.

The Orbit-Stabilizer Theorem tells us that the order of each conjugacy class divides the order of the group. We also observe that an element x belongs to a conjugacy class of size 1 if and only if $gxg^{-1} = x,\ \forall\, g \in G$ (or, equivalently, if and only if x is in the centre of G, as $xg = gx \Leftrightarrow x = gxg^{-1}$). As the conjugacy classes partition G it is a trivial observation to note that the sum of the sizes of the distinct conjugacy classes of G equals the order of G. This and the preceding remarks form the basis of the so-called *Class Equation* of G. First we state those observations formally. If $C_1, C_2, \ldots, C_r$ are the distinct conjugacy classes of a finite group G, then it follows that

$$|G| = \sum_{i=1}^{r} |C_i|.$$

Suppose we now order those conjugacy classes such that C_1 is the conjugacy class containing

the identity (which has size 1) and that $C_2, \ldots, C_t, C_{t+1}, \ldots, C_r$ are the remaining classes, but where $C_2, \ldots, C_t$ are the trivial classes containing only one element. From what we have said previously we know that

$$|Z(G)| = \sum_{i=1}^{t} |C_i|,$$

that is, the size of the centre is equal to the sum of all of the conjugacy classes of size 1 since each element in those classes must be in the centre. This then leads us to the formal definition:

Definition 6.2 (Class Equation)**.** Let $C_1, C_2, \ldots, C_r$ be the distinct conjugacy classes of a finite group G, ordered so that C_1 is the conjugacy class containing just the identity and $C_2, \ldots, C_t$ $(t \leq r)$ are any further classes that contain just one element. Then the *class equation* of G is

$$|G| = |Z(G)| + \sum_{i=t+1}^{r} |C_i|.$$

In this equation, the summation is the sum of the sizes of all of the non-trivial conjugacy classes. An important property of the Class Equation is that each of the terms on the right hand side is a divisor of the order of G. This follows since $Z(G)$ is a subgroup of G, so the size of $Z(G)$ must divide the order of G and the size of each summand (being an orbit of the action) also divides the order of G.

Example 6.3.

The class equation of D_3 is

$$\begin{aligned} |D_3| &= |\{e\}| + |\{r_1, r_2\}| + |\{s_1, s_2, s_3\}| \\ &= 1 + 2 + 3 \\ &= 6. \end{aligned}$$

6.2 Finite p-Groups

Before proceeding with our development of the Sylow Theorems we pause to consider the structure of finite p-groups (that is, finite groups in which the order of every element is a power of a prime p (definition) or, equivalently, groups of order p^r for some prime p - see Theorem 3.6). We know that groups of order a prime p are cyclic (and hence abelian). We will soon show that groups of order p^2 are abelian and, therefore, isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. We first prove that all finite p-groups have a non-trivial centre (that is, the centre must contain more than one element).

Lemma 6.2. *A finite p-group G of order p^r has a non-trivial centre.*

Proof.

Consider the class equation for G:

$$|G| = |Z(G)| + \sum_{t+1}^{r} |C_i|.$$

Now p divides the order of G and p also divides $\sum_{t+1}^{r} |C_i|$. It follows that p must divide $|Z(G)|$. Therefore $|Z(G)|$ is at least p.

□

Lemma 6.3. *Let G be a non-abelian group. Then $G/Z(G)$ is non-cyclic.*

Proof.

Suppose $G/Z(G)$ is cyclic. This means there is an element $g \in G$ such that

$$\{g^i Z(G) : i \in \mathbb{Z}\} = G/Z(G)$$

that is, the element $gZ(G)$ generates all of $G/Z(G)$. This now means that every element of G can be written in the form $g^i z$ for some $i \in \mathbb{Z}$ and $z \in Z(G)$. Now let $h_1, h_2 \in G$.

There are $i, j \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$ such that $h_1 = g^i z_1 =$ and $h_2 = g^j z_2$. We have:

$$\begin{aligned} h_1 h_2 &= g^i z_1 g^j z_2 = g^i g^j z_1 z_2 = g^j g^i z_1 z_2 \\ &= g^j g^i z_2 z_1 = g^j z_2 g^i z_1 = h_2 h_1. \end{aligned}$$

Therefore, for all $h_1, h_2 \in G$ $h_1 h_2 = h_2 h_1$ and G is abelian. This yields the desired contradiction.

□

Theorem 6.1. *A group G of order p^2, where p is prime, is necessarily abelian.*

Proof.

By Lemma 6.2, p divides the order of $|Z(G)|$. Therefore the order of $Z(G)$ is either p or p^2. If $|Z(G)| = p^2$, then $G = Z(G)$ and G is therefore abelian. We may therefore assume that $|Z(G)| = p$.

Now observe that if $|Z(G)| = p$, then $|G/Z(G)| = p^2/p = p$. Recall that groups of prime order are always cyclic and, hence, abelian. Therefore $G/Z(G)$ is abelian. Lemma 6.3 now implies that G must be abelian.

□

For any prime p, there are exactly two isomorphically distinct groups, $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$, of order p^2.

Proof.

The result follows from the Fundamental Theorem of Finite Abelian Groups and the fact that for any prime, p, $\mathbb{Z}_p \times \mathbb{Z}_p$ is abelian as is $\mathbb{Z}_{p^2}$ by the above theorem.

□

Example 6.4.

The only groups of order

- 4 are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$;
- 9 are $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$;
- 10,201 are $\mathbb{Z}_{10201}$ and $\mathbb{Z}_{101} \times \mathbb{Z}_{101}$.

But what about groups of order p^3?

Let us consider first groups of order $8 = 2^3$. There are two non-abelian groups of order 8: D_4 and Q_8. This means that we need a little more than Theorem 6.1 to classify groups of order p^3.

Notice that every non-abelian group G of order p^3 must have a centre of order p. This follows since if $|Z(G)| = p^2$, then $G/Z(G)$ has order p and so, by Lemma 6.2, G must be abelian which would be a contradiction.

Now if $Z(G)$ has order p, then $G/Z(G)$ has order p^2 and so is abelian.

Example 6.5.

Both non-abelian groups of order 8 have centres of order 2. The centre of D_4 is $\{e, r_2\}$, while the centre of Q_8 is $\{1, -1\}$. (Recall that $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$).

6.3 Centralisers and Sylow's First Theorem

In Lemma 6.1 we showed that a group acts on its own elements by conjugation (that is, conjugation is a group action). Whenever we have a group action we have orbits and stabilizers; the orbits of this action are what we have called the conjugacy classes of the group, but what about the stabilizers?

Definition 6.3 (Centraliser)**.** Let x be an element from a group G. The *centraliser* of x in G is denoted and defined by

$$cent_G(x) = \{g \in G \,|\, gxg^{-1} = x\} = \{g \in G \,|\, gx = xg\}.$$

So, the centraliser of x in G consists of all of the elements of G that commute with x. Notice that $cent_G(x) = G$ if and only if x is in the centre of G

> **!** Note
>
> Do **NOT** confuse the centre of a group with the centraliser of an element.
>
> If G is abelian, $cent_G(x) = G$ for all $x \in G$. However, for non-abelian group, this only happens when x is in the centre of G. For example, in D_3:
>
> $$\begin{aligned} cent_G(e) &= D_3 \\ cent_G(r_1) &= \{e, r_1, r_2\} = cent_G(r_2) \\ cent_G(s_1) &= \{e, s_1\} \\ cent_G(s_2) &= \{e, s_2\} \\ cent_G(s_3) &= \{e, s_3\} \end{aligned}$$

Lemma 6.4. *Let x be an element from a group G. Then $cent_G(x)$ is a subgroup of G.*

Proof.

We give a direct and indirect proof.

- **Indirect proof:** The $cent_G(x)$ is the stabiliser of x under the action of G on itself by conjugation. By Theorem 3.2, $cent_G(x)$ is therefore a subgroup of G.
- **Direct proof:** we carry out the subgroup checks.
  - Clearly $e \in cent_G(x)$ since $ex = xe$.
  - Let $g, h \in cent_G(x)$. Then

    $$ghx = gxh = xgh$$

    and so $gh \in cent_G(x)$.

– Let $g \in cent_G(x)$. Then $gx = xg$. Post and pre-multiplying by g^{-1} we have:

$$xg^{-1} = g^{-1}gxg^{-1} = g^{-1}xgg^{-1} = g^{-1}x$$

and so $g^{-1} \in cent_G(x)$. This complete the subgroup checks and so $cent_G(x)$ is a group.

□

Example 6.6.

The conjugacy classes in D_3 are $\{e\}$, $\{r_1, r_2\}$ and $\{s_1, s_2, s_3\}$. Notice the following:

$$\begin{aligned} |cent_G(e)| \times |conj_G(e)| &= |D_3| \times |\{e\}| = 6 \\ |cent_G(r_1)| \times |conj_G(r_1)| &= |\{e, r_1, r_2\}| \times |\{r_1, r_2\}| = 6 \\ |cent_G(s_i)| \times |conj_G(s_i)| &= |\{e, s_i\}| \times |\{s_1, s_2, s_3\}| = 6. \end{aligned}$$

This is not a coincidence, merely an application of the Orbit-Stabiliser Theorem (Theorem 3.3) applied to the conjugation action of:

$$|\operatorname{stab}(x)| \times |\operatorname{orb}(x)| = |G|.$$

Under the conjugacy action, $\operatorname{stab}(x) = cent_G(x)$ and $conj_G(x) = \operatorname{orb}(x)$.

We are now in a position to state and prove Sylow's First Theorem.

Theorem 6.2 (Sylow's First Theorem)**.** *Let G be a finite group of order $p^\alpha s$, where p is a prime not dividing s. Then G has a subgroup of order p^β for each integer β such that $0 \leq \beta \leq \alpha$.*

Proof.

We prove this result by induction on the order of G.

Our base case occurs when $|G| = 1$. In this case the result is readily seen to hold.

Next assume that that $|G| = p^\alpha s$ (for a prime p and $\gcd(s, p) = 1$) and the result holds for all groups of order strictly less than $p^\alpha s$. The aim is to get to a point in which we can apply the inductive step. Our key tool is the Class equation Definition 6.2:

$$|G| = |Z(G)| + \sum_{i=t+1}^{r} |C_i|.$$

There are two cases to consider: either p does not divide $|C_i|$ for *some* i or for *any* i between $t+1$ and r, p divides $|C_i|$. We consider the first case first.

- **Case 1:** : Let i be such that p does not divide $|C_i|$ and let $x \in C_i$. By the Orbit-Stabiliser Theorem $|C_i| \times |cent_G(x)| = |G|$. Therefore p^α divides $|cent_G(x)|$ since p^α does not divide $|C_i|$. Notice moreover that since $x \notin \mathbb{Z}(G)$, $cent_G(x) \neq G$ and so $|cent_G(x)| < |G|$. Therefore we may apply the inductive hypothesis to conclude the the result holds for $cent_G(x)$. Since $cent_G(x) < G$, then the result holds in G as well.

- **Case 2:** In this case p divides the order of $\mathbb{Z}(G)$, since p divides $|C_i$ for all i and p divides $|G|$. We may now apply Cauchy's Theorem (Theorem 3.5) to conclude that $\mathbb{Z}(G)$ has a subgroup N of order p. Notice that as $N \leq Z(G)$, then N is a normal subgroup of G ($gng^{-1} = n$ for all $g \in G$ and $n \in N$). Now as G/N has order $p^{\alpha-1}s$ we may therefore apply the induction hypothesis to G/N. Let β be a number between 0 and $\alpha - 2$. By induction G/N has a subgroup of order p^β. Applying the correspondence theorem (Theorem 4.5), there is therefore a subgroup $H \leq G$ such that H/N is a subgroup of G/N of order p^β. Now observe that H must have have order $p^{\beta+1}$ since, if $H/N = \{N, h_2N, \ldots, h_{p^\beta}N\}$, then

  $$H = N \sqcup h_2N \sqcup \ldots \sqcup h_{p^\beta}N$$

  has order $p^{\beta+1}$. Therefore, for all i between 0 and α, G has a subgroup of order p^i

(the trivial subgroup $\{e\}$ of G is a subgroup of order 1.)

□

Definition 6.4 (Sylow p-subgroup)**.** Let G be a finite group of order $p^\alpha s$, where p is a prime not dividing s. A subgroup of G of order p^α is called a *Sylow p-subgroup* of G.

Example 6.7.

We consider some groups we have already encountered:

- $|D_3| = 2 \times 3$. The Sylow-2 subgroups are $\{e, s_i\}$, $i = 1, 2, 3$. The only Sylow-3 subgroup is $\{e, r_1, r_2\}$.
- $|A_4| = 12 = 4 \times 3$. Thus A_4 has Sylow 3-subgroups of order 3 (each generated by a three-cycle) and a Sylow 2-subgroup of order 4 namely $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

The notion of conjugacy can be extended to subsets of a group G, though in practice only subgroups are of importance.

Definition 6.5. Let H be a subgroup of a group G, and $g \in G$. The subset $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is called the *conjugate of H by g*.

We have seen this idea before when we proved Theorem 4.6 using group actions, and needed the fact that if H is a subgroup then gHg^{-1} is a subgroup. The following Lemma tells us even more.

Lemma 6.5. *Let H be a subgroup of a group G and $g \in G$. Then gHg^{-1} is a subgroup of G isomorphic to H.*

Proof.

First we show that gHg^{-1} is a subgroup.

Clearly, $e \in gHg^{-1}$ since $geg^{-1} = e$.

Let $h_1, h_2 \in H$. Then

$$gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1} \in gHg^{-1}.$$

Therefore gHg^{-1} is closed under products.

Lastly let $h \in H$, then

$$(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$$

and so ghg^{-1} is closed under inverses.

The map $\phi : H \to gHg^{-1}$ by $h \mapsto ghg^{-1}$ is an isomorphism.

Clearly ϕ is surjective. To see that is is injective observe that if

$$gh_1g^{-1} = gh_2g^{-1}$$

then, post-multiplying by g and pre-multiplying by g^{-1} we have:

$$h_1 = g^{-1}gh_1g^{-1}g = g^{-1}gh_2g^{-1}g = h_2.$$

Therefore ϕ is a bijection.

To verify that ϕ is a homomorphism, observe

$$\phi(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \phi(h_1)\phi(h_2)$$

as required.

□

There is an immediate connection between conjugacy and normal subgroups; H is a normal subgroup of G if and only if for all $g \in G,\ gH = Hg$, but $gH = Hg \Leftrightarrow gHg^{-1} = H$. It follows that H is normal in G if and only if H has no distinct conjugates in G, that is we only get H. Note that if H is any subgroup of G then if H is normal in G we have that

$gHg^{-1} = H \ \forall g \in G$; if H is not normal in G then $\exists\, x \in G$ such that $xHx^{-1} \neq H$ but xHx^{-1} is still a subgroup of G.

We can now state the remaining Sylow Theorems.

Theorem 6.3 (Sylow's Second Theorem)**.** *Let H_1 and H_2 be Sylow p-subgroups of a finite group G. Then H_1 and H_2 are conjugate.*

That is, there exists $x \in G$ such that $xH_1x^{-1} = H_2$ and vice versa.

Theorem 6.4 (Sylow's Third Theorem)**.** *The number of Sylow p-subgroups of a finite group G is congruent to 1 modulo p and divides $|G|$.*

We now consider an application.

Let G be a group of order $3 \times 5 = 15$. By Cauchy's Theorem G has at least one subgroup of order 3 and at least one of order 5.

Let n_3 be the number of subgroups of order 3. By Sylow's Third Theorem $n_3 \equiv 1 \pmod 3$ and divides the order of G which is 15. Therefore n_3 must be 1 since $5 \equiv 2 \pmod 3$. Therefore G has a unique Sylow 3-subgroup, N_1. By Sylow's Second Theorem, N_1 must be normal in G since it is conjugate only to itself.

In a similar way G has a normal subgroup N_2 of order 5. Notice that $N_1 \cap N_2 = \{e\}$ since every non-trivial element of N_1 has order 3 and every non-trivial element of order N_2 has order 5.

Let a be a non-trivial element of N_1 and b be a non-trivial element of N_2 and consider the product ab. Now ab has order $1, 3, 5$ or 15.

If the order of $ab = 1$, then $ab = e$ and so $b = a^{-1}$ which contradicts the fact that $N_1 \cap N_2 = \{e\}$.

If the order of $ab = 3$, then $\langle ab \rangle$ must be N_1 (since H_1 is the only Sylow 3-subgroup of G). This means that $ab = n \in N_1$ and so $b = a^{-1}n \in N_1$ which contradicts the fact that $N_1 \cap N_2 = \{e\}$.

If the order of $ab = 5$, then as in the previous case $ab \in N_2$ and $a = mb^{-1}$ for some $m \in N_2$ and so $a \in N_2$ yielding a contradiction.

We must therefore conclude that ab has order 15 and so G is a cyclic group.

Note that the above does not generalise to groups of order pq, for distinct primes p and q since there are non-abelian groups of order pq (e.g . D_p for every prime p is a non-abelian group of order $2p$). In the case where a group G of order p, q has a unique Sylow p-subgroup and a unique Sylow q-subgroup, the argument above does generalise.

Let us suppose that p and q are distinct primes with $q < p$ and consider a group G or order pq.

There is always a unique Sylow p subgroup, since n_p, the number of Sylow p subgroups must divide pq and be congruent to 1 modulo p i.e. n_p divides q and is congruent to 1 modulo p. As an example, consider D_3. This has order 2×3 and a unique (and so normal) Sylow 3-subgroup $\{e, r_1, r_2\}$.

What about n_q the number of Sylow q-subgroups of G? We know that $n_q \equiv 1 \pmod{q}$ and n_q divides pq. This means that n_q is either 1 or p. If p is not congruent to 1 modulo q, then $n_q = 1$ and G is cyclic.

If on the other hand $p \equiv 1 \pmod{q}$, then n_q might be equal to p. For example if we consider the D_p, here $q = 2$, then D_p has p Sylow 2-subgroups: $\{e, s_i\}$, $i = 1, 2, \ldots, p$.

We can summarise the above as follows:

Let p and q be distinct primes with $q < p$ and $p \not\equiv 1 \pmod{q}$. Then a group G of order pq is cyclic.

Applying this to groups of order $n = pq$ for small n we have:

n	q	p	
15	3	5	cyclic only
21	3	7	possibly non-cyclic
33	3	11	cyclic only
35	5	7	cyclic only
55	5	11	possibly non-cyclic
77	7	11	cyclic only
91	7	13	cyclic only
119	7	17	cyclic only

6.4 Problem Sheet 6

Covers Chapter 6.

Question 6.1

Determine whether the converse of Lagrange's Theorem is true for all finite p-groups. Provide either a proof or a counter-example to justify your assertion.

Show Solution 6.1 on P191

Question 6.2

Show that every group of order 63 has a normal subgroup of order 7 and at least one subgroup of order 21.

Show Solution 6.2 on P191

Question 6.3

Use the Sylow Theorems to show that every group of order 980 has a normal subgroup of order 49, and subgroups of orders 245 and 98.

Show Solution 6.3 on P192

Question 6.4

Let G be a group of order pq, where p and q are primes, $p < q$, and p does not divide $q - 1$.

(a) List the possible orders of such groups up to and including 40.

(b) Prove that G contains normal subgroups of orders p and q.

(c) Let $H = \langle x \rangle$ and $K = \langle y \rangle$ be normal subgroups of orders p and q respectively. Show that $x(yx^{-1}y^{-1}) \in H$ and $(xyx^{-1})y^{-1} \in K$. [Hint: the brackets are supposed to be helpful...]

(d) Deduce that $xy = yx$. [Hint: what is $H \cap K$?]

(e) Determine the order of the element xy in G and deduce that G is cyclic.

Show Solution 6.4 on P192

Appendix A

All Solutions

A.1 Chapter 1 solutions

Solution R.1

Define $*$ ***on*** $\mathbb{R}\backslash\{0\}$ ***by*** $a * b = |a|\, b$ ***(so, for example*** $2 * 3 = 6, -2 * 3 = 6, 2 * (-3) = -6$ ***etc.).***

i. Show that $*$ ***is an associative binary operation on*** $\mathbb{R}\backslash\{0\}$***.***

ii. Show that there is an element $e \in \mathbb{R}\backslash\{0\}$ ***such that*** $e * x = x,\ \forall\, x \in \mathbb{R}\backslash\{0\}$***.***

iii. Show that $\forall\, x \in \mathbb{R}\backslash\{0\}, \exists\, x^{-1} \in \mathbb{R}\backslash\{0\}$ ***such that*** $x * x^{-1} = e$***.***

iv. Is $(\mathbb{R}\backslash\{0\}, *)$ ***a group?***

i. We have that, for all $x, y, z \in \mathbb{R}\backslash\{0\}$,

$$(x * y) * z = (|\, x \,|\, y) * z = |\,|\, x \,|\, y \,|z = |\, xy \,|z$$

and

$$x * (y * z) = x * (|\, y \,|\, z) = |\, x \,|(|\, y \,|\, z) = |\, xy \,|z.$$

Hence $*$ is associative on $\mathbb{R}\backslash\{0\}$.

ii. For all $x \in \mathbb{R}\backslash\{0\}$ we have that $1 * x = |\, 1 \,|x = x$, so $e = 1$. Note also, however, that $e = -1$ also works.

iii. Note that $x * \dfrac{1}{|x|} = |x| \dfrac{1}{|x|} = 1$, so $x^{-1} = \dfrac{1}{|x|}$.

iv. No, it is not. There are a number of ways of deciding this.

a. In part ii. we noted that there were two values of e that would satisfy the relationship $e * x = x$ for all $x \in \mathbb{R}\backslash\{0\}$, namely 1 and -1. So both of these appear to have the property of an identity, but we know that in any group the identity is unique.

b. We also know that the identity in a group must commute with every element of the group, that is it must be 'two-sided' in the sense that it must satisfy $e * x = x * e = x$. This is not the case here; for example, try $x = -3$ (with $e = 1$ or -1) and note that $e * x \neq x * e$.

c. Similarly, we can also see that the 'inverse' found in part iii. is not 'two-sided'.

Return to Question R.1 on P31

Solution R.2

If H is a subgroup of a finite group G then the* right coset *of H by g is denoted and defined by

$$Hg = \{hg \,|\, h \in H\}.$$

Prove Lagrange's Theorem using right cosets (the proof using left cosets was given in the second year Abstract Algebra module). In other words, show that every right coset, Hg, of H is the same size as H, that two right cosets of H are either disjoint or equal, and that every element of G is in a right coset of H. Finally deduce that the order of H divides the order of G.

Since H is finite (say with order m) we may write $Hg = \{h_1 g, h_2 g, \ldots, h_m g\}$. It looks as if this set has size m (as it contains m symbols) but remember that $\{1, 1, 2\}$ is a set of size 2 not 3. So to show that Hg really does have size m we need to show that all the symbols represent distinct group elements. As is often the case with pure mathematics, once we have worked out what we need to do actually doing it is

straightforward.

$$h_i g = h_j g \Rightarrow h_i = h_j \text{ (by cancellation) so } |Hg| = m = |H|.$$

To prove that two right cosets are either identical or disjoint we show that if they have an element in common then they are identical. Suppose $Hg_1 \cap Hg_2 \neq \emptyset$ and let $x \in Hg_1 \cap Hg_2$. Then $\exists\, h_1, h_2 \in H$ such that $h_1 g_1 = x$ and $h_2 g_2 = x$. It follows that $g_1 = h_1^{-1} h_2 g_2$ (we will use this later). Let z be any element of Hg_1. We will show that $z \in Hg_2$, from which it will follow that $Hg_1 \subseteq Hg_2$. Let's pause to think how we can do this - the fact that $z \in Hg_1$ means that z can be written as an element of H times g_1. To show that $z \in Hg_2$ we need to write z as an element of H times g_2. We will use the facts that $g_1 = h_1^{-1} h_2 g_2$ and that H is a subgroup so any product of elements of H is another element of H. Here goes... $z \in Hg_1$, so $\exists h \in H$ such that $z = hg_1$. But $g_1 = h_1^{-1} h_2 g_2$, so $z = (hh_1^{-1} h_2) g_2 \in Hg_2$, because $hh_1^{-1} h_2 \in H$. So $Hg_1 \subseteq Hg_2$ and a similar argument shows that $Hg_2 \subseteq Hg_1$. It follows that $Hg_1 = Hg_2$ as required. Finally we show that every element is in a right coset. This is the easiest part of all because H contains the identity element $e \in G$ so $\forall\, g \in G,\ eg = g$ and hence $g \in Hg$. Putting these facts together we have that the right cosets of H partition the elements of G into disjoint subsets which are all the same size as H. It follows that the number of elements in G must be a multiple of the number of elements in H (where this multiple is the number of right cosets). In other words the order of any subgroup must divide the order of the group (Lagrange's Theorem).

Return to Question R.2 on P31

Solution R.3

Let G be a group and H the subset of G consisting of the identity e and all elements of G of order 2, so $H = \{h \in G | h^2 = e\}$. Show that:

i. if G is abelian, then H is a subgroup of G,

ii. if G is non-abelian, then H is not necessarily a subgroup of G.

Here we are being asked to prove that something is true for abelian groups but false for non-abelian ones. The first thing to do is make sure we know what the statement is! Let's look at $G = \mathbb{Z}_4$, we have $0 + 0 = 0, 1 + 1 = 2, 2 + 2 = 0$ and $3 + 3 = 2$, so $H = \{0, 2\}$ and sure enough this forms a subgroup of $\mathbb{Z}_4$. Now let's look at D_3, using the Cayley table for D_3 in the list of Cayley tables just after Example 1.2 we have $H = \{0, 3, 4, 5\}$. This is clearly not a subgroup of D_3, for one thing 4 does not divide 6 (which would upset Lagrange) or, if you prefer, $3 * 4 = 1$ so H is not closed. It's important to use examples in this way even though we cannot use examples to prove statement i.; they are important in helping us understand what the statement means. Notice that we have answered part ii.! For this we only require a single counter-example and we've found one in D_3.

Let's try to prove i.. We need one of our subgroup checking lemmas. Because we are not told that G is finite we need to use Lemma 2.6 from the Abstract Algebra module. Firstly, since $e^2 = e$ we have $e \in H$ so H is non-empty. We now need to show that H is closed, that is if $h_1, h_2 \in H$ then $h_1 * h_2 \in H$. If $h_1, h_2 \in H$, then $h_1^2 = h_2^2 = e$ (and we need to show that $(h_1 h_2)^2 = e$). Once we know what we are trying to show, and what we must use, we can write this concisely as follows. $h_1, h_2 \in H \Rightarrow (h_1 h_2)^2 = h_1 h_2 h_1 h_2 = h_1^2 h_2^2 = e * e = e$ so $h_1 h_2 \in H$ as required. If H were finite then we would be done but because H may be infinite we need to show that the inverse of every element in H is also in H. This is easy once we notice that $h^2 = e \Rightarrow h^{-1} = h$. So the inverse of every element in H is also in H!

Return to Question R.3 on P31

Solution R.4

Show that if H and K are subgroups of an abelian group G, then

$$HK = \{hk \,|\, h \in H, k \in K\}$$

is a subgroup of G. Is this true for non-abelian groups?

Again, we do not know whether HK is a finite or infinite set, so we need to prove closure and then show that every element in the set also has its inverse in the set. In addition, it is obvious that both H and$K$, and hence HK, are non-empty. As usual, to prove closure we take two 'typical' elements of our subset and demonstrate that when they are combined under the binary operation of the group the resulting product remains in the subset. In order to do this it is important to know how membership of the subset is defined. Here we know that every element of HK is of the form hk, where $h \in H$ and $k \in K$. It therefore follows that if $a \in HK$ there must be an $h \in H$ and a $k \in K$ such that $a = hk$. Note, also, that as the group is abelian $hk = kh$. We then proceed as follows:

Let $a, b \in HK$, so $\exists\, h_1, h_2 \in H$ and $\exists\, k_1, k_2 \in K$ such that $a = h_1k_1$ and $b = h_2k_2$. Then,

$$ab = h_1k_1h_2k_2 = h_1h_2k_1k_2 \in HK$$

since

$$h_1h_2 \in H, k_1k_2 \in K.$$

Note that the second step is valid since the group is abelian and the final step is valid since H and K are both groups so must be closed. To show that the subset HK is closed under inverses we need to remember an important property of inverses, namely that $(xy)^{-1} = y^{-1}x^{-1}$. Now,

$$a^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h_1^{-1}k_1^{-1} \in HK$$

since

$$h^{-1} \in H, k^{-1} \in K.$$

Note, again, that the second step is valid since the group is abelian and the final step is valid since H and K are both groups so must be closed under inverses. This statement is not true for non-abelian groups. For example $H = \{e, s_1\}$ and $K = \{e, s_2\}$ are subgroups of D_3, but $HK = \{e, s_1, s_2, r_1\}$ is not a subgroup of D_3.

Return to Question R.4 on P31

Solution R.5

Let $(G_1, \times)$ ***and*** $(G_2, \circ)$ ***be groups and*** $\theta : G_1 \to G_2$ ***an isomorphism. Prove that*** H ***is a subgroup of*** G_1 ***if and only if*** $\theta(H) = \{\theta(h) \,|\, h \in H\}$ ***is a subgroup of*** G_2***.***

The usual procedures and caveats for proving 'subgroupness' apply here. It is also important to note that different binary operations are at work, depending on the group, and that this is an 'if and only if' statement so both forward and backward implications need to be considered. It should also be obvious that we will need to use the definition of an isomorphism, that is a bijective mapping from G_1 to G_2 such that for all $a, b \in G_1$, $\theta(a \times b) = \theta(a) \circ \theta(b)$. Taking the forward implication first, the proof then proceeds as follows (bearing in mind that we are trying to show that $\theta(H)$ is a subgroup of G_2):

Let H be a subgroup of G_1. Clearly both H and $\theta(H)$ are non-empty. Let h_1', h_2' be any two elements of θH. Then $\exists\, h_1, h_2 \in H$ such that $\theta(h_1) = h_1'$ and $\theta(h_2) = h_2'$. Hence

$$h_1' \circ h_2' = \theta(h_1) \circ \theta(h_2) = \theta(h_1 \times h_2) \in \theta(H)$$

since

$$h_1 \times h_2 \in H.$$

The second step above uses the definition of an isomorphism and the last step is justified since we know that H is a group and therefore closed.

Now, for all $h' \in \theta(H)$ there exists $h \in H$ such that $\theta(h) = h'$. But

$$(h')^{-1} = (\theta(h))^{-1} = \theta(h^{-1}) \in \theta(H)$$

since

$$h^{-1} \in H.$$

For the backward implication (converse), that is if $\theta(H)$ is a subgroup of G_2 then H is a subgroup of G_1, we either construct a similar argument to that above or (much better) use the fact that $\theta^{-1} : G_2 \to G_1$ is an isomorphism from G_2 to G_1 and so the result follows immediately.

Return to Question R.5 on P32

Solution R.6

Show that if G ***is an abelian group then***

$$\{g^2 \,|\, g \in G\}$$

is a subgroup of G***, but this is not true for groups in general.***

You should be used to the process by now! Let $H = \{g^2 \,|\, g \in G\}$. Clearly H is non-empty by definition. Let $a, b \in H$. Then there exist $g_1, g_2 \in G$ such that $a = g_1^2$ and $b = g_2^2$. Then,

$$ab = g_1^2 g_2^2 = g_1 g_1 g_2 g_2 = g_1 g_2 g_1 g_2 = (g_1 g_2)^2 \in H$$

since

$$g_1 g_2 \in G.$$

Further,

$$a^{-1} = (g_1^2)^{-1} = g_1^{-2} = (g_1^{-1})^2 \in H$$

since

$$g_1^{-1} \in G.$$

Hence, $H = \{g^2 \,|\, g \in G\}$ is a subgroup of G.

To show that this is not the case for groups in general we need to find a non-abelian group to give us a counter example, but this isn't obvious. We would usually look to the dihedral groups to provide such a counter example, but, in fact, the given statement is true for D_n for all n. (Can you see why? If not, ask!). In fact we need to go to A_4, a group of order 12, to find the first counter example. Why this group provides a counter example will become clearer once we have completed the chapter on permutations, but the reason is as follows. A_4 consists of the identity, 8 permutations of the form $(* \ * \ *)$ and 3 permutations of the form $(* \ *)(* \ *)$ (12 elements in total). Since squaring the identity or the permutations of the form $(* \ *)(* \ *)$ gives the identity and squaring the 3-cycles just gives the 3-cycles (all eight of them), then the subset $H = \{g^2 \,|\, g \in A_4\}$ contains nine elements. This cannot form a subgroup of A_4 as that would violate Lagrange's Theorem.

Return to Question R.6 on P32

Solution R.7

We know that every proper subgroup of a cyclic group is itself cyclic. State the converse and give a counter example to demonstrate that the converse is false.

The converse of the statement is "If a group G is such that every proper subgroup is cyclic, then G is cyclic". This statement is false since any non-cyclic group of order pq where p and q are prime (e.g D_{pq}) has only proper subgroups of prime order which

are necessarily cyclic (as is $\{e\}$).

Return to Question R.7 on P32

Solution R.8

In each of the following cases, find the order of the given element in the direct product:

i. $(3,7)$ ***in*** $\mathbb{Z}_9 \times \mathbb{Z}_{14}$***;***

ii. $(8,11)$ ***in*** $\mathbb{Z}_{10} \times \mathbb{Z}_{15}$***;***

iii. $(3,7,12)$ ***in*** $\mathbb{Z}_4 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$***.***

First, recall that to find the order of (a,b) in $G_1 \times G_2$, where $a \in G_1$ and $b \in G_2$, we take the lowest common multiple of the orders of a in G_1 and b in G_2. Remember, also, that an element a in $\mathbb{Z}_m$ has order equal to $m/\gcd(a,m)$.

i. $(3,7)$ in $\mathbb{Z}_9 \times \mathbb{Z}_{14}$. Obviously 3 has order 3 in $\mathbb{Z}_9$ and 7 has order 2 in $\mathbb{Z}_{14}$. So the order of $(3,7)$ in $\mathbb{Z}_9 \times \mathbb{Z}_{14}$ is lcm$(3,2) = 6$.

ii. $(8,11)$ in $\mathbb{Z}_{10} \times \mathbb{Z}_{15}$: The order of 8 in $\mathbb{Z}_{10}$ is $10/\gcd(8,10) = 5$. Similarly the order of 11 in $\mathbb{Z}_{15} = 15$. So, the order of $(8,11)$ in $\mathbb{Z}_{10} \times \mathbb{Z}_{15}$ is lcm$(5,15) = 15$.

iii. $(3,7,12)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$. The order of 3 in $\mathbb{Z}_4$ is $4/\gcd(3,4) = 4$. Similarly the order of 7 in $\mathbb{Z}_{10} = 10$, and the order of 12 in $\mathbb{Z}_{15} = 5$. So, the order of $(3,7,12)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$ is lcm$(4,10,5) = 20$.

Return to Question R.8 on P32

Solution R.9

i. Write down all of the generators of

a. $\mathbb{Z}_{14}$***,***

b. $\mathbb{Z}_{15}$***.***

ii. Classify, according to the Fundamental Theorem of Finite Abelian Groups, all of the abelian groups of orders

a. 54,

b. 600.

iii. In part ii.a. above, state which of the groups of order 54 is cyclic and which is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_9$.

i. Recall that the generators of $\mathbb{Z}_m$ are those elements that are relatively prime to m. So the generators of $\mathbb{Z}_{14}$ are 1, 3, 5, 9, 11, 13 and the generators of $\mathbb{Z}_{15}$ are 1, 2, 4, 7, 8, 11, 13, 14.

ii. We state, first, the Theorem: >Every finitely abelian group is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}}$$

where the p_i are primes, not necessarily distinct (and r may be 0).

a. Now, $54 = 2 \times 3 \times 3 \times 3$, which is its prime decomposition. Hence the possible groups, in accordance with the theorem, are $\mathbb{Z}_2 \times \mathbb{Z}_{27}$, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$, and $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

b. $600 = 2^3 \times 3 \times 5^2$. So the isomorphically distinct groups are $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$, $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$.

iii. Remember that $\mathbb{Z}_r$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $r = mn$ and m and n are relatively prime. So, for example, $\mathbb{Z}_{12}$ is not isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$ as 6 and 2 are not relatively prime. If we are dealing with a direct product of more than two cyclic groups then the same principle applies except that the orders have to be pairwise relatively prime. Now we know that $\mathbb{Z}_n$ is cyclic for all n, so $\mathbb{Z}_{54}$ must be cyclic. This is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{27}$ since 2 and 27 are relatively prime, so $\mathbb{Z}_2 \times \mathbb{Z}_{27}$ must be cyclic. The group that is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_9$ is $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$, since $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ as 2 and 3 are relatively prime.

Return to Question R.9 on P33

Solution 1.1

Let R be a relation on a non-empty set, S

- ***a. Define a relation on $\mathbb{Z}^+$ by, for $x, y \in \mathbb{Z}^+$, xRy if and only if x and y have the same number of digits in the usual base 10 notation. Show that this is an equivalence relation.***
- ***b. Find the equivalence class containing 37.***

Recall that, for a relation to be an equivalence relation, we require that it is reflexive, symmetric and transitive. These terms are defined as follows: A relation, R, on a non-empty set S is said to be

i. **reflexive:** if aRa for all $a \in S$,

ii. **symmetric:** if, whenever aRb, then bRa,

iii. **transitive** if, whenever aRb and bRc, then aRc.

Applying the definitions to our relation:

i. trivial, since an integer has the same number of digits as itself so xRx;

ii. again, it is obvious that if x has the same number of digits as y then y has the same number of digits as x, so if xRy then yRx;

iii. it is clear that if $w \in \mathbb{Z}^+$ and xRw and wRy, then xRy.

Thus R is an equivalence relation on the set S. Obviously, all of the members of any given equivalence class must have the same number of digits. thus the class containing 37 will be $[37] = \{10, 11, \ldots, 37, \ldots, 99\}$.

Return to Question 1.1 on P33

Solution 1.2

Define a relation on $\mathbb{R}$ by, for $a, b \in \mathbb{R}$, aRb if and only if $|a| = |b|$. Is this an equivalence relation? If so, how does it partition the set?

Applying the definitions to our relation:

i. aRa since, $\forall a \in \mathbb{R}$, $|a| = |a|$.

ii. If aRb then, by definition, $|a| = |b|$. It then follows, since $|b| = |a|$, that bRa.

iii. We know, for any real numbers x, y, z that if $x = y$ and $y = z$, then $x = z$. Now, if aRb and bRc then $|a| = |b|$ and $|b| = |c|$ and hence it follows that $|a| = |c|$ and so aRc.

Thus R is an equivalence relation on the real numbers. The relation partitions $\mathbb{R}$ as follows:

$$[0] = \{0\} \qquad [a] = \{a, -a\} \quad \forall a \in \mathbb{R}.$$

Return to Question 1.2 on P34

Solution 1.3

Define a relation that partitions the plane into the origin and all circles centred at the origin with radius $r \in \mathbb{R}$. ***Prove that this is an equivalence relation.***

Recall that a circle centred at the origin is the set of all points of the plane that are at a given distance from the origin. In Cartesian coordinates, a point (x_1, y_1) has distance $\sqrt{x_1^2 + y_1^2}$ from the origin. It follows that if a point (x_2, y_2) lies on the same circle then $\sqrt{x_1^2 + y_1^2} = \sqrt{x_2^2 + y_2^2}$. Since distances are always positive we thus have that $x_1^2 + y_1^2 = x_2^2 + y_2^2$. This allows us to define the relation that partitions the plane as described:

$$(x_1, y_1)R(x_2, y_2) \quad \Leftrightarrow \quad x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

We now need to show that this is an equivalence relation.

i. Clearly $x_1^2 + y_1^2 = x_1^2 + y_1^2$, hence $(x_1, y_1)R(x_1, y_1)$ and so the relation is reflexive.

ii. Equally clearly, if $x_1^2 + y_1^2 = x_2^2 + y_2^2$ then $x_2^2 + y_2^2 = x_1^2 + y_1^2$, hence if $(x_1, y_1)R(x_2, y_2)$, then $(x_2, y_2)R(x_1, y_1)$, so the relation is symmetric.

iii. If $(x_1, y_1)R(x_2, y_2)$ and $(x_2, y_2)R(x_3, y_3)$ then it follows that $x_1^2 + y_1^2 = x_2^2 + y_2^2$

and $x_2^2 + y_2^2 = x_3^2 + y_3^2$. Hence, $x_1^2 + y_1^2 = x_3^2 + y_3^2$ and so $(x_1, y_1)R(x_3, y_3)$, demonstrating that the relation is transitive.

Thus we have demonstrated that the relation, as defined, is an equivalence relation.

Return to Question 1.3 on P34

Solution 1.4

In the group

$$\langle A, B, C \mid A^7 = B^3 = C^2 = 1, BA = A^3B, CA = AC, CB = B^2C \rangle$$

express each of the following in the form $A^r B^s C^t$***:***

i. $(BC)^2$***;***
ii. B^2A^3***;***
iii. C^3B^{-2}***;***
iv. $(AB)^3$***;***
v. $(ABC)^{-1}$***.***

i. Here we use the fourth condition, namely $CB = B^2C$, so

$$(BC)^2 = BCBC = B(CB)C = B(B^2C)C = B^3C^2.$$

ii. First, we repeatedly apply the second condition, $BA = A^3B$, that is

$$\begin{aligned} B^2A^3 &= B(BA)AA = B(A^3B)AA = BA^3(BA)A \\ &= BA^3(A^3B)A = BA^6(BA) = BA^9B \end{aligned}$$

and then we use $A^7 = 1$ so

$$BA^9B = BA^2B = (BA)AB = A^3(BA)B = A^3(A^3B)B = A^6B^2.$$

iii. First use the fact that $C^2 = 1$, so $C^3B^{-2} = CB^{-2}$. Now, $B^3 = 1$, so $BB^2 = 1$

and hence $B^2 = B^{-1}$ or $B^{-2} = B$. Then,

$$C^3B^{-2} = CB^{-2} = CB = B^2C.$$

iv. $(AB)^3 = ABABAB = A(BA)(BA)B$. We now use $BA = A^3B$ on each of the bracketed expressions,

$$A(BA)(BA)B = A(A^3B)(A^3B)B = A^4BA^3B^2.$$

Now we use the same relation three times to 'hop' the A over the B as follows

$$A^4BA^3B^2 = A^4(BA^3)B^2 = A^4(A^9B)B^2 = A^{13}B^3 = A^6$$

as $A^7 = 1$ and $B^3 = 1$.

v. Note that $A^7 = 1 \Rightarrow A^6 = A^{-1}$; $B^3 = 1 \Rightarrow B^2 = B^{-1}$; $C^2 = 1 \Rightarrow C = C^{-1}$. So $(ABC)^{-1} = C^{-1}B^{-1}A^{-1} = CB^2A^6$. Now use the relation $CB = B^2C$ twice to 'hop' the B over to the front of the C, that is $CB^2A^6 = B^4CA^6 = BCA^6$ since $B^3 = 1$. Next use $CA = AC$ six times to 'hop' the A over the C,

$$BCA^6 = BA^6C.$$

Finally we use $BA = A^3B$ six times to 'hop' the A over the B, that is

$$BA^6C = A^{18}BC = A^4BC$$

since $A^7 = 1$. And so we have that $(ABC)^{-1} = A^4BC$. You may, however, have approached this problem from a different angle. Suppose we start by 'hopping' the A over the B. We can do this in two steps using $BA = A^3B$ as

follows:

$$CB^2A^6 = CBBA^6 = CBA^{18}B = CBA^4B$$

as $A^7 = 1$. We now repeat that step four more times

$$CBA^4B = CA^{12}BB = CA^5B^2$$

since $A^7 = 1$. Now apply $CA = AC$ five times to 'hop' the A over the C as follows $CA^5B^2 = A^5CB^2$. Finally, we use $CB = B^2C$ to obtain

$$A^5CB^2 = A^5B^4C = A^5BC$$

since $B^3 = 1$. And so we have that $(ABC)^{-1} = A^5BC$. What has gone wrong? Well, actually, nothing at all has gone wrong! Both answers are perfectly valid. So what is going on?

Return to Question 1.4 on P34

Solution 1.5

Let $G = \langle a, b, c \,|\, a^4 = b^3 = 1, ab = ba, ac = ca, bc = cb \rangle$***. Classify*** G ***according to the Fundamental Theorem.***

Note that the generators commute with each other pairwise, so we know that the group is abelian. So every product can be reduced to the form $a^ib^jc^k$ where $0 \leq i < 4$, $0 \leq j < 3$ and $k \in \mathbb{Z}$ (no constraint on k). Hence, the group is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}$ with the isomorphism given by $a^ib^jc^k \mapsto (i, j, k)$.

Return to Question 1.5 on P35

Solution 1.6

If $G = \langle a, b \mid ab = ba, a^4 = b^3 = 1 \rangle$ ***and*** H ***is the cyclic subgroup generated by*** b***, classify*** G ***according to the Fundamental Theorem, and find the left and right cosets of*** H ***in*** G***.***

It should be obvious that $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$. Note that this group is abelian and so the distinct right and left cosets will coincide. We have:

$$\begin{aligned} H &= \{0, b, 2b\} \\ a + H = H + a &= \{a, a + b, a + 2b\} \\ 2a + H = H + 2a &= \{2a, 2a + b, 2a + 2b\} \\ 3a + H = H + 3a &= \{3a, 3a + b, 3a + 2b\}. \end{aligned}$$

Return to Question 1.6 on P35

Solution 1.7

In the dihedral group $D_5 = \langle a, b \mid a^5 = 1, b^2 = 1, ab = ba^{-1} \rangle$***, simplify:***

i. $a^7b^3a^{-2}baba^3ba^2a^7b^2a$***;***

ii. $a^{13}b^5a^2b^{-7}a^2ba$***.***

i. First, using $a^5 = 1$ and $b^2 = 1$ we have

$$a^7b^3a^{-2}baba^3ba^2a^7b^2a = a^2ba^3baba^3ba^4b^2a.$$

Now bracket together all the terms ba and then use $ab = ba^{-1} \Rightarrow ba = aba^2$.

Hence

$$\begin{aligned}
&a^2ba^3baba^3ba^4b^2a \\
&= a^2(ba)a^2(ba)(ba)a^2(ba)a^3b^2a \\
&= a^2(aba^2)a^2(aba^2)(aba^2)a^2(aba^2)a^4 \\
&= a^3ba^5ba^3ba^5ba^6 \\
&= a^3b^2a^3b^2a \\
&= a^7 \\
&= a^2.
\end{aligned}$$

ii. Note that, $a^5 = 1$ and as $b^2 = 1$, then $b = b^{-1}$ and so $b^n = b^{-n}$. Then

$$\begin{aligned}
&a^{13}b^5a^2b^{-7}a^2ba \\
&= a^3ba^2ba^2ba \\
&= a^2(ab)a(ab)a(ab)a \\
&= a^2(ba^{-1})a(ba^{-1})a(ba^{-1})a \\
&= a^2bbb \\
&= a^2b.
\end{aligned}$$

Return to Question 1.7 on P35

Solution 1.8

In $(\mathbb{Q},+)$***, describe the elements of*** $\langle\frac{1}{2}\rangle$ ***and*** $\langle\frac{1}{2},\frac{1}{3}\rangle$***. Show that*** $(\mathbb{Q},+)$ ***is not finitely generated.***

In $(\mathbb{Q},+)$, $\langle\frac{1}{2}\rangle$ consists of all integer multiples of $\frac{1}{2}$, so $\langle\frac{1}{2}\rangle = \{\frac{n}{2} \mid n \in \mathbb{Z}\}$. For $\langle\frac{1}{2},\frac{1}{3}\rangle$ we now have two generators, so the subgroup consists of all sums of multiples of $\frac{1}{2}$ and $\frac{1}{3}$. Hence $\langle\frac{1}{2},\frac{1}{3}\rangle = \{\frac{m}{2}+\frac{n}{3} \mid m,n \in \mathbb{Z}\} = \{\frac{n}{6} \mid n \in \mathbb{Z}\}$. The final equality follows

because gcd(2,3)=1 and hence every integer can be expressed in the form $3m + 2n$ (why?). Given a finite set S in $(\mathbb{Q}, +)$, $\langle S \rangle$ will only contain rationals which can be expressed with denominator equal to the lowest common multiple of the denominators of the elements of S. So any fraction whose denominator is not of this form is not in $\langle S \rangle$ and hence $\mathbb{Q}$ has no finite generating set. For an explicit example take a prime p greater than all the denominators in S, then $\frac{1}{p} \notin \langle S \rangle$.

Return to Question 1.8 on P36

A.2 Chapter 2 solutions

Solution 2.1

Which of the following permutations is different from the other two:

$$(1\ 4\ 2\ 8)(3\ 7\ 5), \quad (1\ 8\ 2\ 4)(5\ 7\ 3), \quad (7\ 5\ 3)(2\ 8\ 1\ 4).$$

Note that disjoint cycles commute and cycles that have the same cyclic structure are the same as each other (e.g $(1\ 2\ 3\ 4) = (3\ 4\ 1\ 2)$). Hence, using the above, we can see that $(1\ 4\ 2\ 8)(3\ 7\ 5) = (7\ 5\ 3)(2\ 8\ 1\ 4)$, but the middle one is different.

Return to Question 2.1 on P52

Solution 2.2

Write down all of the permutations in S_5 with each of the following cycle structures:

i. $(* *)$***;***

ii. $(* * * *)$***;***

iii. $(* *)(* *)$***.***

i.

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

ii.

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

iii.

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

Return to Question 2.2 on P52

Solution 2.3

Write down all of the cycle structures in S_6 together with the number of each. [Do not attempt to list the permutations themselves!]

$I \quad 1$

$(* *) \quad \dfrac{6 \times 5}{2} = 15$

$(* * *) \quad \dfrac{6 \times 5 \times 4}{3} = 40$

$(* * * *) \quad \dfrac{6 \times 5 \times 4 \times 3}{4} = 90$

$(* * * * *) \quad \dfrac{6 \times 5 \times 4 \times 3 \times 2}{5} = 144$

$(* * * * * *) \quad \dfrac{6!}{6} = 120$

$(* *)(* *) \quad \left[\left(\dfrac{6 \times 5}{2}\right) \times \left(\dfrac{4 \times 3}{2}\right)\right] /2 = \dfrac{15 \times 6}{2} = 45$

$(* *)(* * *) \quad \left(\dfrac{6 \times 5}{2}\right) \times \left(\dfrac{4 \times 3 \times 2}{3}\right) = 120$

$(* *)(* * * *) \quad \left(\dfrac{6 \times 5}{2}\right) \times \dfrac{4!}{4} = 90$

$(* *)(* *)(* *) \quad \left[\left(\dfrac{6 \times 5}{2}\right) \times \left(\dfrac{4 \times 3}{2}\right) \times \left(\dfrac{2 \times 1}{2}\right)\right] /3! = 15$

$(* * *)(* * *) \quad \left[\left(\dfrac{6 \times 5 \times 4}{3}\right) \times \left(\dfrac{3!}{3}\right)\right] /2 = 40$

Note that $|S_6| = 720$ and the above numbers sum to 720. For $(* * *)(* * *)$ there are $\frac{6\times5\times4}{3}$ choices for the first 3-cycle, which leaves $\frac{3\times2\times1}{3} = 2$ choices for the second, so there are $\frac{6\times5\times4}{3} \times \frac{3\times2\times1}{3}$ possible products. However, this counts each twice (for example, $(1\ 2\ 3)(4\ 5\ 6) = (4\ 5\ 6)(1\ 2\ 3)$). When counting $(* *)(* * *)$ there is no need for this final adjustment as there is no double counting!

Return to Question 2.3 on P52

Solution 2.4

Write down the elements of A_4.

$$A_4 = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4),$$
$$(1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}.$$

Return to Question 2.4 on P53

Solution 2.5

Let $a = (2\ 5\ 3)(4\ 6)$ ***and*** $b = (1\ 2\ 6)$. ***Calculate:***

i. ab***;***
ii. ba***;***
iii. $(ab)^{-1}$***;***
iv. a^{-1}***;***
v. b^{-1}***;***
vi. $b^{-1}a^{-1}$***.***

We have:

i. $ab = (2\ 5\ 3)(4\ 6)(1\ 2\ 6) = (1\ 5\ 3\ 2\ 4\ 6)$;
ii. $ba = (1\ 2\ 6)(2\ 5\ 3)(4\ 6) = (1\ 2\ 5\ 3\ 6\ 4)$;
iii. $(ab)^{-1} = (1\ 5\ 3\ 2\ 4\ 6)^{-1} = (1\ 6\ 4\ 2\ 3\ 5)$;
iv. $a^{-1} = (4\ 6)(2\ 3\ 5)$
v. $b^{-1} = (1\ 6\ 2)$;
vi. $b^{-1}a^{-1} = (ab)^{-1} = (1\ 6\ 4\ 2\ 3\ 5)$.

Return to Question 2.5 on P53

Solution 2.6

Write down the orders of the following permutations:

i. $(1\ 2\ 3\ 4\ 5)$***;***

ii. $(1\ 2\ 3\ 4\ 5)(7\ 8)$***;***

iii. $(1\ 2\ 3\ 4\ 5\ 6)(7\ 8)$***;***

iv. $(1\ 2)(3\ 4)(5\ 6)(7\ 8)$***;***

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

We will denote by $|g|$ the order of a group element g. Recall that to find the order of a permutation we take the lowest common multiple of the lengths of the *disjoint cycles*.

i. $|(1\ 2\ 3\ 4\ 5)| = 5$;

ii. $|(1\ 2\ 3\ 4\ 5)(7\ 8)| = 10$;

iii. $|(1\ 2\ 3\ 4\ 5\ 6)(7\ 8)| = 6$;

iv. $|(1\ 2)(3\ 4)(5\ 6)(7\ 8)| = 2$;

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

Return to Question 2.6 on P53

Solution 2.7

In each of the following cases find the order of ab***:***

i. $a = (1\ 2)$ ***and*** $b = (1\ 2\ 3)$***;***

ii. $a = (4\ 5)$ ***and*** $b = (1\ 2\ 3)$***;***

iii. $a = (1\ 4)$ ***and*** $b = (1\ 2\ 3)$***;***

iv. $a = (1\ 2)(3\ 4)$ ***and*** $b = (1\ 2\ 3)$***;***

v. $a = (3\ 4)(5\ 6)$ ***and*** $b = (1\ 2\ 3)(4\ 5\ 6)$***;***

vi. $a = (3\ 4)(6\ 7)$ ***and*** $b = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)$***.***

i. $ab = (1\ 2)(1\ 2\ 3) = (1)(2\ 3)$. So, $|ab| = 2$.

ii. $ab = (4\ 5)(1\ 2\ 3)$. So, $|ab| = 6$.

iii. $ab = (1\ 4)(1\ 2\ 3) = (1\ 2\ 3\ 4)$. So, $|ab| = 4$.

iv. $ab = (1\ 2)(3\ 4)(1\ 2\ 3) = (1)(2\ 4\ 3)$. So, $|ab| = 3$.

v. $ab = (3\ 4)(5\ 6)(1\ 2\ 3)(4\ 5\ 6) = (1\ 2\ 4\ 6\ 3)$. So, $|ab| = 5$.

vi. $ab = (3\ 4)(6\ 7)(1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9) = (1\ 2\ 4\ 5\ 7\ 8\ 9\ 6\ 3)$. So, $|ab| = 9$.

Return to Question 2.7 on P53

Solution 2.8

Given** $N \in \mathbb{N}$**, show that there is a number** $n \in \mathbb{N}$ **and elements** $a, b \in S_n$ **such that

- $a^2 = I$**,**
- $b^3 = I$**, and,**
- ***the order of** ab **is greater than** N**.***

We just need to generalise part vi. of Question 2.7 above. Let $a = (3\ 4)(6\ 7)\dots(3n\ 3n+1)$ and $b = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)\dots(3n+1\ 3n+2\ 3n+3)$ be elements of S_n. Then $|a| = 2$, $|b| = 3$ and $|ab| = 3n+3$ for any $n \in \mathbb{N}$.

Return to Question 2.8 on P54

Solution 2.9

Find the largest order for an element of** S_{10}**.

For $f \in S_{10}$, $|f|$ is the lowest common multiple of the lengths of the disjoint cycles. (i.e. the lcm of the sizes of the orbits of f). By considering likely candidates, a 10-cycle has order 10, a 9-cycle and a 1-cycle has order 9, an 8-cycle and a 2-cycle has order 8, but a 3-cycle and a 7-cycle has order 21. This looks best possible until we consider a 2-cycle, 3-cycle and 5-cycle which has order 30. (How could this have been deduced without trial and error?)

Return to Question 2.9 on P54

Solution 2.10

In each of the following cases find the conjugate of a ***with*** b***, i.e. compute*** bab^{-1}***:***

- ***a.*** $a = (1\ 2)$ ***and*** $b = (2\ 3\ 4\ 5)$***;***
- ***b.*** $a = (1\ 3)(2\ 5\ 6)$ ***and*** $b = (2\ 3)(4\ 5)$***;***
- ***c.*** $a = (1\ 4)(2\ 5)$ ***and*** $b = (1\ 3\ 2\ 5)$***;***
- ***d.*** $a = (1\ 2)(3\ 4)$ ***and*** $b = (1\ 2\ 3)$***;***
- ***e.*** $a = (1\ 3\ 2\ 5)$ ***and*** $b = (1\ 4)(2\ 5)$***;***
- ***f.*** $a = (1\ 5\ 6)$ ***and*** $b = (1\ 5\ 6)$***.***

a. $bab^{-1} = (1\ 3)$;

b. $bab^{-1} = (1\ 2)(3\ 4\ 6)$;

c. $bab^{-1} = (3\ 4)(5\ 1)$;

d. $bab^{-1} = (2\ 3)(1\ 4)$;

e. $bab^{-1} = (4\ 3\ 5\ 2)$;

f. $bab^{-1} = (5\ 6\ 1) = a$, as expected.

Return to Question 2.10 on P54

Solution 2.11

In each of the following cases find, where possible, permutations $b \in S_6$ ***and*** $d \in A_6$ ***such that*** $bab^{-1} = c = dad^{-1}$***:***

- ***a.*** $a = (1\ 3\ 2)(4\ 5)$***, and*** $c = (1\ 5)(2\ 3\ 4)$***;***
- ***b.*** $a = (1\ 4)(2\ 3)$***, and*** $c = (1\ 6)(2\ 4)(3\ 5)$***;***
- ***c.*** $a = (1\ 2)(3\ 4)$***, and*** $c = (1\ 3)(2\ 4)$***;***
- ***d.*** $a = (1\ 4)$***, and*** $c = I$***;***
- ***e.*** $a = (1\ 3)$***, and*** $c = (1\ 3)$***.***

a. For $a = (1\ 3\ 2)(4\ 5)$, and $c = (1\ 5)(2\ 3\ 4)$, we can take

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

b. For $a = (1\ 4)(2\ 3)$, and $c = (1\ 6)(2\ 4)(3\ 5)$, there is no such b as a and c have different cycle structures.

c. For $a = (1\ 2)(3\ 4)$, and $c = (1\ 3)(2\ 4)$ we can take

$$b = (2\ 3).$$

d. For $a = (1\ 4)$, and $c = I$, there is no such b.

e. For $a = (1\ 3)$, and $c = (1\ 3)$ we can take

$$b = I.$$

Return to Question 2.11 on P55

Solution 2.12

***Let** $n \geq 5$. **Let** $a, c \in A_n$ **be 3-cycles. Show that there is an element** $b \in A_n$ **such that** $bab^{-1} = c$.*

***Does the statement above hold when** $n \in \{3, 4\}$?*

[Hint: For the first part of the question, find a conjugate in** S_n**; if it is not an element of** A_n **how can you make it into an elmement of** A_n **using the fact that disjoint cycles commute?]

Clearly there is an element $b \in S_n$ such that $bab^{-1} = c$. If b is an element of A_n we are done. Therefore, suppose b is not an element of A_n. Let $i, j \in \{1, 2, \ldots, n\}$ be such that $a(i) = i$ and $a(j) = j$. Notice that i and j exists since a is a three-cycle and $n \geq 5$. Thus the element $b(i\ j)$ is an element of A_n. Moreover, as $(i\ j)$ is disjoing from a, we have

$$b(i\ j)a(i\ j)b^{-1} = ba(i\ j)(i\ j)b^{-1} = bab^{-1} = c$$

as required.

Notice that $A_3 = \{(1\ 2\ 3), (1\ 3\ 2), ()\} \cong \mathbb{Z}_3$ is abelian and so its two three cycles cannot be conjugate to one another.

Now consider the elements $(1\ 2\ 3)$ and $(1\ 3\ 2)$ in A_4. Suppose $b \in A_4$ is such that

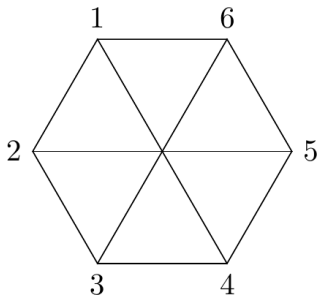
$b(1\ 2\ 3)b^{-1} = (1\ 3\ 2)$. Notice that it must be the case that $\{b(1), b(2), b(3)\} = \{1, 2, 3\}$. Thus there is an element $b' \in S_3$ such that $b'(1\ 2\ 3)(b')^{-1} = (1\ 3\ 2)$. However, we have already seen that no such element exists.

Return to Question 2.12 on P55

A.3 Chapter 3 solutions

Solution 3.1

Consider the group D_6 (the group of symmetries of a regular hexagon) acting on the set, X, of vertices of the regular hexagon shown below and numbered sequentially 1 to 6 in an anticlockwise direction with the upper left vertex being number 1.



Using our standard notation for the elements of D_6:

- ***a. find the orbits of X;***
- ***b. find the stabiliser of each element of X;***
- ***c. show how your results in parts a. and b. above demonstrate the Orbit-Stabiliser Theorem.***

a. $\text{orb}(1) = \{1, 2, 3, 4, 5, 6\} = \text{orb}(2) = \text{orb}(3) = \text{orb}(4) = \text{orb}(5) = \text{orb}(6)$, so there is just the one orbit of X.

b.

$$\text{stab}(1) = \{e, s_6\} = \text{stab}(4)$$
$$\text{stab}(2) = \{e, s_4\} = \text{stab}(5)$$
$$\text{stab}(3) = \{e, s_2\} = \text{stab}(6).$$

c. Consider $g \in X$. Then $|\text{orb}(g)| \times |\text{stab}(g)| = 6 \times 2 = 12 = |D_4|$. This is true for all $g \in X$.

Return to Question 3.1 on P79

Solution 3.2

In how many ways can the edges of a regular octagon be coloured with four different colours if two colourings are indistinguishable when one can be obtained from the other by

i. a rotation of the octagon.

ii. a rotation or reflection of the octagon.

i. Here we are considering the action of the subgroup of D_8 that consists of the identity and the seven rotations, That is $G = \{e, r_1, r_2, r_3, r_4, r_5, r_6, r_7, \}$. There are four colour choices for each of the eight edges. This gives

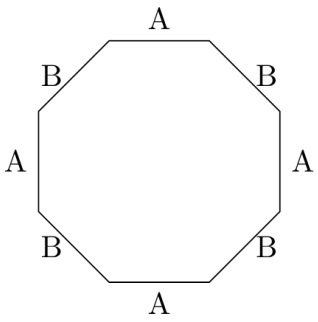
$$|X| = 4^8 = 65,536 = |\,\text{fix}(e)\,|.$$

It is important to remember, in what follows, that when we label an edge with a letter, we are not referring directly to a particular colour; the letterings relate to the relationships between edges and their respective colours. So, for a given letter we have a free choice of colour, but having made that choice then that colour must be used wherever that letter appears. In general, for a regular n-gon, the rotations will be of $\frac{i2\pi}{n}$ radians where i is an integer such that $0 \leq i < n$. Now, for the colourings to be indistinguishable under the rotations where i and n are relatively prime (that is, in this case, odd i since n is 8) all of the edges must have the same colour. So we have that

$$|\,\text{fix}(r_1)\,| = |\,\text{fix}(r_3)\,| = |\,\text{fix}(r_5)\,| = |\,\text{fix}(r_7)\,| = 4.$$

For the rotations of $\frac{\pi}{2}$ and $\frac{3\pi}{2}$ radians, that is r_2 and r_6, we can have the

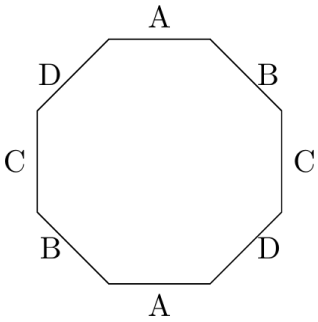
following configuration:



This, in terms of colours, means that we either use just two colours, in which case they must alternate around the edges, or just the same colour for each edge. So, we have

$$|\,\mathrm{fix}(r_2)\,| = |\,\mathrm{fix}(r_6)\,| = 4^2 = 16.$$

The remaining rotation, that is r_4 through π radians, requires the following configuration:



So, we have

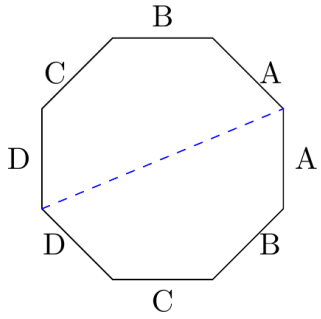
$$|\,\mathrm{fix}(r_4)\,| = 4^4 = 256.$$

Then, by Burnside's Lemma, the number of orbits (and, hence, the number of

distinct colourings) is

$$\frac{1}{|G|}\sum |\,\mathrm{fix}(g)\,| = \frac{1}{8}\left(4^8 + (4\times 4) + (2\times 4^2) + 4^4\right) = 8230.$$

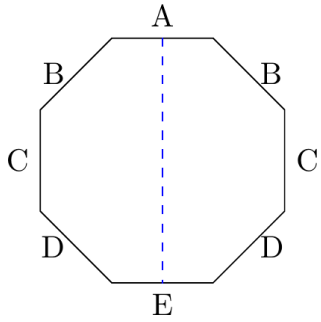
ii. Here we are considering the action of the full dihedral group D_8 and so as well as the rotations discussed above we also need to look at the reflections. Note that there are two types of lines of symmetry; vertex to opposite vertex and midpoint of edge to midpoint of opposite edge. For vertex to vertex we have the following:



So

$$|\,\mathrm{fix}(s_1)\,| = |\,\mathrm{fix}(s_3)\,| = |\,\mathrm{fix}(s_5)\,| = |\,\mathrm{fix}(s_7)\,| = 4^4 = 256.$$

For midpoint to midpoint we have:



So

$$|\,\mathrm{fix}(s_2)\,| = |\,\mathrm{fix}(s_4)\,| = |\,\mathrm{fix}(s_6)\,| = |\,\mathrm{fix}(s_8)\,| = 4^5 = 1024.$$

It is important to note, in this last case, that using five letters does not imply that we need five colours! Then, by Burnside's Lemma, the number of orbits (and, hence, the number of distinct colourings) is

$$\frac{1}{|G|}\sum |\,\mathrm{fix}(g)\,| = \frac{1}{16}\left(4^8+(4\times 4)+(2\times 4^2)+4^4+(4\times 4^4)+(4\times 4^5)\right) = 4435.$$

Return to Question 3.2 on P80

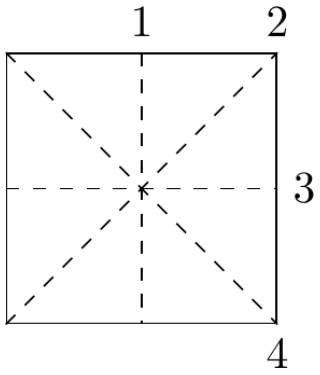
Solution 3.3

Use Burnside's Lemma to count the distinguishable colourings of the edges of

- ***i. a square,***
- ***ii. a regular pentagon,***

using at most three colours under the relevant full dihedral group of symmetries in each case.

i. **The square:** Here we are considering the action of the dihedral group D_4 that consists of the identity, three rotations and four reflections. We will use the usual notation with r_i being an anticlockwise rotation through $\frac{i\pi}{2}$ radians and the reflections being s_i where $i = 1, 2, 3, 4$. Note, in particular, that the lines of reflection 1 and 3 are midpoint to midpoint whilst 2 and 4 are vertex to vertex.



There are three colour choices for each of the four edges. This gives

$$|X| = 3^4 = 81 = |\,\mathrm{fix}(e)\,|.$$

For the rotations (noting that 1 and 3 are relatively prime to 4) we have

$$|\,\mathrm{fix}(r_1)\,| = |\,\mathrm{fix}(r_3)\,| = 3.$$

and

$$|\,\mathrm{fix}(r_2)\,| = 3^2 = 9.$$

For the reflections (using the principles established in Q1) we have

$$|\,\mathrm{fix}(s_1)\,| = |\,\mathrm{fix}(s_3)\,| = 3^3 = 27.$$

and

$$|\,\mathrm{fix}(s_2)\,| = |\,\mathrm{fix}(s_4)\,| = 3^2 = 9.$$

Then, by Burnside's Lemma, the number of orbits (and, hence, the number of distinct colourings) is

$$\frac{1}{|G|}\sum |\,\mathrm{fix}(g)\,| = \frac{1}{8}\left(81 + (2\times 3) + 9 + (2\times 3^2) + (2\times 3^3)\right) = 21.$$

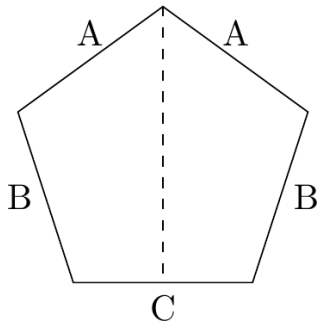
ii. **The pentagon:** The case for a regular pentagon is straightforward.

$$|\,\mathrm{fix}(e)\,| = 3^5 = 243.$$

Since the number of sides is prime, the size of the fix for all rotations is the same (since for each r_i we have that i is relatively prime to 5). Hence

$$|\,\mathrm{fix}(r_i)\,| = 3 \quad \forall i,\ i = 1, 2, 3, 4.$$

Furthermore, as there is only one type of reflection (each one passes from a vertex to the midpoint of the opposite side) we have



$$|\,\mathrm{fix}(s_i)\,| = 3^3 = 27 \quad \forall i,\ i = 1, 2, 3, 4, 5.$$

Then, by Burnside's Lemma, the number of orbits (and, hence, the number of distinct colourings) is

$$\frac{1}{|G|}\sum |\,\mathrm{fix}(g)\,| = \frac{1}{10}\left(243 + (4 \times 3) + (5 \times 27)\right) = 39.$$

Return to Question 3.3 on P80

Solution 3.4

Use Burnside's Lemma to count the distinguishable colourings of the edges of a square with four distinct colours when two colourings are indistinguishable if one can be obtained from the other by

i. a rotation of the square,

ii. a rotation or reflection of the square.

We use the same reasoning as in the previous examples.

i. Rotation of the square: There are four colour choices for each of the four edges. This gives

$$|X| = 4^4 = 256 = |\,\mathrm{fix}(e)\,|.$$

For the rotations (noting that 1 and 3 are relatively prime to 4) we have

$$|\,\mathrm{fix}(r_1)\,| = |\,\mathrm{fix}(r_3)\,| = 4.$$

(all edges have the same colour), and

$$|\,\mathrm{fix}(r_2)\,| = 4^2 = 16.$$

(opposite edges have the same colour). Then, by Burnside's Lemma, the number of distinct colourings is

$$\frac{1}{|G|}\sum |\,\mathrm{fix}(g)\,| = \frac{1}{4}\left(256 + 16 + (2 \times 4)\right) = 70.$$

ii. Rotation or reflection of the square: We need, in addition to the above, to consider the reflections in addition to the rotations. So, the whole of D_4 is acting. For the reflections we have:

$$|\,\mathrm{fix}(s_1)\,| = |\,\mathrm{fix}(s_3)\,| = 4^3 = 64.$$

and

$$|\,\mathrm{fix}(s_2)\,| = |\,\mathrm{fix}(s_4)\,| = 4^2 = 16.$$

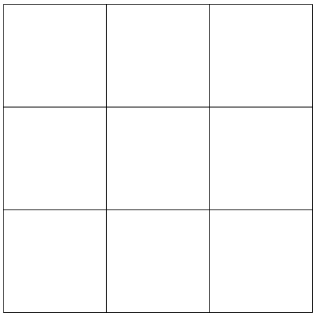
Then, by Burnside's Lemma, the number of orbits (and, hence, the number of distinct colourings) is

$$\frac{1}{|G|}\sum |\,\mathrm{fix}(g)\,| = \frac{1}{8}\left(256 + 16 + (2 \times 4) + (2 \times 4^2) + (2 \times 4^3)\right) = 55.$$

Return to Question 3.4 on P81

Solution 3.5

Use Burnside's Lemma to enumerate the distinguishable colourings of the regions of the following square grid using at most two colours:



a. under the group of rotations of the square;

b. under the full dihedral group D_4.

Give an example of two colourings that are distinguishable in part a. but not in part b.

a. *rotations of the square*: The number of distinguishable colourings is given by the number of orbits of the action of the rotation group, $\{e, r_1, r_2, r_3\}$, on the set of all colourings of the figure. We use the usual notation. There are just two colour choices for each of the nine regions. This gives

$$|X| = 2^9 = 512 = |\,\mathrm{fix}(e)\,|.$$

For the rotations r_1 and r_3 (noting that 1 and 3 are relatively prime to 4) we must have that each of the corner squares must be the same colour as each other and each of the mid-side squares must be the same colour as each other (though not necessarily different from the corner squares), with the centre square being any of the two colours we choose. Thus:

$$|\,\mathrm{fix}(r_1)\,| = |\,\mathrm{fix}(r_3)\,| = 2^3 = 8.$$

A	B	C
B	C	B
A	B	A

and for the rotation r_2 (through π radians) we have the following:

$$|\,\mathsf{fix}(r_2)\,| = 2^5 = 32.$$

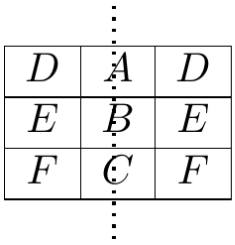
A	B	C
D	E	D
C	B	A

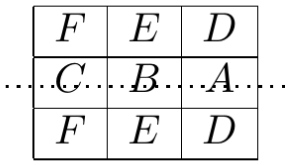
Then, by Burnside's Lemma, the number of distinct colourings is

$$\frac{1}{|G|}\sum |\,\mathsf{fix}(g)\,| = \frac{1}{4}\left(512 + 2^5 + (2\times 8)\right) = 140.$$

b. *under the full dihedral group* D_4

For the reflections we note that there are two types of line of symmetry; vertex to vertex and mid-point to mid-point. For mid-point to mid-point we have:





$$|\,\mathsf{fix}(s_1)\,| = |\,\mathsf{fix}(s_3)\,| = 2^6 = 64.$$

For vertex to vertex we have:

$$|\,\text{fix}(s_2)\,| = |\,\text{fix}(s_4)\,| = 2^6 = 64.$$

Then, by Burnside's Lemma, the number of distinct colourings is (taking into account rotations and reflections)

$$\frac{1}{|G|}\sum |\,\text{fix}(g)\,| = \frac{1}{8}\left(512 + 2^5 + (2\times 8) + (4\times 2^6)\right) = 102.$$

Note that for all rotations, colourings will be distinguishable if any given pair of diametrically opposed squares are not of the same colour. All we then need to do is to construct a colouring with that property but which has reflective symmetry about a line of symmetry. Given what we have said about diagonally opposed pairs, it makes sense to use a line of symmetry that is mid-point to mid-point, and we shall use the vertical line. So, in the diagram below, no rotation will turn the configuration on the left to the one on the right, but the right configuration is a reflection of the left configuration.

1	1	2
1	1	1
2	2	2

2	1	1
1	1	1
2	2	2

Return to Question 3.5 on P81

Solution 3.7

A teacher has a bank of n test questions and wants to assign to each of 3 students, A, B, C, one of the n questions in this bank. The teacher is not concerned if the same question is assigned to more than one student, and is not concerned about the order in which the questions are assigned to the students. Using Burnside's Lemma determine the number of essentially different ways of assigning a question from the bank to each student.

Let X be the set of all valid assignment of test questions to the students. The size of X is n^3 (since the same question can be assigned to more than 1 student).

Let T_1, T_2, T_3 be test questions, write $T_1T_2T_3$ for the assignment $T_1 \to A$, $T_2 \to B$ and $T_3 \to C$. Since the teacher is not concerned about the order in which questions are allocated to students, we consider two assignments equal if they use the same test questions. In particular if T_1, T_2 and T_3 are test questions, then the assigment $T_1T_2T_3$ is equivalent to any assigment in the set

$$\{T_1T_2T_3, T_1T_3T_2, T_2T_1T_3, T_2T_3T_1, T_3T_1T_2, T_3T_2T_1\}.$$

In particular, two assignments $T_1T_2T_3$ and $t_1t_2t_3$ are equal if there is an element $\sigma \in S_3$ such that $t_1t_2t_3 = T_{\sigma(1)}T_{\sigma(2)}T_{\sigma(3)}$.

Now that we know what the acting group is, we can apply Burnside's Lemma.

The identity permutation fixes all assignments: $|\operatorname{fix}(())| = n^3$.

An assigment is fixed by a three cycle, if and only if it is of the form TTT for T a test question. Therefore for σ a three cycle, $|\operatorname{fix}(\sigma)| = n$.

The 2-cycle $(1\ 2)$ fixes all assigments of the form TTT' for T and T' test questions. Thus $|\operatorname{fix}((1\ 2))| = n^2$. A similar argument holds for the other 2-cycles. In particular, for σ a 2-cycle, $|\operatorname{fix}(\sigma)| = n^2$.

By Burnside's Lemma, the number of essentiall different assigments, is:

$$\frac{n^3 + 2n + 3n^2}{6}.$$

Return to Question 3.6 on P82

Solution 3.7

Consider the proof of Cauchy's Theorem with $G = D_5$ and $p = 5$. Describe the set X and the group acting on X. Determine the possible sizes of the orbits in X under this action and write out, in full, two distinct orbits for each of these possible sizes.

$X = \{(g_1, g_2, g_3, g_4, g_5) \in G^5 \mid g_1g_2g_3g_4g_5 = e\}$ so $|X| = 10^4 = 2^4 \times 5^4$, which is a multiple of 5. The group acting on X is $\langle(1\ 2\ 3\ 4\ 5)\rangle$ which is the cyclic group of order 5 and since the size of each orbit divides 5 this must have size either 1 or 5. Orbits of size 1 correspond to the identity or elements of order 5, so two such orbits are

$$\{(e, e, e, e, e)\} \quad \text{and} \quad \{(r_1, r_1, r_1, r_1, r_1)\}.$$

Orbits of size 5 can take a variety of forms, but two simple examples (which are independent of how we define D_5) are

$$\{(e, r_1, r_2, r_3, r_4), (r_1, r_2, r_3, r_4, e), (r_2, r_3, r_4, e, r_1),$$
$$(r_3, r_4, e, r_1, r_2), (r_4, e, r_1, r_2, r_3)\}$$

and

$$\{(s_1, s_1, s_2, s_2, e), (s_1, s_2, s_2, e, s_1), (s_2, s_2, e, s_1, s_1),$$
$$(s_2, e, s_1, s_1, s_2), (e, s_1, s_1, s_2, s_2)\}.$$

Return to Question 3.7 on P82

A.4 Chapter 4 solutions

Solution 4.1

Classify each of the following groups according to the Fundamental Theorem of Finite Abelian Groups and in each case give an isomorphism from the stated group to the group given as your answer.

(a) $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1,0)\rangle$.
(b) $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$.
(c) $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(2,2)\rangle$.

(a) $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1,0)\rangle$ is an abelian group of order 6 (as $|\,(\mathbb{Z}_3 \times \mathbb{Z}_6)\,| = 3 \times 6 = 18$ and $|\,\langle(1,0)\rangle\,| = 3$) so it must be isomorphic to $\mathbb{Z}_6$ since there is only one group of this order that is abelian (up to isomorphism). But $\mathbb{Z}_6$ is not in the form given by the FTFAG as 6 is not the power of a prime. So the given group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$ (which is, of course, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$). You should check that this follows from Theorem 5.3. An isomorphism from $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1,0)\rangle$ to $\mathbb{Z}_6$ is easy (just map $(x,y) + \langle(1,0)\rangle$ to y), but we need a mapping from $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1,0)\rangle$ to $\mathbb{Z}_2 \times \mathbb{Z}_3$. Since both groups are cyclic we just map a generator in one group to a generator in another, for example:

$$(0,1) + \langle(1,0)\rangle \mapsto (1,1).$$

It then follows that

$$\begin{aligned}
(0,2)+\langle(1,0)\rangle &\mapsto (0,2)\\
(0,3)+\langle(1,0)\rangle &\mapsto (1,0)\\
(0,4)+\langle(1,0)\rangle &\mapsto (0,1)\\
(0,5)+\langle(1,0)\rangle &\mapsto (1,2)\\
(0,6)+\langle(1,0)\rangle &\mapsto (0,0) \qquad \text{as expected!}
\end{aligned}$$

(b) This one is not so obvious, so we need to kick it around a bit.

$$\langle(1,2)\rangle = \{(0,0),(1,2),(2,4),(3,6)\} = H.$$

Now we can see that $(0,1)+H$ has order 8 (because the first multiple of $(0,1)$ in H is $(0,0)$) and since $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$ has order 8 it must be isomorphic to $\mathbb{Z}_8$. An isomorphism is given by

$$(x,y)+H \mapsto y.$$

Note that this is in the correct form for the FTFAG as 8 is a power of a prime.

(c) Again, this is not obvious, so let

$$H = \langle(2,2)\rangle = \{(0,0),(2,2),(0,4),(2,6)\}.$$

Hence, $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(2,2)\rangle$ has order 8. This time $(0,1)+H$ has order 4 (make sure you understand why). This rules out $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, but still leaves $\mathbb{Z}_8$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$ as possibilities. We could list the order of each of the elements, or look for elements of order 8, or for more than one element of order 2 (because cyclic groups of even order have exactly one element of order 2). You should beware of falling into the following trap. It may be tempting to say that, since

$(0,2)+H$ and $(2,0)+H$ both have order 2, the group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$. But, $(0,2)+H$ and $(2,0)+H$ are both the same coset (list the elements if you cannot see this directly)!! However, $(1,1)+H$ and $(0,2)+H$ are *distinct* elements of order 2 so the group is indeed isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$. The following is an isomorphism

$$\begin{aligned} H &\mapsto (0,0) & (1,1)+H &\mapsto (1,0) \\ (0,1)+H &\mapsto (0,1) & (1,2)+H &\mapsto (1,1) \\ (0,2)+H &\mapsto (0,2) & (1,3)+H &\mapsto (1,2) \\ (0,3)+H &\mapsto (0,3) & (1,4)+H &\mapsto (1,3) \end{aligned}$$

Return to Question 4.1 on P106

Solution 4.2

Let H be a subgroup of a group G.

(a) Show that, for all $g \in G$, the set

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

forms a subgroup of G.

(b) Deduce that if G has exactly one subgroup, H, of a given finite order, then H is a normal subgroup of G.

(a) Clearly $gHg^{-1} \neq \emptyset$ and $gHg^{-1} \subseteq G$ so we just need to show that the set gHg^{-1} is closed under products and inverses. Let $g_1, g_2 \in gHg^{-1}$. So, there exist $h_1, h_2 \in H$ such that $g_1 = gh_1g^{-1}$ and $g_2 = gh_2g^{-1}$. Then

$$g_1g_2 = (gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in gHg^{-1}$$

(because $h_1h_2 \in H$ as H is a subgroup). Also,

$$g_1^{-1} = (gh_1g^{-1})^{-1} = (g^{-1})^{-1}h_1^{-1}g^{-1} = gh_1^{-1}g^{-1} \in gHg^{-1}$$

(because $h_1^{-1} \in H$ as H is a subgroup).

(b) If H is the only subgroup of order $|H|$ then, for all $g \in G$, $gHg^{-1} = H$ (think about it...). That is, H is normal in G.

Return to Question 4.2 on P107

Solution 4.3

Let H be a subgroup of a group G. Prove that the centre of G is a normal subgroup of the normaliser of H. [Hint: all you really need to show is that $Z(G) \subseteq N(H)$ and the rest is 'obvious'.]

First recall the definitions. The *centre* of G is denoted and defined by

$$Z(G) = \{z \in G \,|\, zg = gz \;\forall\, g \in G\}.$$

The *normaliser* of H in G is denoted and defined by

$$N(H) = \{g \in G \,|\, gH = Hg\}.$$

Now we know that $N(H)$ is a subgroup of G and we also know that $Z(G)$ is a normal subgroup of G. So, if we can show that $Z(G) \subseteq N(H)$, then it follows that $Z(G)$ is a normal subgroup of $N(H)$. Now, let $x \in Z(G)$. Then,

$$\begin{aligned}
& xg = gx && \forall\, g \in G \\
\Rightarrow & xh = hx && \forall\, h \in H \qquad \text{(as } h \in G \text{ also)} \\
\Rightarrow & xH = Hx \\
\Rightarrow & x \in N(H).
\end{aligned}$$

Hence $Z(G) \subseteq N(H)$, as required. (Note that $Z(G)$ must be normal in $N(H)$ else it would not be normal in G.)

Return to Question 4.3 on P107

Solution 4.4

Let $n \geq 3$. Show that the centre of S_n is trivial. What is the centre of S_2?

Suppose $g \in S_n$ is a non-trivial element of $Z(S_n)$. There is a point $x \in \{1, 2, \ldots, n\}$ such that $g(x) = y \neq x$. Let $z \in \{1, 2, \ldots, n\} \backslash \{x, y\}$. Notice that z exists since $n \geq 3$.

Consider $g(x\ y\ z)g^{-1}$. Since $g \in Z(S_n)$, then $g(x\ y\ z)g^{-1} = (x\ y\ z)$. We compute

$$g(x\ y\ z)g^{-1} = (g(x)\ g(y)\ g(z)) = (y\ g(y)\ g(z)) = (x\ y\ z).$$

It follows that $g(y) = z$ and $g(z) = x$.

Now consider the two cycle $(x\ y)$. We must also have $g(x\ y)g^{-1} = (x\ y)$. However, from above, $g(x\ y)g^{-1} = (yz) \neq (x\ y)$ (since $z \neq x$). This yields the desired contradiction. We conclude that $Z(S_n)$ contains only the identity permutation.

The group S_2 is isomorphic to Z_2 and so is abelian and equal to its own centre.

Return to Question 4.4 on P107

Solution 4.5

Let N be a normal subgroup of a finite group G, and H be a further subgroup of G (which need not be normal in G). Show that the set NH, where

$$NH = \{nh \,|\, n \in N, h \in H\}$$

forms a subgroup of G.

Clearly $e \in NH$ so $NH \neq \emptyset$. Since G and, hence, the set NH is finite we need only check the closure of NH under products. Let $n_1, h_1, n_2, h_2 \in NH$. Then,

$$\begin{aligned}(n_1h_1)(n_2h_2) &= n_1(h_1n_2)h_2 && \text{(associativity)}\\ &= n_1(n_3h_1)h_2 && \text{(for some } n_3 \in N \text{ because } h_1N = Nh_1)\\ &= (n_1n_3)(h_1h_2) \ \in NH && \text{(as } n_1n_3 \in N \text{ and } h_1h_2 \in H).\end{aligned}$$

Hence NH is a subgroup of G.

Return to Question 4.5 on P108

Solution 4.6

In D_4, let e and r_2 denote the identity and π radians rotation respectively. Given that $N = \{e, r_2\}$ is a normal subgroup of D_4, give an example of a surjective homomorphism

$$\phi : D_4 \to D_4/N$$

and classify D_4/N according to the Fundamental Theorem of Finite Abelian Groups.

Note that $|D_4| = 8$ and $|N| = 2$, so $|D_4/N| = 4$. Hence it follows (from the Fundamental Theorem) that either $D_4/N \cong \mathbb{Z}_4$ or $D_4/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. The elements of D_4/N are:

$$\begin{aligned}N = r_2N &= \{e, r_2\}\\ r_1N = r_3N &= \{r_1, r_3\}\\ s_1N = s_3N &= \{s_1, s_3\}\\ s_2N = s_4N &= \{s_2, s_4\}.\end{aligned}$$

Clearly $(s_1N)^2 = (s_2N)^2 = N$ and $(r_1N)^2 = r_2N = N$, so all non-identity elements

have order 2. Hence $D_4/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. A surjective homomorphism $\phi : D_4 \to D_4/N$ is

$$\begin{aligned} \phi(e) = \phi(r_2) &= N \\ \phi(r_1) = \phi(r_3) &= r_1 N \\ \phi(s_1) = \phi(s_3) &= s_1 N \\ \phi(s_2) = \phi(s_4) &= s_2 N. \end{aligned}$$

Return to Question 4.6 on P108

Solution 4.7

Consider the quarternion group Q_8 with elements $\{\pm 1, \pm i, \pm j, \pm k\}$ and multiplication defined by the rules:

$$(-1)^2 = 1,$$
$$i^2 = j^2 = k^2 = -1,$$

and

$$ij = k = -(ji), jk = i = -(kj), ki = j = -(ik).$$

The group $N = \{1, -1\}$ is a normal subgroup of Q_8. Find elements $g_1, g_2, \ldots, g_i \in Q_8$ such that $\{g_1 N, g_2 N \ldots, g_i N\}$ are the distinct left cosets of N in G.

Classify the group Q_8/N according to the Fundamental Theorem of finite abelian groups.

The distinct left cosets are given by N, iN, jN, kN. This follows since for distinct elements $a, b \in \{i, j, k\}$, $-ab \in \{\pm i, \pm j, \pm k\}$. Now observe that in Q_8/N, the elements iN, jN and kN all have period 2. We conclude that Q_8/N is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Return to Question 4.7 on P108

A.5 Chapter 5 solutions

Solution 5.1

Let $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to D_4$ ***be a homomorphism with kernel*** $K = \langle (2,2) \rangle$***, where*** D_4 ***denotes the dihedral group of order 8.***

- ***(i) List the elements of*** K ***and of*** $(\mathbb{Z}_4 \times \mathbb{Z}_6)/K$***.***
- ***(ii) Classify*** $\phi(\mathbb{Z}_4 \times \mathbb{Z}_6)$ ***according to the Fundamental Theorem of Finite Abelian Groups.***

(i) $K = \{(0,0),(0,2),(0,4),(2,0),(2,2),(2,4)\}$. $(\mathbb{Z}_4 \times \mathbb{Z}_6)/K = \{K, (1,0)+K, (0,1)+K, (1,1)+K\}$.

(ii) Since $|\,(\mathbb{Z}_4 \times \mathbb{Z}_6)/K\,|$ is 4, then this group is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note that each non-identity element of $(\mathbb{Z}_4 \times \mathbb{Z}_6)/K$ has order 2 (convince yourselves that this is the case) and so $(\mathbb{Z}_4 \times \mathbb{Z}_6)/K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Hence $\phi(\mathbb{Z}_4 \times \mathbb{Z}_6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Return to Question 5.1 on P122

Solution 5.2

Let $\phi : G \to G'$ ***be a group homomorphism. Show that if*** $|G|$ ***and*** $|G'|$ ***are finite, then:***

- ***(a)*** $|\phi(G)|$ ***is a divisor of*** $|G'|$***.***
- ***(b)*** $|\phi(G)|$ ***is a divisor of*** $|G|$***.***
- ***(c)*** $\forall\, g \in G$***, the order of*** $\phi(g)$ ***divides the order of*** g***.***

(a) $\phi(G)$ is a subgroup of G' and so, by Lagrange's Theorem, $|\phi(G)|$ divides $|G'|$.

(b) We know that $\phi(G) \cong G/K$, where K is the kernel of ϕ. As these two groups are isomorphic it follows that they must have the same order and so

$$|\,\phi(G)\,| = |\,G/K\,| = \frac{|\,G\,|}{|\,K\,|}$$

and hence $|\,K\,| = \dfrac{|\,G\,|}{|\,\phi(G)\,|}$. It then follows that $|\,\phi(G)\,|$ divides $|\,G\,|$.

(c) We have that $\phi(g^m) = (\phi(g))^m$ for all $m \in \mathbb{Z}$. So, if g has order k in G, then

$$e' = \phi(e) = \phi(g^k) = (\phi(g))^k$$

and so the order of $\phi(g)$ divides k (recall that the order of an element is the smallest positive integer power, n say, such that $\phi(g))^n = e'$. So, if $(\phi(g))^k = e'$, then n must divide k).

Return to Question 5.2 on P122

Solution 5.3

Let $\phi : G \to G'$ be a group homomorphism. For each of the following statements, show whether it is true or false by providing either a proof or a non-trivial counter-example as appropriate. (The trivial homomorphism from G to G' is defined by $\phi(g) = e', \ \forall\, g \in G$.)

(a) If G is abelian, then G' is abelian.
(b) If G' is abelian, then G is abelian.
(c) If G is abelian, then $\phi(G)$ is abelian.
(d) If $\phi(G)$ is abelian, then G is abelian.

(a) This statement is *false*. Consider the mapping $\phi : \mathbb{Z}_2 \to \mathbb{Z}_2 \times D_3$ defined by $\phi(0) = (0, e)$ and $\phi(1) = (1, e)$. This is a homomorphism since

$$\phi(0 + 1) = \phi(1) = (1, e) = (0, e)(1, e) = \phi(0)\phi(1),$$

and whilst $\mathbb{Z}_2$ is abelian, $\mathbb{Z}_2 \times D_3$ is not abelian.

(b) This statement is *false*. Consider the mapping $\phi : D_3 \to \mathbb{Z}_2$ defined by $\phi(e) = \phi(r_1) = \phi(r_2) = 0$ and $\phi(s_i) = 1$ for all $i = 1, 2, 3$. Clearly this is a homomorphism (convince yourselves) and whilst $\mathbb{Z}_2$ is abelian, D_3 is non-abelian.

(c) This statement is *true*. Let $\phi(x), \phi(y) \in \phi(G)$. Then,

$$\begin{aligned} \phi(x)\phi(y) &= \phi(xy) && \text{(homomorphism)} \\ &= \phi(yx) && (G \text{ is abelian}) \\ &= \phi(y)\phi(x), \end{aligned}$$

so $\phi(G)$ is abelian.

(d) This statement is *false*. The counter example in part (b) above will suffice. (If you want a non-surjective homomorphism then you could have $\phi : D_3 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by $\phi(e) = \phi(r_1) = \phi(r_2) = (0,0)$ and $\phi(s_i) = (1,0)$ for all $i = 1, 2, 3$.)

Return to Question 5.3 on P122

Solution 5.4

By considering all of the normal subgroups of D_4, determine the number of distinct homomorphisms that exist from D_4 to A_4.

The first thing to note is that as the kernel of a homomorphism mapping from G to G' is a normal subgroup of G and, therefore, in this example, must be one of the normal subgroups of D_4. There are six normal subgroups of D_4 which are D_4, $\{e\}$, $\{e, r_2\}$, $\{e, r_1, r_2, r_3\}$, $\{e, r_2, s_1, s_3\}$, and $\{e, r_2, s_2, s_4\}$. If $\phi : D_4 \to A_4$ is a homomorphism, then $K = \ker(\phi)$ is a normal subgroup of D_4 and $\phi(D_4)$ is a subgroup of A_4 (Theorem 5.1), with

$$|K| \times |\phi(D_4)| = 8.$$

(This follows from the First Isomorphism Theorem; as $\phi(G) \cong G/K$ then the sizes of these two groups must be the same, so $|K| \times |\phi(G)| = |G|$.) Clearly, $K \neq \{e\}$ since

A_4 has no subgroup of order 8 ($|A_4| = 12$). If $K = D_4$, his implies that ϕ is the trivial homomorphism. If $|K| = 4$ then $|\phi(D_4)| = 2$, so $\phi(D_4) = \{\,\mathrm{id}, (1\ 2)(3\ 4)\}$, $\{\,\mathrm{id}, (1\ 3)(2\ 4)\}$, or $\{\,\mathrm{id}, (1\ 4)(2\ 3)\}$, giving three homomorphisms for each of the three possible choices of K (there are three normal subgroups of D_4 of order 4). Hence, there are 9 distinct homomorphisms of this type. If $|K| = 2$ then $K = \{e, r_2\}$ and

$$D_4/K = \{\{e, r_2\}, \{r_1, r_3\}, \{s_1, s_3\}, \{s_2, s_4\}\},$$

which has order 4. So $D_4/K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ as each non-identity element in D_4/K has order 2. Hence, $\phi(D_4) = \{\,\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ by the First Isomorphism Theorem. We know that $\phi(e) = \phi(r_2) =$ id, $\phi(r_1) = \phi(r_3)$, $\phi(s_1) = \phi(s_3)$, and $\phi(s_2) = \phi(s_4)$. There are no further restrictions, so there are 6 homomorphisms of this type. Hence the total number of homomorphisms is $1 + 9 + 6 = 16$.

Return to Question 5.4 on P122

Solution 5.5

Let** G, H, K **be groups.

- ***a.** **If** $\phi : G \to H$ **is a homomorphism and** $\psi : H \to K$ **is a homomorphism, show that** $\psi\phi : G \to K$**.***
- ***b.** **If** $\phi : G \to H$ **is an isomorphism, show that** $\phi^{-1} : H \to G$ **is also an isomorphism.***

a. Let $x, y \in G$. Then

$$\psi\phi(xy) = \psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) = \psi\phi(x)\psi\phi(y)$$

as required.

b. Clearly ϕ^{-1} is also a bijection. Therefore it remains to show that ϕ^{-1} is a homomorphism. Let $s, t \in H$. There are $x, y \in G$ such that $\phi(x) = s$ and

$\phi(y) = t$. We have

$$\phi^{-1}(st) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(s)\phi^{-1}(t)$$

as required.

Return to Question 5.5 on P123

Solution 5.6

Let G be a group and fix an element $g \in G$. Define a mapping $\kappa_g : G \to G$ by $\kappa_g(h) = ghg^{-1}$ for all $h \in G$. Show that κ_g is an isomorphism from G to G.

First we show that κ_g is invertible (and so a bijection). Define $\kappa_{g^{-1}} : G \to G$ by $\kappa_{g^{-1}}(h) = g^{-1}hg$ for all $h \in G$. Observe that for any $h \in G$,

$$\kappa_g\kappa_{g^{-1}}(h) = \kappa_g(g^{-1}hg) = g(g^{-1}hg)g^{-1} = h.$$

Similarly, $\kappa_{g^{-1}}\kappa_g(h) = h$ for all $h \in G$.

It follows that $\kappa_{g^{-1}} = \kappa_g^{-1}$. Therefore, κ_g is invertible and so a bijection.

Now we show that κ_g is a homomorphism.

Let $h, k \in G$, then,

$$\kappa_g(hk) = ghkg^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1}) = \kappa_g(h)\kappa_g(k)$$

as required.

Return to Question 5.6 on P123

Solution 5.7

Write down a non-trivial homomorphism from A_4 to D_3 and describe its kernel, K. Form the quotient group A_4/K and show directly that this is isomorphic to the image of A_4. (This is a bit tricky; remember that the image of A_4 need not be the whole of D_3, but must be a non-trivial subgroup of D_3.)

If $\phi : A_4 \to D_3$ is a homomorphism, then $\phi(A_4)$ is a subgroup of D_3 isomorphic to A_4/K (First Isomorphism Theorem). Now, $|A_4| = 12$ so, by Lagrange's Theorem, we know that $|K| = 1, 2, 3, 4, 6$ or 12. $|K| = 1 \Rightarrow |\, A_4/K \,| = 12$ and $|K| = 3 \Rightarrow |\, A_4/K \,| = 4$, but neither of these are possible since D_3 does not have subgroups of orders 12 or 4 (as $|D_3| = 6$). $|K| = 12 \Rightarrow |\, A_4/K \,| = 1$, so ϕ is trivial. $|K| \neq 6$ since A_4 has no subgroup of order 6. Now, A_4 has eight elements of order 3 and three of order 2 (cyclic structures $(* \ * \ *)$ and $(* \ *)(* \ *)$ respectively - see Problem Sheet 3 Q4). By part 1(c) above, the elements of order 3 must map to the identity or one of the rotations in D_3 and, similarly, the elements of order 2 must map onto the identity or a reflection. Now, if $|K| = 2$ then $A_4/K \cong D_3$ but this is not possible since A_4/K only has two elements of order 2 whereas D_3 has three elements (each of the reflections) of order 2. We now consider why this is so. Any subgroup of order 2 in A_4 must contain the identity and one element of order 2. So, there are only three possible subgroups of A_4 of order 2, namely $\{id, (1\ 2)(3\ 4)\}, \{id, (1\ 3)(2\ 4)\}$ and $\{id, (1\ 4)(2\ 3)\}$. Now, a coset, σK from A_4/K has order 2 if and only if $\sigma \notin K$ (if it were then $\sigma K = K$ and that has order 1 in A_4/k), *and* $\sigma^2 \in K$. We illustrate this last point by example. Suppose that $K = \{id, (1\ 2)(3\ 4)\}$, how can we form a σK of order 2 in A_4/K? Well, $(1\ 3)(2\ 4)K = (1\ 4)(2\ 3)K$ and this coset has period 2, but there are no others. Also, any other coset σK such that $\sigma = (* \ * \ *)$ does not have order 2 since $\sigma^2 \neq$ id nor is $\sigma^2 \in K$. So, there is exactly one element of period 2 in A_4/K, and so $A_4/K \ncong D_3$. If $|K| = 4$ then $|A_4/K| = 3$ and hence $A_4/K \cong \{e, r_1, r_2\}$. Now, $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ and $A_4/K = \{K, (1\ 2\ 3)K, (1\ 2\ 4)K\}$. We now define a homomorphism $\phi : A_4 \to D_3$ by: $\phi(e) = \phi((1\ 2)(3\ 4)) = \phi((1\ 3)(2\ 4)) = \phi((1\ 4)(2\ 3)) = e$ $\phi(\sigma) = r_1 \quad \forall\, \sigma \in (1\ 2\ 3)K = \{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\}$ $\phi(\sigma) = r_2 \quad \forall\, \sigma \in (1\ 2\ 4)K =$

$\{(1\ 2\ 4), (1\ 4\ 3), (1\ 3\ 2), (2\ 3\ 4)\}$ This then forces the isomorphism (see the proof to the First Isomorphism Theorem) $\mu : A_4/K \to \phi(D_3)$ (where $\phi(D_3) = \{e, r_1, r_2\}$) defined by $\mu(aK) \to \phi(a)$.

Return to Question 5.7 on P123

A.6 Chapter 6 solutions

Solution 6.1

Determine whether the converse of Lagrange's Theorem is true for all finite p-groups. Provide either a proof or a counter-example to justify your assertion.

G is a finite p-group if and only if $|G| = p^n$ for some $n \in \mathbb{N}$. By Sylow's First Theorem G contains subgroups of orders $p^\alpha,\ 0 \leq \alpha \leq n$ and since these are the only divisors of p^n then the converse of Lagrange's Theorem holds for p-groups.

Return to Question 6.1 on P138

Solution 6.2

Show that every group of order 63 has a normal subgroup of order 7 and at least one subgroup of order 21.

$63 = 7 \times 9$, so G must have a subgroup of order 7 (Cauchy's Theorem). Let n_7 denote the number of these subgroups. Then, by the Sylow Theorems, $n_7 \equiv 1 \pmod 7$ so $n_7 = 1 + 7k$ for some $k \in \mathbb{Z}$, and $n_7 \mid 63$. These conditions are only satisfied for $n_7 = 1$, hence the subgroup is unique and so normal in G. Denote this subgroup N. Then we can factor G by N (as N is normal) and $|G/N| = 9$ which means that G/N is isomorphic to either $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$ (recall the result of Theorem 7.1). Each of these contains a subgroup H/N of order 3 (this is clear from the proof of the Correspondence Theorem - every subgroup of G/N has the form H/N for some H).

Then, by the Correspondence Theorem, H is a subgroup of G and since $|H/N| = 3$ and $|N| = 7$ so $|H| = 21$.

Return to Question 6.2 on P138

Solution 6.3

Use the Sylow Theorems to show that every group of order 980 has a normal subgroup of order 49, and subgroups of orders 245 and 98.

$980 = 2^2 \times 5 \times 7^2$, so every group of order 980 contains at least one Sylow 7-subgroup, N, of order 49. Let n_7 be the number of such subgroups. Then, by the third theorem n_7 is congruent to 1 modulo 7 so is of the form $7k + 1$ for some $k \in \mathbb{N}$ and also divides 980. Since n_7 divides 980 it must also divide 20 (since it cannot divide 49). Clearly, then, $n_7 = 1$ and so N is unique and, by the second theorem, is normal in G. Now $|G/N| = 20$, so G/N has a subgroup, H/N, of order 5 and a subgroup H'/N of order 2. Hence, H and H' are subgroups of G of orders 245 and 98 respectively.

Return to Question 6.3 on P138

Solution 6.4

Let G be a group of order pq, where p and q are primes, $p < q$, and p does not divide $q - 1$.

- ***(a) List the possible orders of such groups up to and including 40.***
- ***(b) Prove that G contains normal subgroups of orders p and q.***
- ***(c) Let $H = \langle x \rangle$ and $K = \langle y \rangle$ be normal subgroups of orders p and q respectively. Show that $x(yx^{-1}y^{-1}) \in H$ and $(xyx^{-1})y^{-1} \in K$. [Hint: the brackets are supposed to be helpful...]***
- ***(d) Deduce that $xy = yx$. [Hint: what is $H \cap K$?]***
- ***(e) Determine the order of the element xy in G and deduce that G is cyclic.***

(a) $3 \times 5 = 15$, $3 \times 11 = 33$, $5 \times 7 = 35$.

(b) Let n_p be the number of Sylow p-subgroups of order p and n_q be the number of Sylow q-subgroups of order q. By Sylow's Third Theorem, $n_p = 1 + kp$ for

some integer k, $n_q = 1 + mq$ for some integer m and both n_p and n_q divide pq. It then follows that both n_p and n_q are equal to 1, p or q (we dismiss the case pq since that is impossible as there is only one normal subgroup with the same order as the group, namely the group itself). Now, $n_p = 1 + kp \neq p$ and $n_q = 1 + mq \neq q$. Also, $p < q$ so $n_q \neq p$. If $n_p = q$ then $1 + kp = q \Rightarrow q - 1$ is a multiple of p and this is not allowed. Hence we have that $n_p = n_q = 1$ and, therefore, both Sylow subgroups are normal.

(c) Note that $x \in H$ and so $x^{-1} \in H$. Also, H is normal in G and so for all $y \in G$ we have that $yx^{-1}y^{-1} \in H$. Hence, since H is closed, $x(yx^{-1}y^{-1}) \in H$. Similarly, $y, y^{-1} \in K$ and K is normal in G, so for all $x \in G$ we have $(xyx^{-1}) \in K$ and, hence $(xyx^{-1})y^{-1} \in K$.

(d) Since all non-identity elements of H have order p and all non-identity elements of K have order q then it follows that $H \cap K = \{e\}$. But in (c) above we showed that $xyx^{-1}y^{-1} \in H$ and $xyx^{-1}y^{-1} \in K$, so $xyx^{-1}y^{-1} \in H \cap K$. Hence $xyx^{-1}y^{-1} = e$ and so

$$xy = (x^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx.$$

(e) We know that xy has order $1, p, q$ or pq. We also know that $H \cap K = \{e\}$. If xy has order 1 then $x = y^{-1} \in K$. This is a contradiction as $x \notin K$ since it has order p. If xy has order p then $xy \in H$ and so $xy = x^i$ for some $i \in \mathbb{Z}$. Then $y = x^{i-1} \in H$ which is a contradiction since $y \notin H$. If xy has order q then, similarly, $x \in K$ which is a contradiction. It then follows that xy has order pq and, since that is the order of G, then G must be cyclic.

Return to Question 6.4 on P139