MT4003 Groups

MRQ

April 27, 2018

Contents

Introduction

The purpose of this course is to introduce the detailed study of groups. These algebraic structures occur throughout mathematics and the physical sciences since they are the natural way to encode symmetry. They have been introduced in some previous courses (MT2505 primarily, but also MT1003), but here we shall pursue a much more in-depth study. In this course we shall encounter how to analyse the structure of a group — and what the term "structure" signifies — and consider how to classify groups.

Prerequisite

- MT2505

As Honours students, a higher level of mathematical maturity will be expected compared to the study of abstract algebra at 2000-level. Some of the content of MT2505 will be assumed (particularly an ability to manipulate permutations effectively), but some material will be discussed again in order to take the study deeper.

Overview of course structure

Groups: Definitions and examples.

Subgroups: Finding groups inside larger groups. How to describe new groups via generating sets. Theoretical restrictions on subgroups. This provides the first example of basic structure within groups.

Homomorphisms & quotient groups: Further examples of basic structure within groups. Quotients enable us to "factorise" a group into smaller groups. The Correspondence Theorem explains how the structure of a quotient group is related to that of the original group, and in particular why is it more simplified. The Isomorphism Theorems describe how the three aspects of structure (subgroups, homomorphisms, and quotients) relate to each other.

Constructing groups: How to build new groups from old. We shall use one of these constructions to describe a classification of all finite abelian groups.

Simple groups: These are the smallest building blocks from which to construct groups. We shall establish that the alternating group A_n is simple whenever $n \geqslant 5$.

The centre, conjugation, and commutators: Three useful tools which enable us to examine the structure of a group in more detail. We define two new classes of groups: soluble groups and nilpotent groups. These are more general than abelian groups but still more tractable to in-depth study than arbitrary groups. (My lecture notes

for *MT5824 Topics in Groups* cover these concepts in more detail. Other lecturers may cover other material instead in that module.)

Sylow's Theorem: The most important theorem in finite group theory. We shall illustrate this with numerous applications.

Final applications: Classification of groups of small order, namely order p, p^2, pq (p, q distinct primes) and order $\leqslant 15$.

Textbooks

Almost any textbook on group theory or abstract algebra is likely to cover the material in this course and provide a good supplement to the lecture course. The following are particularly recommended and are available for consultation in the library:

- R.B.J.T. Allenby, *Rings, Fields and Groups: An Introduction to Abstract Algebra*, Chapters 5 and 6. Second Edition: Butterworth-Heinemann, 1991; QA162.A6F91. First Edition: Edward Arnold, 1983; QA162.A6: Nicely written, reasonably modern, and fits this course well.
- W. Ledermann, *Introduction to Group Theory*, Oliver and Boyd, 1973; QA171.L43: Reasonably good fit to the course.
- John S. Rose, *A Course on Group Theory*, Dover, 1994, up to Chapter 6; QA171.R7: Reasonably detailed at the level we want; quite cheap.
- T.S. Blyth & E.F. Robertson, *Algebra Through Practice: A Collection of Problems in Algebra with Solutions, Book 5: Groups*, CUP, 1985; QA157.B6R7;5
- Thomas W. Hungerford, *Algebra*, Holt, Rinehart and Winston, 1974, Chapters 1 and 2; QA155.H8
- I. N. Herstein, *Topics in Algebra, Second Edition*, Wiley, 1975, Chapter 2; QA159.H4F76: A classic text on general algebra, though less easy for modern readers, also a little idiosyncratic in some definitions and notations.
- Derek J.S. Robinson, *A Course in the Theory of Groups, Second Edition*, Springer, 1996; QA171.R73: An advanced text, so goes quite rapidly through the material we cover in its early chapters.
- Joseph J. Rotman, *An Introduction to the Theory of Groups, Fourth Edition*, Springer, 1995; QA171.R7: Similarly advanced, though perhaps slightly less speedy in its coverage of our material.

Standard notation

The following are standard pieces of mathematical notation that will be used throughout the notes.

$x \in A$: x is an element of the set A.

$A = \{\, x \mid \ldots \}$: A is the set of those elements x that satisfy the condition present in the second part of the bracket (replacing "$\ldots$"). Also written $A = \{\, x\colon \ldots \}$ in some textbooks. The definitions that follow give examples of the use of this notation.

$A \cap B$: The intersection of A and B, defined by

$$A \cap B = \{\, x \mid x \in A \text{ and } x \in B \,\}.$$

$A \cup B$: The union of A and B, defined by

$$A \cup B = \{\, x \mid x \in A \text{ or } x \in B \,\}.$$

$A \setminus B$: The complement of B in A, defined by

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

This set therefore consists of all those elements of A which do not belong to B.

$A \times B$: The set of all ordered pairs (a, b) where $a \in A$ and $b \in B$; that is,

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

$\phi\colon A \to B$: ϕ is a *function* (or *mapping*) with *domain* A and *codomain* B. This means that we can apply ϕ to elements in A to produce as output elements of B. In this course, *we write maps on the right*, so that if a is an element of A, then the output when ϕ is applied to a is denoted by $a\phi$ (rather than $\phi(a)$ as would be common in other branches of mathematics, such as analysis, etc.).

Chapter 1

Definition and Examples of Groups

The axioms of a group

Abstract algebra is the study of sets with operations defined upon them. These operations in some sense mimic addition or multiplication of numbers. The following definition provides the operations we work with.

Definition 1.1 Let G be any (non-empty) set. A *binary operation* on G is a function

$$G \times G \to G.$$

We usually denote the image of a pair (x, y) under a binary operation by a notation such as $x * y$, $x \circ y$, $x + y$, xy, etc. This has the advantage of encouraging us to view binary operations as generalisations of our familiar arithmetic operations. For most of this course, we shall use *multiplicative notation* for our binary operations and so we write xy for the image of (x, y) under the operation; that is, xy denotes the effect of combining two elements x and y using the operation.

Definition 1.2 A *group* is a set G together with a binary operation such that

(i) the binary operation is *associative*, that is,

$$x(yz) = (xy)z \qquad \text{for all } x, y, z \in G;$$

(ii) there is an *identity element* 1 in G having the property

$$x1 = 1x = x \qquad \text{for all } x \in G;$$

(iii) every element x in G possesses an *inverse* x^{-1} also belonging to G having the property

$$xx^{-1} = x^{-1}x = 1.$$

Remarks:

(i) Some authors specify "closure" as an axiom for a group; that is, for all $x, y \in G$, the product xy belongs to G. Note, however, that this is built into the definition of a binary operation as a function $G \times G \to G$ that *takes values back in* G.

Nevertheless, when verifying that a particular example is a group, we should not ignore that establishing we have a binary operation is part of the steps. So, to be explicit, when checking the axioms of a group, we need to check for (1) closure (that we do indeed have a binary operation defined on our set), (2) associativity, (3) existence of identity, and (4) existence of inverses.

(ii) As we are using multiplication notation, we often refer to the binary operation as the *group multiplication*. There are, however, some groups where it is more natural to use addition as the binary operation (see, for example, Example 1.5 below) and we adjust our terminology appropriately.

(iii) Some authors use e to denote the identity element in a group. These lectures follow the more common (and perhaps slightly more sophisticated) approach of using 1. We shall rely on the experience of the student to be able to distinguish from the context between the identity element of a group and the integer 1.

It follows by repeated use of the associativity axiom that any bracketing of a product $x_1x_2\dots x_n$ of elements $x_1, x_2, \dots, x_n$ in a group G can be converted to any other bracketing without changing the value of the product. In view of this, we can safely omit the brackets in any such product and still know that we have specified a unique element in our group by the product.

For example,

$$\big(x_1(x_2x_3)\big)x_4 = \big((x_1x_2)x_3\big)x_4 = (x_1x_2)(x_3x_4).$$

What should be noticed is that the order of the elements in a product does matter. The axioms of a group do not tell us any clear link between the products

$$x_1x_2x_3, \quad x_1x_3x_2, \quad x_2x_1x_3, \quad \text{etc.}$$

and there are examples of groups where such products are all different. We give a special name for groups where we can reorder the elements without changing the value of a product.

Definition 1.3 An *abelian* group is a group G where the binary operation is *commutative*, that is,

$$xy = yx \qquad \text{for all } x, y \in G.$$

We shall often make statements such as "G is a group" to mean that G is a set with a binary operation defined upon it satisfying the axioms of Definition 1.2. This illustrates how we often do not distinguish between a group and the underlying set upon which the binary operation is defined. We take this into account when making the following definition.

Definition 1.4 Let G be a group. The *order* of G, denoted by $|G|$, is the number of elements in the underlying set on which our group is defined.

A *finite group* is a group whose order is a finite number, while an *infinite group* is a group G for which $|G| = \infty$.

Examples of groups

We now illustrate how groups arise in multiple settings across mathematics by providing a range of examples.

Example 1.5 (Groups of numbers) Consider the set $\mathbb{Z}$ of all integers. This forms a group under addition $+$, as we shall now show. The sum of two integers is an integer, so addition is a binary operation on $\mathbb{Z}$. Our familiarity with addition of numbers tells us

$$x + (y + z) = (x + y) + z \qquad \text{for all } x, y, z \in \mathbb{Z}.$$

The identity element is 0, since

$$x + 0 = 0 + x = x \qquad \text{for all } x \in \mathbb{Z}.$$

The inverse of x is $-x$, since

$$x + (-x) = (-x) + x = 0 \qquad \text{for all } x \in \mathbb{Z}.$$

Moreover, $\mathbb{Z}$ is an abelian group under addition, since

$$x + y = y + x \qquad \text{for all } x, y \in \mathbb{Z}.$$

In the same way, the rational numbers $\mathbb{Q}$ forms an abelian group under addition, the real numbers $\mathbb{R}$ forms an abelian group under addition, and the complex numbers $\mathbb{C}$ forms an abelian group under addition.

However, none of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ form groups under multiplication. [Exercise: Show that 0 has no inverse in any of these sets with respect to multiplication. Indeed, in $\mathbb{Z}$ only ± 1 have multiplicative inverses.]

Removing 0 from some of these sets does yield a multiplicative group. The set of non-zero rationals $\mathbb{Q} \setminus \{0\}$ is a group with respect to multiplication. For we know that the product of two non-zero rational numbers is a rational number, so multiplication is a binary operation on $\mathbb{Q} \setminus \{0\}$. Multiplication is associative:

$$x(yz) = (xy)z \qquad \text{for all } x, y, z \in \mathbb{Q} \setminus \{0\}.$$

The identity element is 1:

$$x1 = 1x = x \qquad \text{for all } x \in \mathbb{Q} \setminus \{0\}.$$

The inverse of $x = m/n$ is $1/x = n/m$ for $x \neq 0$:

$$x \cdot \tfrac{1}{x} = \tfrac{1}{x} \cdot x = 1.$$

Moreover, $\mathbb{Q} \setminus \{0\}$ forms an abelian group under multiplication since $xy = yx$ for all $x, y \in \mathbb{Q},\ x, y \neq 0$.

In the same way, the non-zero real numbers $\mathbb{R} \setminus \{0\}$ and the non-zero complex numbers $\mathbb{C} \setminus \{0\}$ form abelian groups under multiplication.

Example 1.6 (Symmetric groups) A common way to produce groups is as sets of bijective functions (often those satisfying nice properties) under composition. In algebra, it is most common to write functions *on the right* so that when composing them we can read from left to right. Thus if X is a set, the *composite* of two functions $\alpha\colon X \to X$ and $\beta\colon X \to X$ is the function $\alpha\beta\colon X \to X$ given by

$$x(\alpha\beta) = (x\alpha)\beta \qquad \text{for each } x \in X.$$

Lemma 1.7 *Composition of functions is associative.*

PROOF: Let $\alpha, \beta, \gamma \colon X \to X$ be functions defined on X. We calculate the effect of $\alpha(\beta\gamma)$ and $(\alpha\beta)\gamma$ on an element of X:

$$x\big(\alpha(\beta\gamma)\big) = (x\alpha)(\beta\gamma) = \big((x\alpha)\beta\big)\gamma$$

and

$$x\big((\alpha\beta)\gamma\big) = \big(x(\alpha\beta)\big)\gamma = \big((x\alpha)\beta\big)\gamma.$$

Hence $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. □

A *permutation* of the set X is a function $\sigma \colon X \to X$ that is *bijective*; that is, it is

injective: if $x, y \in X$ and $x\sigma = y\sigma$, then $x = y$; and

surjective: if $y \in X$, then there is some $x \in X$ such that $x\sigma = y$.

This guarantees we can find an inverse σ^{-1} of σ that has the effect of "undoing" the application of σ. Thus

$$\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma \tag{1.1}$$

where $\varepsilon = \varepsilon_X$ is the identity map on X $(\varepsilon \colon x \mapsto x$ for all $x \in X)$.

The set of all permutation on X forms a group under the composition of permutations. This is called the *symmetric group* and is denoted S_X or $\mathrm{Sym}(X)$. Associativity of composition is provided by Lemma 1.7; the identity element is the identity map $\varepsilon = \varepsilon_X$:

$$\varepsilon\sigma = \sigma\varepsilon = \sigma \qquad \text{for all } \sigma \in S_X;$$

and the inverse of a permutation σ as a function is the inverse in the group (see Equation (1.1) above).

Although we have been careful to use ε to denote our identity element in S_X to emphasise that it is a mapping, we will frequently follow the usual convention of writing 1 for the identity element in our group. (Sometimes even when 1 happens also to denote an element of X. Though in this case, context will always make the difference clear!)

We are particularly interested in the symmetric group S_X in the case when $X = \{1, 2, \ldots, n\}$. We then write S_n for the *symmetric group of degree* n consisting of all permutations of $X = \{1, 2, \ldots, n\}$. A permutation of this X can be written in two-row notation where the elements of X are listed in the top row and below i we write the image $i\sigma$. For example,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \text{and} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

are two permutations from S_4. Their product $\sigma\tau$ is calculated by first applying σ to an element of $X = \{1, 2, 3, 4\}$ and then applying τ. (Remember that we are writing maps on the right!) Thus

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

The inverse of σ is calculated by undoing the effect of applying σ; i.e., interchanging the rows of σ and reordering the columns to get the result in the correct form:

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

Let us also calculate

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix},$$

so $\sigma\tau \neq \tau\sigma$ and we conclude that S_4 is a non-abelian group. Similar examples show that S_n is non-abelian for $n \geqslant 3$, while it is easy to check that S_1 and S_2 are abelian.

An alternative — and more compact — way of denoting a permutation is to write it as a product of disjoint cycles. The *cycle*

$$(i_1\ i_2\ \ldots\ i_r)$$

is the permutation that maps i_1 to i_2, i_2 to i_3, $\ldots$, i_{r-1} to i_r, i_r to i_1, and fixes all other points of X (that is, all those not listed in the cycle). The above cycle is said to be of *length* r (or is called an *r-cycle*) and two cycles are called *disjoint* if no point of X is moved by both of them (essentially when there is no point in common listed in the two cycles).

If

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix},$$

then

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

expresses σ as a product of disjoint cycles. (Note that a 1-cycle is the identity element.) We record as a reminder:

Theorem 1.8 *Every permutation of $X = \{1, 2, \ldots, n\}$ can be written (in an essentially unique way) as a product of disjoint cycles.*

Here "essentially unique" refers to the obvious rearrangements that do not change a product of disjoint cycles. Firstly, a cycle can be begun at any point within it, so cycling around the entries in a cycle do not change the product. Secondly, disjoint cycles commute, so we can reorder them in a product without changing the result.

A 2-cycle is also called a *transposition*. Since

$$(i_1\ i_2\ \ldots\ i_r) = (i_1\ i_2)(i_1\ i_3)\ldots(i_1\ i_r),$$

we conclude that every cycle can be written as a product of transpositions. We then deduce:

Proposition 1.9 *Every permutation in S_n is a product of transpositions.*

There is no claim here that such a decomposition is in any way unique.

This completes our first stage in the reminder on permutations. More facts about them will arrive in due course. We continue this section by introducing some further examples of groups.

Example 1.10 (General linear groups) Let F be a field and consider the set of $n \times n$ matrices with entries from F. Matrix multiplication is associative:

$$A(BC) = (AB)C \qquad \text{for all } n \times n \text{ matrices } A,\ B \text{ and } C.$$

The identity matrix I (with 1 in every diagonal entry and 0 elsewhere) has the property that

$$IA = AI = A \qquad \text{for all } n \times n \text{ matrices } A.$$

If $\det A \neq 0$, then A has an inverse A^{-1} such that

$$AA^{-1} = A^{-1}A = I.$$

The *general linear group* $\mathrm{GL}_n(F)$ (or $\mathrm{GL}(n, F)$ in some books) consists of all $n \times n$ matrices with entries from F having non-zero determinant. The above observations ensure this forms a group under matrix multiplication. This is a non-abelian group provided $n \geqslant 2$.

Cayley tables

One way to present a group is to specify completely its multiplication via a *Cayley table* (or *multiplication table*). In this, the group elements are listed along the side and along the top of the table and the product xy is written in the entry with row label x and column label y.

Example 1.11 (Klein 4-group) The *Klein* 4*-group*, denoted by V_4 (for *viergruppe*) in some books and K_4 in others, is the group with elements $\{1, a, b, c\}$ and multiplication as follows:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

From this table, we can see that 1 is the identity element and that

$$1^2 = a^2 = b^2 = c^2 = 1,$$

so every element equals its own inverse:

$$1^{-1} = 1, \quad a^{-1} = a, \quad b^{-1} = b, \quad c^{-1} = c.$$

Verifying associativity is not so easy. In this case, it is reasonably straightforward to check

$$x(yz) = (xy)z$$

for each of the $4^3 = 64$ choices of x, y and z, by reducing the number of choices (e.g., if one of x, y or z is the identity then the equation becomes easier to verify).

Advantages of Cayley tables

- Easy to understand.
- Identity and inverses relatively easy to spot.
- Whether or not the group is abelian is relatively easy to spot (look for symmetry across the diagonal).

Disadvantages of Cayley tables

- Only really available for finite groups and only those which are small enough to fit on the piece of paper.
- Associativity hard to recognise.
- Very difficult to extract useful information about the group.

One of the things we shall discover in this course is how to determine useful information about a group to replace the cumbersome Cayley table.

Example 1.12 (Quaternion group) The *quaternion group* Q_8 has elements

$$1, -1, i, -i, j, -j, k, -k,$$

where the first four elements are the usual complex numbers, while j and k behave similarly to the imaginary square root i of -1. The multiplication is given by

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

The Cayley table is:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

What we try to do in group theory

The lofty aim, though perhaps also naive, deluded or even impossible, is to classify all groups; that is, answer the question:

> Given a set of properties, can we list all groups satisfying those properties?

This is a ridiculously impossible question to answer in any form of generality. For example, it is now (from 1997) known that there are 10 494 213 essentially different groups with 512 elements and we are unlikely to write down or work with a list of 10 million groups. Nevertheless, the above aim is behind the general study of groups. We hope to provide some sort of analysis on the structure of or restrictions on groups satisfying particular properties.

In this context, we need to give some thought about what "essentially the same" means for a group. A natural way to produce groups that are in reality identical but superficially different is to write down a Cayley table for a group, but then replace each element by a different symbol. For example,

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

are surely describing essentially the same group. In view of this we make the following definition:

Definition 1.13 Let G and H be two groups (both with multiplicatively written binary operation). An *isomorphism* $\phi\colon G \to H$ is a bijective map such that

$$(xy)\phi = (x\phi)(y\phi) \qquad \text{for all } x, y \in G.$$

We say that G and H are *isomorphic*, written $G \cong H$, if there is an isomorphism from G to H.

Two groups that are isomorphic are essentially the same and really only differ in the labelling of the elements. If $\phi\colon G \to H$ is an isomorphism, then it first gives a one-one correspondence between the elements of G and of H. Second if two elements $x, y \in G$ multiply to an element $z = xy$, then the corresponding elements $x\phi$ and $y\phi$ multiply in H to $z\phi = (xy)\phi = (x\phi)(y\phi)$. Consequently, the multiplication in G and in H are essentially the same, if we were to write out the Cayley tables, they would look the same, and so the groups should be viewed as the same.

For the future, when attempting to classify groups, we only ever classify up to isomorphism and only list one group of each isomorphism-type. It is unnecessary to list a group that is isomorphic to one we already know. We will also want to ensure that any definitions we may make are *group theoretical properties*, that is, if G and H are isomorphic groups then any definition applies in the same way to both groups. So if G has a particularly property, then so should H. If G does not have a property, then H should not.

Basic properties of group elements

So far we have introduced the definition of a group, presented some examples and said that we wish to classify groups up to isomorphism. To make a start on this task, we first establish some basic properties of the elements of a group before we move on in future sections to consider what we mean by the structure of a group.

Lemma 1.14 *Let G be a group.*

(i) *The identity element 1 of G is unique.*

(ii) *Each element x in G has a unique inverse x^{-1}.*

(iii) $1^{-1} = 1$.

(iv) *If $x \in G$, then $(x^{-1})^{-1} = x$.*

(v) *If $x, y \in G$, then $(xy)^{-1} = y^{-1}x^{-1}$.*

Proof: (i) Suppose e is also an identity element in G. Then

$$xe = ex = x \qquad \text{for all } x \in G,$$

while

$$x1 = 1x = x \qquad \text{for all } x \in G.$$

Taking $x = 1$ in the first and $x = e$ in the second gives

$$1 = 1e = e.$$

(ii) Suppose x^{-1} and y are both inverses for x. So

$$xx^{-1} = x^{-1}x = 1 = xy = yx.$$

Then

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

and

$$(x^{-1}x)y = x^{-1}(xy) = x^{-1}1 = x^{-1}.$$

Therefore

$$x^{-1} = y.$$

(iii) Since 1 is the identity element, $11 = 1$. Hence 1 is the unique element y satisfying $1y = y1 = 1$; that is, $1^{-1} = 1$.

(iv) Exercise on Problem Sheet I.

(v)

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1x^{-1} = xx^{-1} = 1$$

and

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}1y = y^{-1}y = 1.$$

Hence $(xy)^{-1} = y^{-1}x^{-1}$. □

Since we can multiply elements in a group, we can take a single element x of a group and multiply it by itself a number of times to form powers of x.

Definition 1.15 Let G be a group and $x \in G$. If n is a positive integer, we define

$$x^n = \underbrace{xx\ldots x}_{n \text{ times}}$$
$$x^{-n} = (x^{-1})^n = \underbrace{x^{-1}\,x^{-1}\ldots x^{-1}}_{n \text{ times}}$$

and

$$x^0 = 1.$$

As the binary operation in our group is associative, we do not have to specify the bracketing in the product $xx\ldots x$. Hence x^n (and so also x^{-n}) is a uniquely specified element of the group.

Proposition 1.16 (Power Laws) *Let G be a group, $x \in G$ and $m, n \in \mathbb{Z}$. Then*

(i) $x^m\,x^n = x^{m+n}$;

(ii) $(x^m)^n = x^{mn}$.

Proof: Exercise, based on analysis of the signs of m, n, etc. □

The order of an element

We can use the powers of x to make a useful definition. Let G be a group, x be an element of G and consider the set of all powers of x:

$$\ldots, x^{-2}, x^{-1}, 1, x, x^2, x^3, \ldots \tag{1.2}$$

If the elements in this list have repeats (as must be the case if G is a finite group), then there exist $i, j \in \mathbb{Z}$ with $i < j$ and

$$x^i = x^j.$$

Multiply by the inverse of x^i, that is x^{-i}, to find

$$x^{j-i} = x^j x^{-i} = x^i x^{-i} = x^{i-i} = x^0 = 1.$$

Hence there exists a positive integer m such that $x^m = 1$.

We therefore make the following definition:

Definition 1.17 Let G be a group and x be an element of G. We say that x has *finite order* if there exists a positive integer m such that $x^m = 1$. If not, we say x has *infinite order*.

In the case that x has finite order, the *least* positive integer m satisfying $x^m = 1$ is called the *order* of x and is denoted by $o(x)$ (or by $|x|$ in some books).

In summary,

- the list (1.2) has repeats if and only if $o(x) < \infty$;
- the elements in the list (1.2) are distinct if and only if $o(x) = \infty$;
- in a finite group, every element has finite order.

What we shall discover is that if G is finite, then $o(x)$ *divides* $|G|$ for all $x \in G$. This will depend upon the theory of subgroups, developed in the next section.

Example 1.18 Consider the case of $G = S_3$. For $\sigma = (1\ 2\ 3)$, we calculate

$$(1\ 2\ 3)^2 = (1\ 3\ 2), \qquad (1\ 2\ 3)^3 = 1,$$

so

$$o\big((1\ 2\ 3)\big) = 3.$$

For $\tau = (1\ 2)$, we calculate

$$(1\ 2)^2 = 1,$$

so

$$o\big((1\ 2)\big) = 2.$$

For a general r-cycle

$$\sigma = (i_1\ i_2\ \ldots\ i_r)$$

in an arbitrary symmetric group S_n of degree n, we can calculate the effect of successive powers of σ on the points of $X = \{1, 2, \ldots, n\}$:

$$i_j\sigma = i_{j+1}, \quad i_j\sigma^2 = i_{j+2}, \quad \ldots, \quad i_j\sigma^{r-1} = i_{j-1}, \quad i_j\sigma^r = i_j$$

Hence σ^r fixes all points in X (since σ fixes all points of X other than i_1, i_2, $\ldots$, i_r). Thus $\sigma^r = 1$ and all lower powers of σ are non-identity. Thus

$$o(\sigma) = o\big((i_1\ i_2\ \ldots\ i_r)\big) = r.$$

Our final result for this section is:

Lemma 1.19 *Let G be a group and let x be an element in G of finite order. Then*

$$x^n = 1 \qquad \textit{if and only if} \qquad o(x) \textit{ divides } n.$$

PROOF: If $o(x)$ divides n, say $n = o(x) \cdot m$, then

$$x^n = (x^{o(x)})^m = 1^m = 1.$$

Conversely, suppose $x^n = 1$. Divide n by $o(x)$ to obtain a quotient and a remainder:

$$n = q \cdot o(x) + r \qquad \text{where } 0 \leqslant r < o(x).$$

Then

$$1 = x^n = x^{q \cdot o(x) + r} = (x^{o(x)})^q x^r = 1^q x^r = x^r.$$

Hence $x^r = 1$. However, by definition, $o(x)$ is the *smallest* positive integer such that $x^{o(x)} = 1$ and here we have $0 \leqslant r < o(x)$. This forces $r = 0$ and so $n = q \cdot o(x)$; that is, $o(x)$ divides n. □

This brings us to the end of our introductory section. If we are to make progress in our goal of studying and classifying groups, then we have to move beyond the consideration of elements alone in a group. It is in view of this that we move to more "structural" considerations. The first example of this is subgroups in the next section. We shall see that the presence of smaller groups appearing inside a large group places considerable rigidity upon it.

Chapter 2

Subgroups

As we observed in the previous section, the use of the Cayley table is somewhat limited and we need to find aspects of "structure" in groups to enable us to actually make progress in their study. The first example of something providing structure is the concept of a subgroup (a copy of a smaller group found within another group).

Definition 2.1 Let G be a group. A *subgroup* of G is a subset H of G which is itself a group under the multiplication of G. We write $H \leqslant G$ to denote that H is a subgroup of G.

It is more useful to have a precise characterisation of this condition.

Theorem 2.2 *The following are equivalent for a subset H of a group G:*

(i) *H is a subgroup of G;*

(ii) *H is a non-empty subset of G such that $xy \in H$ and $x^{-1} \in H$ whenever $x, y \in H$;*

(iii) *H is a non-empty subset of G such that $xy^{-1} \in H$ whenever $x, y \in H$.*

PROOF: We show that (i) and (ii) are equivalent and leave the equivalence of (iii) to Problem Sheet II.

(i) $\Rightarrow$ (ii): The binary operation on G must induce a binary operation on the subgroup H, so $xy \in H$ whenever $x, y \in H$. Note that H and G must share the same identity element, since the identity element e of H satisfies $e^2 = e$ and multiplying by its inverse (as an element of G) gives $e = 1$. Therefore the inverse of an element x in H must also be an inverse for it as an element of G. Since the inverse in G is unique, we conclude $x^{-1} \in H$ for all $x \in H$.

(ii) $\Rightarrow$ (i): Since $xy \in H$ for all $x, y \in H$, we obtain a binary operation defined on H. It is associative since $x(yz) = (xy)z$ for all $x, y, z \in G$ and therefore certainly for all $x, y, z \in H$.

By assumption, H is non-empty, so contains some element a. Then $a^{-1} \in H$ by hypothesis. Then $aa^{-1} \in H$ by assumption; that is, $1 \in H$. Since $1x = x1 = x$ for all $x \in H$ (as this holds for $x \in G$), we conclude that 1 is also the identity element for H.

Finally by hypothesis, each $x \in H$ has an inverse in H, namely the element x^{-1}, which lies in H. Thus H forms a group under the multiplication in G, so $H \leqslant G$. $\square$

Example 2.3 If G is any group, the sets $\{1\}$ and G are subgroups of G. The former is called the *trivial subgroup* of G and is also denoted $\mathbf{1}$.

VERIFICATION: $1 \cdot 1 = 1$ and $1^{-1} = 1$, so $\{1\}$ satisfies the condition to be a subgroup. It is immediate that G satisfies the condition. □

Example 2.4 It follows straight from Definition 2.1 that as additive groups, $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$.

Recall from Proposition 1.9 that every permutation in S_n can be written as a product of transpositions. It is a theorem (proved in *MT2505* but omitted here) that a permutation can either be written as a product of an even number of transpositions or an odd number of transpositions, but never both. We may therefore make the following definition:

Definition 2.5 A permutation $\sigma \in S_n$ is called *even* (respectively, *odd*) if it can be written as a product of an even number (resp., odd number) of transpositions. The set of all even permutations in S_n is called the *alternating group* of degree n and is denoted by A_n.

Our comment above ensures that a permutation is either even or odd, but never both.

Theorem 2.6 *The alternating group A_n is a subgroup of the symmetric group S_n of degree n.*

PROOF: There certainly are permutations that are even (for example, just multiply any two transpositions), so A_n is non-empty. If $\alpha, \beta \in A_n$, say $\alpha = \sigma_1\sigma_2 \dots \sigma_{2k}$ and $\beta = \tau_1\tau_2 \dots \tau_{2\ell}$ as products of even numbers of transpositions, then

$$\alpha\beta = \sigma_1\sigma_2 \dots \sigma_{2k}\tau_1\tau_2 \dots \tau_{2\ell}$$

is a product of $2(k + \ell)$ transpositions, so is even. Equally

$$\begin{aligned} \alpha^{-1} &= (\sigma_1\sigma_2 \dots \sigma_{2k})^{-1} \\ &= \sigma_{2k}^{-1}\sigma_{2k-1}^{-1} \dots \sigma_2^{-1}\sigma_1^{-1} \\ &= \sigma_{2k}\sigma_{2k-1} \dots \sigma_2\sigma_1 \end{aligned}$$

is a product of $2k$ transpositions, so is even. Hence

$$\alpha\beta, \alpha^{-1} \in A_n \qquad \text{for all } \alpha, \beta \in A_n,$$

so $A_n \leqslant S_n$. □

Generating sets

We shall now present a way of defining subgroups of a group. This is analogous to the concept of a spanning set in a vector space. We first start with an observation about subgroups.

Theorem 2.7 *Let G be a group and $\{ H_i \mid i \in I \}$ be a set of subgroups of G (indexed by some set I). Then the intersection*

$$\bigcap_{i \in I} H_i$$

is also a subgroup of G.

PROOF: Let us write $H = \bigcap_{i \in I} H_i$. Since each H_i is a subgroup, they all contain the identity element 1 of G. Hence $1 \in H$, so H is non-empty. Now let $x, y \in H$. Then $x, y \in H_i$ for each i, so by Theorem 2.2, we see that $xy, x^{-1} \in H_i$ for each i. Therefore $xy, x^{-1} \in H$, and Theorem 2.2 tells us that H is a subgroup of G. □

(As a side comment, it is very rare for the union of subgroups to be a subgroup.)

Definition 2.8 Let G be a group and X be a subset of G. The *subgroup generated by* X, denoted by $\langle X \rangle$, is the intersection of all subgroups of G containing X.

Remarks:

(i) There is at least one subgroup of G containing X, namely G itself. So our definition makes sense.

(ii) Theorem 2.7 guarantees that $\langle X \rangle$ is a subgroup of G. Moreover, every subgroup we are intersecting contains X, so we conclude $X \subseteq \langle X \rangle$. That is, $\langle X \rangle$ is a subgroup of G containing the set X.

In fact, we can do better than (ii) above. If H is *any* subgroup of G containing X, then H is one of the subgroups we intersect and so by construction, $\langle X \rangle \leqslant H$. This establishes:

Lemma 2.9 *The subgroup $\langle X \rangle$ generated by X is the smallest subgroup of G containing X.*

This is "smallest" in the sense of containment: $\langle X \rangle$ is a subgroup of G and if $X \subseteq H \leqslant G$, then $\langle X \rangle \leqslant H$.

The problem with our Definition 2.8 is that, although it guarantees the existence of this subgroup, it provides us with nothing concrete in terms of the description of $\langle X \rangle$ or its elements. The following is somewhat more useful and gives a better feel for what "generating a subgroup" actually means.

Theorem 2.10 *Let G be a group and X be a non-empty subset of G. The subgroup $\langle X \rangle$ generated by X is the set of all possible products of elements of X and their inverses:*

$$\langle X \rangle = \{\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N},\, x_i \in X,\, \varepsilon_i = \pm 1 \text{ for } i = 1, 2, \dots, n \,\}.$$

PROOF: Let us write H for the set appearing on the right-hand side of the above equation. First $\langle X \rangle$ is a subgroup of G, so is closed under products and inverses, and it contains X. Therefore $\langle X \rangle$ must contain all the products that appear in H, so

$$H \subseteq \langle X \rangle.$$

On the other hand, H is non-empty (it contains X). If $g, h \in H$, say

$$g = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m} \qquad \text{and} \qquad h = y_1^{\eta_1} y_2^{\eta_2} \dots y_n^{\eta_n},$$

where $m, n \in \mathbb{N}$, $x_i, y_j \in X$ and $\varepsilon_i, \eta_j = \pm 1$ for all i and j, then

$$gh = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m} y_1^{\eta_1} y_2^{\eta_2} \dots y_n^{\eta_n} \in H$$

and

$$g^{-1} = x_m^{-\varepsilon_m} x_{m-1}^{-\varepsilon_{m-1}} \dots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1} \in H.$$

Hence H is a subgroup of G. Since this subgroup contains X, we conclude (by Lemma 2.9) that

$$\langle X \rangle \leqslant H.$$

Hence

$$\langle X \rangle = H,$$

as required. □

Let us consider the special case of Definition 2.8 and Theorem 2.10 when the set X contains a single element: $X = \{x\}$. Theorem 2.10 then says

$$\langle x \rangle = \{\, x^n \mid n \in \mathbb{Z} \,\},$$

so the subgroup generated by the element x consists of all powers of x. (As a consequence, this guarantees that the set of all powers of the element x is a subgroup of whichever group we are working within.) Note that we tend to drop extraneous brackets and simply write $\langle x \rangle$ rather than $\langle \{x\} \rangle$.

We make the following definition:

Definition 2.11 Let G be a group. We say that G is *cyclic* if there exists some $x \in G$ such that $G = \langle x \rangle$ and then call this x a *generator* of G.

More generally, if x is an element of a group G, we call $\langle x \rangle$ the *cyclic subgroup generated by* x.

Example 2.12 Consider the group $\mathbb{Z}$ of integers under addition. Since we are *adding* elements in this group, powers become *multiples*. In particular

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = n.$$

Hence

$$\mathbb{Z} = \langle 1 \rangle.$$

There is a tight link between the subgroup generated by an element x of a group G and the order of the element x. Recall first that if x has infinite order, then the powers x^n, for $n \in \mathbb{Z}$, of x are all distinct. As a consequence

if x has infinite order, then $\langle x \rangle$ contains infinitely many elements,

namely the distinct powers of x.

On the other hand, suppose x has finite order. Recall that $o(x)$ is the least positive integer satisfying $x^{o(x)} = 1$. If n is any integer, divide it by $o(x)$ to obtain a quotient and remainder:

$$n = q \cdot o(x) + r \qquad \text{where } 0 \leqslant r < o(x).$$

Then

$$x^n = x^{q \cdot o(x) + r} = (x^{o(x)})^q x^r = x^r.$$

So every power of x equals x^r for some $r \in \{0, 1, \ldots, o(x) - 1\}$ and so

$$\langle x \rangle = \{1, x, x^2, \ldots, x^{o(x)-1}\}.$$

Moreover the powers listed in the set above are distinct. For if it were the case that $x^i = x^j$ for some i, j with $0 \leqslant i < j \leqslant o(x) - 1$, then

$$x^{j-i} = 1$$

and here $0 < j - i < o(x)$. This would contradict the definition of $o(x)$.

Putting the above together, we have established the following:

Proposition 2.13 *Let G be a group and $x \in G$. Then*

$$|\langle x \rangle| = o(x).$$

□

(For when $o(x) = \infty$, the subgroup generated by x is infinite. When $o(x) < \infty$, the subgroup generated by x contains precisely $o(x)$ distinct powers of x.)

Notice also that if $o(x) = k$ is finite (as would happen for an element in a finite group), then

$$x^k = 1$$

so

$$x^{-1} = x^{k-1}.$$

This means that we can replace x^{-1} by a product of copies of x. We can then immediately deduce the following from Theorem 2.10.

Corollary 2.14 *Let G be a* finite *group and X be a non-empty subset of G. Then*

$$\langle X \rangle = \{\, x_1 x_2 \dots x_n \mid n \in \mathbb{N},\ \ x_i \in X \text{ for } i = 1, 2, \dots, n \,\}.$$

□

The generation algorithm

In view of Corollary 2.14, we can find all the elements in the subgroup $\langle X \rangle$ generated by a subset X of a finite group by successively finding ever longer products of the elements in X and stopping when multiplying the products we have found by the elements in X produces no new elements. This is what is done by the following algorithm for computing all the elements in the subgroup of a finite group G generated by the set $X = \{x_1, x_2, \dots, x_m\}$.

Initialise: Take $A = \{1\}$.

For each $a \in A$:

Calculate ax_1, ax_2, …, ax_m

If any ax_i is not currently listed in A

Append this ax_i to A.

Repeat until no new products are generated.

This calculates $\langle X \rangle$ since it computes a set A of products of the x_1, x_2, …, x_m such that there are no such products not in the set A. Thus when we finish $\langle X \rangle = A$.

Example 2.15 *Calculate the elements in the subgroup H of S_8 generated by the permutations*

$$\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \qquad \textit{and} \qquad \tau = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6).$$

SOLUTION: We apply the above algorithm:

$$\begin{aligned}
a_1 &= 1 \\
a_2 = a_1\sigma &= (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \\
a_3 = a_1\tau &= (1\ 5\ 3\ 7)(2\ 8\ 4\ 6) \\
a_4 = a_2\sigma &= (1\ 3)(2\ 4)(5\ 7)(6\ 8) \\
a_5 = a_2\tau &= (1\ 8\ 3\ 6)(2\ 7\ 4\ 5) \\
a_6 = a_3\sigma &= (1\ 6\ 3\ 8)(2\ 5\ 4\ 7) \\
a_3\tau &= (1\ 3)(2\ 4)(5\ 7)(6\ 8) = a_4 \\
a_7 = a_4\sigma &= (1\ 4\ 3\ 2)(5\ 8\ 7\ 6) \\
a_8 = a_4\tau &= (1\ 7\ 3\ 5)(2\ 6\ 4\ 8) \\
a_5\sigma &= (1\ 5\ 3\ 7)(2\ 8\ 4\ 6) = a_3 \\
a_5\tau &= (1\ 4\ 3\ 2)(5\ 8\ 7\ 6) = a_7 \\
a_6\sigma &= (1\ 7\ 3\ 5)(2\ 6\ 4\ 8) = a_8 \\
a_6\tau &= (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) = a_2 \\
a_7\sigma &= (1)(2)(3)(4)(5)(6)(7)(8) = 1 = a_1 \\
a_7\tau &= (1\ 6\ 3\ 8)(2\ 5\ 4\ 7) = a_6 \\
a_8\sigma &= (1\ 8\ 3\ 6)(2\ 7\ 4\ 5) = a_5 \\
a_8\tau &= (1)(2)(3)(4)(5)(6)(7)(8) = 1 = a_1
\end{aligned}$$

So $H = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$, a group of order 8. (In fact, by constructing the multiplication table — and putting the elements in the right order — we can see that this group H is isomorphic to the quaternion group Q_8.) □

Dihedral groups

Further to the example above, it is a theorem (that we shall meet in due course) that every finite group occurs as the subgroup of some symmetric group S_n (or, more precisely, every finite group is isomorphic to a subgroup of some S_n). One important collection of groups is most easily described by providing generators for them as subgroups of various S_n.

Definition 2.16 Let $n \geqslant 3$. The *dihedral group of order* $2n$, denoted by D_{2n} (or by D_n in roughly half the textbooks), is the subgroup of S_n generated by

$$\alpha = (1\ 2\ 3 \cdots n) \qquad \text{and}$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & n & n-1 & \cdots & 2 \end{pmatrix} = (2\ n)(3\ n{-}1)\cdots(i\ n{+}2{-}i)\cdots .$$

The basic properties of the dihedral groups are as follows:

Theorem 2.17 *Let $n \geqslant 3$. The following statements are true for the dihedral group D_{2n} of order $2n$:*

(i) $o(\alpha) = n,\ \ o(\beta) = 2.$

(ii) $\beta\alpha = \alpha^{-1}\beta.$

(iii) $D_{2n} = \{\, \alpha^i\beta^j \mid 0 \leqslant i \leqslant n-1,\ 0 \leqslant j \leqslant 1 \,\}$ *and* $|D_{2n}| = 2n.$

(iv) *D_{2n} is non-abelian.*

PROOF: (i) is obvious and (ii) is simply a matter of direct calculation. If $3 \leqslant i \leqslant n$, we calculate

$$i\beta\alpha = (n+2-i)\alpha = n+3-i$$
$$i\alpha^{-1}\beta = (i-1)\beta = (n+2)-(i-1) = n+3-i.$$

The values for $i = 1$ and 2 are calculated separately and we conclude

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n-1 & n \\ 2 & 1 & n & n-1 & \cdots & 4 & 3 \end{pmatrix} = \alpha^{-1}\beta.$$

(iii) $D_{2n} = \langle \alpha, \beta \rangle$, so by Corollary 2.14 every element in D_{2n} is a product of these two permutations. Consider such a product. Whenever we see $\beta\alpha$ occurring, we can replace it by $\alpha^{-1}\beta = \alpha^{n-1}\beta$. By repeating this procedure, we can move all the occurrences of α to the left of all the occurrences of β. Thus, every element in D_{2n} can be written in the form $\alpha^i\beta^j$. Since $o(\alpha) = n$ and $o(\beta) = 2$, we can always take i and j in the ranges $0 \leqslant i \leqslant n-1,\ \ 0 \leqslant j \leqslant 1$. Hence

$$D_{2n} = \{\, \alpha^i\beta^j \mid 0 \leqslant i \leqslant n-1,\ 0 \leqslant j \leqslant 1 \,\}$$

and

$$|D_{2n}| \leqslant 2n.$$

To complete this part, we must establish the above $2n$ elements are distinct. First, since $o(\alpha) = n$, the powers 1, α, α^2, …, α^{n-1} are distinct (as was observed earlier). If $\alpha^i\beta = \alpha^j\beta$, then multiplying by β^{-1} gives $\alpha^i = \alpha^j$, so $i = j$. Finally suppose $\alpha^i\beta = \alpha^j$, so $\beta = \alpha^{j-i}$. But β fixes 1, while α^{j-i} moves 1 to $1+j-i$, so this forces $j = i$ and so $\beta = 1$, which is false. Hence the $2n$ products listed above are distinct and

$$|D_{2n}| = 2n.$$

(iv) Follows from (ii) and (iii):

$$\beta\alpha = \alpha^{-1}\beta = \alpha^{n-1}\beta \neq \alpha\beta.$$

□

It can be shown that each element of D_{2n} corresponds to a rotation or a reflection of a regular n-sided polygon and that the dihedral group D_{2n} is isomorphic to the group of symmetries of this polygon.

Cosets and Lagrange's Theorem

We have now met the definition of a subgroup and discovered how to generate a subgroup using a set of elements from a group. However, the claim was that subgroups were useful because they provide some sort of structure and constraint upon the group within which they are found. We shall now establish this by showing how a group is partioned into the union of cosets of any subgroup.

Definition 2.18 Let G be a group and suppose that H is a subgroup of G. Let $x \in G$. The *right coset* of H with *representative* x is the following subset of G:

$$Hx = \{\, hx \mid h \in H \,\}.$$

Similarly the *left coset* of H with representative x is

$$xH = \{\, xh \mid h \in H \,\}.$$

Most of the time one only needs to work with one type of coset. In this course, we shall place almost all our attention on right cosets and there will be only one or two places where we need to consider both right and left cosets. For this reason, we shall often simply speak of *cosets* and we shall mean right cosets when we do so.

Theorem 2.19 *Let G be a group and H be a subgroup of G.*

(i) *If $x, y \in G$, then $Hx = Hy$ if and only if $xy^{-1} \in H$.*

(ii) *Two right cosets of H in G are either equal or disjoint.*

(iii) *G is the disjoint union of the right cosets of H.*

(iv) *Every right coset contains the same number of elements as the subgroup H: if $x \in G$, then $|Hx| = |H|$.*

Although not proved here, we comment that analogous statements hold for left cosets. The only significant change is an appropriate alteration to the condition for two left cosets to be equal.

PROOF: (i) Suppose first $Hx = Hy$. Now $x = 1x \in Hx$, so $x \in Hy$. Therefore $x = hy$ for some $h \in H$ and then

$$xy^{-1} = h \in H.$$

Conversely, suppose $xy^{-1} \in H$. Then if $h \in H$,

$$hx = h(xy^{-1})y \in Hy,$$

as $h(xy^{-1}) \in H$, and we deduce $Hx \subseteq Hy$. Similarly, if $h \in H$,

$$hy = hyx^{-1}x = h(xy^{-1})^{-1}x \in Hx,$$

as $h(xy^{-1})^{-1} \in H$. We deduce $Hy \subseteq Hx$, and hence conclude

$$Hx = Hy.$$

(ii) Consider the two cosets Hx and Hy. These cosets are disjoint when $Hx \cap Hy = \varnothing$. Let us suppose that $Hx \cap Hy \neq \varnothing$, so there exists some element $g \in Hx \cap Hy$. Since $g \in Hx$, $g = hx$ for some $h \in H$. Equally, as $g \in Hy$, $g = ky$ for some $k \in H$. Then

$$hx = ky,$$

so

$$xy^{-1} = h^{-1}k \in H.$$

Then part (i) tells us $Hx = Hy$.

So the cosets Hx and Hy are either disjoint, or if not disjoint then they are equal.

(iii) If $x \in G$, then $x = 1x \in Hx$. Hence every element of G lies in some coset of H, and therefore G is the union of the cosets of H. Part (ii) tells us this is a disjoint union.

(iv) Define a mapping $\alpha\colon H \to Hx$ by

$$h\alpha = hx.$$

By definition of the coset, this is a surjective map. Let $h, k \in H$ and suppose that $h\alpha = k\alpha$; that is,

$$hx = kx.$$

Multiply by x^{-1} to deduce

$$h = (hx)x^{-1} = (kx)x^{-1} = k.$$

Hence α is injective. We conclude that α is a bijection and so

$$|H| = |Hx|.$$

□

Remarks:

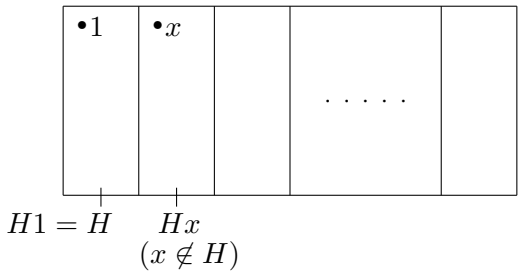
(i) If H is a subgroup of G, we can define a relation $\sim$ on the group G by

$$x \sim y \qquad \text{if and only if} \qquad xy^{-1} \in H.$$

Similar arguments and effort to that in the proof of Theorem 2.19 shows that $\sim$ is an equivalence relation on G and the equivalence classes are the right cosets of G. This is an alternative way to see that G is the disjoint union of the right cosets of H.

(ii) Note that the coset $H1$ with representative 1 (the identity) is equal, as a set, to the original subgroup H.

We have shown that the group G is the disjoint union of the right cosets of the subgroup H and each coset contains $|H|$ elements. We can represent this by the following diagram:



This means that the order of G must equal the number of cosets of H multiplied by the order of H.

Definition 2.20 Let G be a group and H be a subgroup of G. The *index* of H in G is the number of cosets of H occurring in G. It is denoted by $|G : H|$ (or by $[G : H]$ in some books).

We have proved:

Theorem 2.21 (Lagrange's Theorem) *Let G be a group and H be a subgroup of G. Then*

$$|G| = |G : H| \cdot |H|.$$

In particular, if G is a finite group, then $|H|$ divides $|G|$.

Corollary 2.22 *Let G be a finite group and $x \in G$. Then the order $o(x)$ of x divides $|G|$.*

PROOF: Proposition 2.13 says $o(x) = |\langle x \rangle|$, which divides $|G|$ by Lagrange's Theorem. □

We can now prove our first classification theorem:

Corollary 2.23 *Let p be a prime number. Any group of order p is cyclic.*

PROOF: Let G be a group of order p. Let $x \in G \setminus \{1\}$. Then $|\langle x \rangle|$ divides p, so $|\langle x \rangle| = p = |G|$ (since $x \neq 1$). Hence $G = \langle x \rangle$. □

We shall describe the structure of cyclic groups in full detail later. In particular, we shall show that there is, up to isomorphism, exactly one cyclic group of each order.

Example 2.24 Let $G = S_3$ and $H = \langle (1\ 2) \rangle = \{1, (1\ 2)\}$. Let us calculate the cosets of H: we know that there will be 3 right cosets.

$$\begin{aligned} H = H1 &= \{1, (1\ 2)\} = H(1\ 2) \\ H(2\ 3) &= \{(2\ 3), (1\ 3\ 2)\} = H(1\ 3\ 2) \\ H(1\ 3) &= \{(1\ 3), (1\ 2\ 3)\} = H(1\ 2\ 3) \end{aligned}$$

Let us also calculate the left cosets:

$$\begin{aligned} H = 1H &= \{1, (1\ 2)\} = (1\ 2)H \\ (2\ 3)H &= \{(2\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H \\ (1\ 3)H &= \{(1\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H \end{aligned}$$

Note that the right cosets and left cosets *do not* coincide.

We finish this section by recording a variation on Lagrange's Theorem that is frequently useful.

Theorem 2.25 *Let G be a group and H and K be subgroups of G with $K \leqslant H \leqslant G$. Then*

$$|G : K| = |G : H| \cdot |H : K|.$$

PROOF: For G infinite this requires a lot of care. This proof is omitted. (It can be found in books and on Problem Sheet I of my version of *MT5824*.)

For G finite, the proof is easy using Lagrange's Theorem:

$$|G : K| = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = |G : H| \cdot |H : K|.$$

□

Chapter 3

Normal Subgroups, Quotient Groups and Homomorphisms

In this section we introduce the second and third basic aspects of structure within groups, though, as we shall see, these are heavily linked. The most important definition here will be that of a homomorphism, which is a map between groups that preserve the group multiplications. We begin by defining the concept of a normal subgroup.

Normal subgroups and quotient groups

Definition 3.1 Let G be a group and N be a subgroup of G. We call N a *normal subgroup* of G if

$$g^{-1}xg \in N \qquad \text{for all } x \in N \text{ and } g \in G.$$

We write $N \trianglelefteqslant G$ to denote that N is a normal subgroup of G.

The element $g^{-1}xg$ is called the conjugate of x by g. It is frequently denoted by x^g. Conjugation will be discussed at greater length later.

Example 3.2 If G is any group, it is straightforward that

$$G \trianglelefteqslant G.$$

Furthermore, $g^{-1}1g = g^{-1}g = 1$, so we deduce

$$\mathbf{1} \trianglelefteqslant G.$$

The above two subgroups provide the only normal subgroups that are guaranteed to exist within any group. Any other normal subgroups exist for some reason to do with the actual nature of the group we are working with. A particularly interesting case will be groups where the trivial subgroup and the whole group itself are the only normal subgroups. We shall examine this in more detail later. The following lies at the other extreme:

Example 3.3 *In an abelian group, every subgroup is normal.*

Proof: Let G be an abelian group and $H \leqslant G$. Let $g \in G$ and $x \in H$. Then

$$g^{-1}xg = g^{-1}gx = 1x = x \in H.$$

So $H \trianglelefteqslant G$. □

Example 3.4 Consider the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Show that the subgroup $Z = \langle -1 \rangle$ is a normal subgroup of Q_8 of order 2.

SOLUTION: $(-1)^2 = 1$, so -1 is an element of Q_8 of order 2. Therefore

$$|Z| = |\langle -1 \rangle| = o(-1) = 2.$$

If $a = \pm i$, $\pm j$ or $\pm k$, then $a^2 = -1$ and $a^4 = 1$. This tells us that the order of a divides 4 and $o(a) \neq 2$, so

$$o(a) = 4 \qquad \text{if } a \in \{\pm i, \pm j, \pm k\}.$$

Now let $x \in Z$. If $x = 1$, then

$$g^{-1}xg = g^{-1}1g = g^{-1}g = 1 \in Z \qquad \text{for all } g \in Q_8.$$

If $x = -1$, then since Question 13 on Problem Sheet I tells us

$$o(g^{-1}xg) = o(x) = 2$$

and we have just observed that $x = -1$ is the unique element of order 2 in Q_8, we conclude

$$g^{-1}xg = x \in Z \qquad \text{for all } g \in Q_8.$$

Hence

$$g^{-1}xg \in Z \qquad \text{for all } x \in Z \text{ and all } g \in Q_8;$$

that is,

$$Z \trianglelefteq Q_8.$$

□

What a normal subgroup enables us to do is to create a group from the set of (right) cosets of the normal subgroup. We shall now do this:

Definition 3.5 Let G be a group and let N be a normal subgroup of G. Let

$$G/N = \{\, Nx \mid x \in G \,\},$$

the set of all right cosets of N in G. Define a multiplication on G/N by

$$Nx \cdot Ny = Nxy$$

for $x, y \in G$ (i.e., we multiply the representatives of the cosets).

We call G/N with this multiplication the *quotient group* of G by N.

We only use the notation G/N when $N \trianglelefteq G$. The set of right cosets of an arbitrary subgroup H of a group G only has a group multiplication defined upon it when H is a normal subgroup.

Theorem 3.6 *Let G be a group and N be a normal subgroup of G. Then G/N is a group with respect to the multiplication defined above.*

Establishing this theorem justifies our terminology: we are allowed to call G/N the "quotient group", since it is indeed a group.

PROOF: The most challenging step in the proof is the first one, verifying that we do have a binary operation on G/N, whereas checking the axioms of a group turns out to be straightforward. The problem is that the multiplication defined in Definition 3.5 depends upon the representatives x and y and we know that cosets can have many different representatives. We need to ensure our multiplication is *well-defined*: it depends only upon the cosets concerned and not on the *choice* of representatives for the cosets.

Consider two cosets of N and suppose that we have written them with different representatives: $Nx = Nx'$ and $Ny = Ny'$. This means that

$$x(x')^{-1} \in N \qquad \text{and} \qquad y(y')^{-1} \in N,$$

by Theorem 2.19(i). Let's give names to these elements of N, say

$$a = x(x')^{-1} \qquad \text{and} \qquad b = y(y')^{-1},$$

so

$$x = ax' \qquad \text{and} \qquad y = by'.$$

Then

$$\begin{aligned} xy = ax'by' &= ax'b(x')^{-1}x'y' \\ &= ab^{(x')^{-1}}x'y'. \end{aligned}$$

Since $N \trianglelefteq G$, $b^{(x')^{-1}} \in N$ and so $ab^{(x')^{-1}} \in N$. Therefore

$$xy(x'y')^{-1} = ab^{(x')^{-1}} \in N$$

and, using Theorem 2.19(i) again,

$$Nxy = Nx'y'.$$

This tells us that we get the same answer for the product $Nx \cdot Ny$ whether we calculate it using the representatives x and y or using the representatives x' and y'. Hence we have a well-defined multiplication on G/N.

The remaining sets of the proof are straightforward. We check the axioms of a group:

Associativity: Let $Nx, Ny, Nz \in G/N$. Then

$$(Nx \cdot Ny) \cdot Nz = Nxy \cdot Nz = N(xy)z$$

and

$$Nx \cdot (Ny \cdot Nz) = Nx \cdot Nyz = Nx(yz).$$

But the multiplication in G is associative, so $(xy)z = x(yz)$ and hence

$$(Nx \cdot Ny) \cdot Nz = Nx \cdot (Ny \cdot Nz),$$

as required.

Identity: $Nx \cdot N1 = Nx1 = Nx$ and $N1 \cdot Nx = N1x = Nx$ for all $x \in G$, so $N1$ is the identity element of G/N.

Inverses: $Nx \cdot Nx^{-1} = Nxx^{-1} = N1$ and $Nx^{-1} \cdot Nx = Nx^{-1}x = N1$, so Nx^{-1} is the inverse of Nx in G/N.

Hence G/N is a group. □

What one could do now is to take a known group G with a known normal subgroup N and then construct the multiplication table of G/N. This can be done, but the process is reasonably complicated. Moreover, it really misses the point. Multiplication tables tend to obscure information about groups and what we really want to understand are the subgroups and, now, the normal subgroups. In a short while we shall meet the Correspondence Theorem which tells us how the structure (i.e., subgroups and normal subgroups) of the quotient group G/N corresponds to just a part of this structure within G. In this sense, the quotient group has a more simplified structure than that of the original G.

As a further illustration, if we are working with a group G of order 44 (for example) and we manage to show that it has a normal subgroup N of order 11, then Lagrange's Theorem tells us $|G/N| = 4$. We now want to understand two groups N and G/N of considerably smaller order and then put them together to understand G. Future sections will explain more clearly how these steps are done.

Homomorphisms

The second part of this section concerns the final aspect of what might be described as basic group structure. This describes how two groups relate to each other via mappings that respect the group multiplication.

Definition 3.7 Let G and H be groups (both with multiplicatively written binary operation). A *homomorphism* $\phi\colon G \to H$ is a map such that

$$(xy)\phi = (x\phi)(y\phi) \qquad \text{for all } x, y \in G.$$

Note once again that we are writing our maps on the right. On the left-hand side we multiply the elements of G and then apply the map ϕ. On the right-hand side we apply ϕ to produce two elements of H and then multiply them in H. We often describe the above condition as saying that a homomorphism "preserves" the group multiplication. Homomorphisms in group theory are the analogues of linear maps in linear algebra, which preserve addition and scalar multiplication of vectors.

Example 3.8 (i) Let G and H be any groups. Define a map $\zeta\colon G \to H$ by

$$x\zeta = 1 \qquad \text{(the identity element of } H\text{)}$$

for all $x \in G$. Then ζ is a homomorphism, often called the *trivial homomorphism* (or "zero homomorphism").

VERIFICATION: $(xy)\zeta = 1$ while $(x\zeta)(y\zeta) = 1 \cdot 1 = 1$. □

(ii) If G is any group, the identity map $\iota\colon G \to G$ is a homomorphism, since $(xy)\iota = xy = (x\iota)(y\iota)$ for all $x, y \in G$.

(iii) The set $\{\pm 1\}$ forms a group under multiplication, indeed it is cyclic of order 2 generated by -1.

Now consider S_n, the symmetric group of degree n. Define a map $\Phi\colon S_n \to \{\pm 1\}$ by

$$\sigma\Phi = \begin{cases} +1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Remember that a permutation is even/odd if it is a product of an even/odd number of transpositions. When we multiply two permutations, we will add the number of transpositions involved, so we observe:

$$\begin{aligned}\text{even perm} \times \text{even perm} &= \text{even perm}\\ \text{even perm} \times \text{odd perm} &= \text{odd perm}\\ \text{odd perm} \times \text{even perm} &= \text{odd perm}\\ \text{odd perm} \times \text{odd perm} &= \text{even perm}\end{aligned}$$

From this it follows that Φ is a homomorphism.

(iv) Let F be a field. The set of non-zero elements of F form a group under multiplication, called the *multiplicative group* of F and denoted F^*. If n is a positive integer, define

$$\delta\colon \mathrm{GL}_n(F) \to F^*$$

by

$$A\delta = \det A.$$

Since $\det(AB) = \det A \cdot \det B$, we conclude δ is a homomorphism.

The first basic properties of homomorphisms are the following:

Lemma 3.9 *Let $\phi\colon G \to H$ be a homomorphism from a group G to a group H. Then*

(i) *$1_G\phi = 1_H$, where 1_G and 1_H denote the identity elements of G and H, respectively.*

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

We normally write $1\phi = 1$ for part (i) since, as ϕ is a map $G \to H$, it is clear that the identity element on the left-hand side must lie in G, as that is the domain of ϕ, and that the right-hand side must be in the codomain H of ϕ. Similarly, in (ii), the inverse on the left-hand side is in G, while that on the right-hand side is calculated in H.

Proof: (i) Let $e = 1\phi = 1_G\phi$. Then as $1 \cdot 1 = 1$ in G, when we apply ϕ we deduce

$$e = 1\phi = (1 \cdot 1)\phi = (1\phi)(1\phi) = e^2.$$

We now multiply by e^{-1}:

$$e = e^2e^{-1} = ee^{-1} = 1 \ \ (= 1_H).$$

(ii) Let $x \in G$ and consider $x\phi$ and $(x^{-1})\phi$. Since ϕ is a homomorphism

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

and

$$(x^{-1})\phi \cdot x\phi = (x^{-1}x)\phi = 1\phi = 1,$$

using part part (i) both times. This shows that $(x^{-1})\phi$ is the inverse of $x\phi$ in the group H. Since inverses are unique, we have established

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

□

Kernels and images

To make progress working with homomorphisms, we need to make the following definitions which are fundamental to the study of these maps. They are, of course, very similar to those made in linear algebra.

Definition 3.10 Let $\phi\colon G \to H$ be a homomorphism from a group G to a group H.

(i) The *kernel* of ϕ is
$$\ker\phi = \{\, x \in G \mid x\phi = 1 \,\}.$$

(ii) The *image* of ϕ is
$$\operatorname{im}\phi = G\phi = \{\, x\phi \mid x \in G \,\}.$$

Note that, in this definition, $\ker\phi$ is a subset of G while $\operatorname{im}\phi$ is a subset of H. In fact, we can say much more:

Lemma 3.11 *Let $\phi\colon G \to H$ be a homomorphism from a group G to a group H. Then*

(i) *the kernel of ϕ is a normal subgroup of G;*

(ii) *the image of ϕ is a subgroup of H.*

Proof: (i) We must first show that $\ker\phi$ is a subgroup of G. To do this, we use Lemma 3.9(i) to tell us $1\phi = 1$, so $1 \in \ker\phi$ (that is, the kernel of ϕ contains the identity element of G). In particular, the kernel is a non-empty subset of G. Now let $x, y \in \ker\phi$, so $x\phi = y\phi = 1$. Then
$$(xy)\phi = (x\phi)(y\phi) = 1 \cdot 1 = 1$$
and
$$(x^{-1})\phi = (x\phi)^{-1} = 1^{-1} = 1.$$
Hence $xy, x^{-1} \in \ker\phi$. This tells us $\ker\phi$ is a subgroup of G.

Now let $x \in \ker\phi$ and $g \in G$. Then
$$(g^{-1}xg)\phi = (g\phi)^{-1}(x\phi)(g\phi) = (g\phi)^{-1}1(g\phi) = (g\phi)^{-1}(g\phi) = 1.$$
Hence $g^{-1}xg \in \ker\phi$ for all $x \in \ker\phi$ and $g \in G$.

We conclude that $\ker\phi$ is a normal subgroup of G.

(ii) Since $1\phi = 1$, we conclude $\operatorname{im}\phi$ is non-empty as it contains the identity element of H. Now let $g, h \in \operatorname{im}\phi$. By definition, $g = x\phi$ and $h = y\phi$ for some $x, y \in G$. Then
$$gh = (x\phi)(y\phi) = (xy)\phi \in \operatorname{im}\phi$$
and
$$g^{-1} = (x\phi)^{-1} = (x^{-1})\phi \in \operatorname{im}\phi.$$
Hence, $\operatorname{im}\phi$ is a subgroup of H. □

The kernel and the image tell us a lot about our homomorphism ϕ. For a start, they inform us whether or not it is injective or surjective:

Lemma 3.12 *Let $\phi\colon G \to H$ be a homomorphism from a group G to a group H.*

(i) *ϕ is injective if and only if* $\ker\phi = \mathbf{1}$.

(ii) *ϕ is surjective if and only if* $\operatorname{im}\phi = H$.

PROOF: (ii) is an immediate consequence of the definitions.

(i) Suppose ϕ is injective. Let $x \in \ker\phi$. Then $x\phi = 1 = 1\phi$ and, as ϕ is injective, we conclude $x = 1$. Thus $\ker\phi = \mathbf{1}$.

Conversely, suppose $\ker\phi = \mathbf{1}$. Let $x, y \in G$ and suppose $x\phi = y\phi$. Then

$$(xy^{-1})\phi = (x\phi)(y\phi)^{-1} = (x\phi)(x\phi)^{-1} = 1.$$

So $xy^{-1} \in \ker\phi = \mathbf{1}$ and $xy^{-1} = 1$. Multiplying by y gives

$$x = xy^{-1}y = 1y = y,$$

and we conclude ϕ is injective. □

The Isomorphism Theorems

We have introduced the concepts of a homomorphism, its kernel and its image. The kernel is always a normal subgroup and, in view of our work earlier in the section, the natural question is what is the quotient group and what does it tell us about the homomorphism ϕ? Before we do that, we present an example that tells us that it is not just the case that kernels are normal subgroups, but the converse also holds, so kernels of homomorphisms and normal subgroups are precisely the same thing.

Example 3.13 Let G be any group and N be a normal subgroup of G. Recall that we can then form the quotient group

$$G/N = \{\, Nx \mid x \in G \,\}$$

with multiplication

$$Nx \cdot Ny = Nxy.$$

Let us define a map $\pi\colon G \to G/N$ by

$$x\pi = Nx \qquad \text{for each } x \in G.$$

(So we map each element of G to the unique coset of N that contains it.) The multiplication in G/N ensures that π is a homomorphism:

$$(xy)\pi = Nxy = Nx \cdot Ny = (x\pi)(y\pi) \qquad \text{for all } x, y \in G.$$

We call π the *natural homomorphism* or *canonical homomorphism* associated to N.

The definition ensures that π is surjective; that is, $\operatorname{im}\pi = G/N$. We now determine the kernel:

$$\begin{aligned}\ker\pi &= \{\, x \in G \mid x\pi = N1 \,\} \\ &= \{\, x \in G \mid Nx = N1 \,\} \\ &= \{\, x \in G \mid x \in N \,\} = N.\end{aligned}$$

In particular, this tells us that every normal subgroup occurs as the kernel of a homomorphism. The First Isomorphism Theorem strengthens what we have done to show that the image of a homomorphism always looks like the quotient by the kernel, which is what we have just observed happens with the natural homomorphism.

Theorem 3.14 (First Isomorphism Theorem) *Let G and H be groups and $\phi\colon G \to H$ be a homomorphism from G to H. Then $\ker\phi$ is a normal subgroup of G, $\operatorname{im}\phi$ is a subgroup of H and*

$$G/\ker\phi \cong \operatorname{im}\phi.$$

PROOF: The first two assertions are found in Lemma 3.11. We need to construct an isomorphism (a bijective homomorphism) between $G/\ker\phi$ and $\operatorname{im}\phi$. So write $K = \ker\phi$ and define

$$\theta\colon G/K \to \operatorname{im}\phi$$

by

$$(Kx)\theta = x\phi.$$

The definition of θ appears to depend on the choice of representative x for the coset Kx, so we must first check that θ is well-defined.

Suppose $Kx = Ky$. Then $xy^{-1} \in K = \ker\phi$, so

$$1 = (xy^{-1})\phi = (x\phi)(y\phi)^{-1}$$

and multiplying by $y\phi$ gives $x\phi = y\phi$. Hence θ is well-defined.

Next

$$(Kx \cdot Ky)\theta = (Kxy)\theta = (xy)\phi = (x\phi)(y\phi) = (Kx)\theta \cdot (Ky)\theta$$

and we deduce θ is a homomorphism.

If $g \in \operatorname{im}\phi$, then $g = x\phi$ for some $x \in G$. Then

$$(Kx)\theta = x\phi = g$$

and we see that θ is surjective.

Finally if $Kx \in \ker\theta$, then $1 = (Kx)\theta = x\phi$, so $x \in \ker\phi = K$ and therefore $Kx = K1$, the identity element in G/K. This shows that $\ker\theta = \{K1\} = \mathbf{1}$ and Lemma 3.12 now tells us θ is injective.

Hence θ is a bijective homomorphism and (comparing Definitions 1.13 and 3.7) this is exactly what an isomorphism is. Hence

$$G/\ker\theta = G/K \cong \operatorname{im}\phi.$$

□

Example 3.15 (i) Recall the homomorphism $\Phi\colon S_n \to \{\pm 1\}$ given by

$$\sigma\Phi = \begin{cases} +1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Provided $n \geqslant 2$, S_n contains both odd and even permutations (e.g., (1 2) and 1, respectively). So

$$\operatorname{im}\Phi = \{\pm 1\}$$

and as A_n consists of all even permutations,

$$\ker\Phi = A_n.$$

The First Isomorphism Theorem tells us $A_n \trianglelefteqslant S_n$ and

$$S_n/A_n \cong \{\pm 1\} \cong C_2,$$

a cyclic group of order 2. In particular, this tells us A_n is a subgroup of index 2 in S_n, so $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}\,n!$.

(ii) Recall the homomorphism $\delta\colon \mathrm{GL}_n(F) \to F^*$ given by

$$A\delta = \det A \qquad \text{for each } A \in \mathrm{GL}_n(F).$$

Since

$$\det \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} = \alpha \qquad \text{for each } \alpha \in F^*,$$

we see that δ is surjective. The *special linear group* $\mathrm{SL}_n(F)$ is the set of all matrices with entries from F and determinant 1. So

$$\ker \delta = \mathrm{SL}_n(F)$$

and it follows from the First Isomorphism Theorem that

$$\mathrm{SL}_n(F) \trianglelefteqslant \mathrm{GL}_n(F) \qquad \text{and} \qquad \frac{\mathrm{GL}_n(F)}{\mathrm{SL}_n(F)} \cong F^*.$$

The conclusion of what we have just done is that images of homomorphisms and quotients by normal subgroups are the same thing. What we really need to understand is how quotient groups behave and the remainder of this section contains three more major theorems which enable us to do this.

Theorem 3.16 (Correspondence Theorem) *Let G be a group and N be a normal subgroup of G. Let*

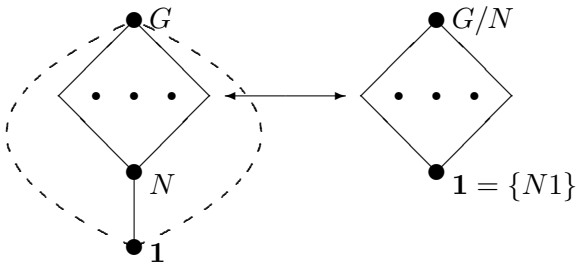
$$\mathcal{A} = \{\, H \mid N \leqslant H \leqslant G \,\},$$

the set of all subgroups of G that contain N, and $\mathcal{B}$ be the set of subgroups of G/N. The map $f\colon \mathcal{A} \to \mathcal{B}$ defined by

$$Hf = H/N = \{\, Nh \mid h \in H \,\}$$

is a bijection and preserves inclusions. Moreover, under this bijection, normal subgroups (of G containing N) correspond to normal subgroups (of G/N).

To interpret this theorem, let us accept that the multiplication table does not provide us with good information about a group and instead that finding the subgroups of a group G, how these relate to each other and their properties (including which are normal) would be far more useful. We could represent them by a diagram where each subgroup is represented by a node, inclusions by upward sloping arrows and normal subgroups are marked (e.g., by colouring them a different colour). What the Correspondence Theorem tells us that, when we have found a normal subgroup N, then that part of the structural diagram lying between N and G is precisely the structural diagram of G/N. (In the sketch below, the dashed lines indicate that there is some part of the subgroup diagram that is not illustrated and we are mainly concentrating on that part lying between N and G, as is referred to in the statement of the Correspondence Theorem.)



PROOF OF THEOREM 3.16: If H is a subgroup of G with $N \leqslant H \leqslant G$, then N is also a normal subgroup of H and we can certainly form H/N. This quotient is a subset of G/N which forms a group under the binary operation on G/N. Thus f is a map from the set $\mathcal{A}$ of all subgroups of G containing N to the set $\mathcal{B}$ of subgroups of G/N. We first establish that f is a bijection.

Let $H_1, H_2 \in \mathcal{A}$ and suppose $H_1 f = H_2 f$; i.e., $H_1/N = H_2/N$. If $x \in H_1$, then $Nx \in H_1/N = H_2/N$, so $Nx = Nh$ for some $h \in H_2$. Thus $xh^{-1} \in N \leqslant H_2$, so $xh^{-1} = k$ where $k \in H_2$ and then $x = kh \in H_2$. This shows $H_1 \leqslant H_2$ and the same argument repeated with H_1 and H_2 interchanged then shows $H_1 = H_2$. Thus f is injective.

Let $S \in \mathcal{B}$. Let $H = \{\, x \in G \mid Nx \in S \,\}$. Since S contains the identity element $N1$ of G/N, we see that $Nx = N1 \in S$ for all $x \in N$ and so $N \leqslant H$. In particular, H is non-empty. Let $x, y \in H$. Then $Nx, Ny \in S$, so

$$Nxy = Nx \cdot Ny \in S \qquad \text{and} \qquad Nx^{-1} = (Nx)^{-1} \in S$$

and therefore $xy, x^{-1} \in H$. Hence H is a subgroup of G containing N, that is, $H \in \mathcal{A}$. By definition, Hf consists of some cosets belonging to S; that is, $Hf \subseteq S$. However, every element of S is a coset Nx and this x belongs to H. Thus $Hf = S$ and we deduce that f is surjective.

If $H_1, H_2 \in \mathcal{A}$ and $H_1 \leqslant H_2$, then

$$H_1 f = \{\, Nx \mid x \in H_1 \,\} \leqslant \{\, Nx \mid x \in H_2 \,\} = H_2 f.$$

On the other hand, suppose $H_1 f \leqslant H_2 f$. If $x \in H_1$, then $Nx \in H_1 f \leqslant H_2 f$, so $x \in H_2$ (using the earlier observation that f is a bijection). Thus

$$H_1 \leqslant H_2 \qquad \text{if and only if} \qquad H_1 f \leqslant H_2 f;$$

that is, f is a bijection $\mathcal{A} \to \mathcal{B}$ which preserves inclusions.

If $K \in \mathcal{A}$ and $K \trianglelefteqslant G$, then for $Nx \in K/N$ and $Ng \in G/N$,

$$(Ng)^{-1}(Nx)(Ng) = Ng^{-1}xg \in K/N,$$

since $g^{-1}xg \in K$. Thus if $K \trianglelefteqslant G$, then $Kf = K/N \trianglelefteqslant G/N$.

If $S \in \mathcal{B}$ and $S \trianglelefteqslant G/N$, let $H \in \mathcal{A}$ be the unique subgroup of G containing N corresponding to S; that is,

$$H = Sf^{-1} = \{\, x \in G \mid Nx \in S \,\} \qquad \text{and} \qquad S = Hf = H/N.$$

Let $x \in H$ and $g \in G$. Then

$$Ng^{-1}xg = (Ng)^{-1}(Nx)(Ng) \in S,$$

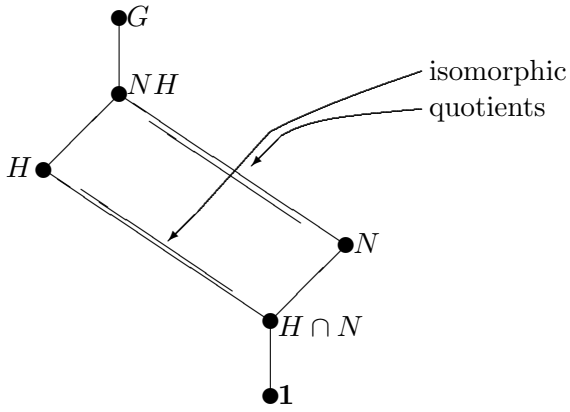
as $S \trianglelefteqslant G/N$. We conclude $g^{-1}xg \in H$ for all $x \in H$ and $g \in G$. Thus $Sf^{-1} = H \trianglelefteqslant G$.

This establishes the final part of the theorem: subgroups in $\mathcal{A}$ which are normal in G correspond to normal subgroups of G/N under f and *vice versa*. □

Theorem 3.17 (Second Isomorphism Theorem) *Let G be a group, H be a subgroup of G and N be a normal subgroup of G. Then $H \cap N$ is a normal subgroup of H, NH is a subgroup of G and*

$$H/(H \cap N) \cong NH/N.$$

Here $NH = \{\, nh \mid n \in N, h \in H \,\}$. What the Second Isomorphism Theorem does is tell us how normal subgroups of a group G interact with other subgroups. Note in particular, that NH/N is a subgroup of the quotient G/N and corresponds to the subgroup NH of G under the Correspondence Theorem. In terms of subgroup diagrams, we have:



PROOF: Since $N \trianglelefteq G$, we can construct the quotient group G/N and the associated natural homomorphism $\pi\colon G \to G/N$. Let $\phi = \pi|_H$ be the restriction of π to H; that is, $\phi\colon H \to G/N$ is the map given by

$$x\phi = x\pi = Nx \qquad \text{for all } x \in H.$$

Since π is a homomorphism, it is immediate that ϕ is also a homomorphism. We seek now to apply the First Isomorphism Theorem to ϕ. The relevant subgroups are

$$\begin{aligned}\ker\phi &= \{\, x \in H \mid x\phi = N1 \,\} \\ &= \{\, x \in H \mid Nx = N1 \,\} \\ &= \{\, x \in H \mid x \in N \,\} = H \cap N\end{aligned}$$

and

$$\operatorname{im}\phi = \{\, Nx \mid x \in H \,\}.$$

Now the First Isomorphism Theorem tells us $\ker\phi = H \cap N$ is a normal subgroup of H. Also $\operatorname{im}\phi$ is a subgroup of G/N and by the Correspondence Theorem it has the form $\operatorname{im}\phi = K/N$ for some subgroup K with $N \leqslant K \leqslant G$. The proof of the Correspondence Theorem tells us what K is:

$$\begin{aligned}K &= \{\, g \in G \mid Ng \in \operatorname{im}\phi \,\} \\ &= \{\, g \in G \mid Ng = Nh \text{ for some } h \in H \,\} \\ &= \{\, g \in G \mid gh^{-1} \in N \text{ for some } h \in H \,\} \\ &= \{\, g \in G \mid gh^{-1} = n \text{ for some } h \in H,\, n \in N \,\} \\ &= \{\, g \in G \mid g = nh \text{ for some } h \in H,\, n \in N \,\} \\ &= NH.\end{aligned}$$

Thus NH is a subgroup of G. Finally

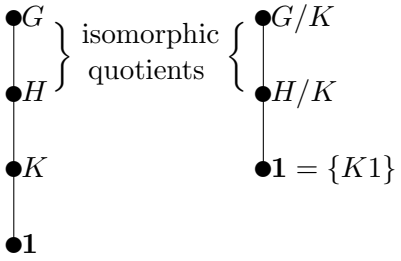
$$H/(H \cap N) = H/\ker\phi \cong \operatorname{im}\phi = K/N = NH/N.$$

□

Theorem 3.18 (Third Isomorphism Theorem) *Let G be a group and let H and K be normal subgroups of G with $K \leqslant H \leqslant G$. Then H/K is a normal subgroup of G/K and*

$$\frac{G/K}{H/K} \cong G/H.$$

If $K \trianglelefteqslant G$, the Correspondence Theorem tells us that normal subgroups of G/K have the form H/K where $K \leqslant H \leqslant G$ and $H \trianglelefteqslant G$. What the Third Isomorphism Theorem does for us is identify the quotient of G/K by such a normal subgroup. It tells us, in particular, that the resulting quotient group is the same as the one found by taking the quotient of G by H. It can be represented pictorially as:



Proof: It follows (as discussed above) straight from the Correspondence Theorem that $H/K \trianglelefteqslant G/K$, but we shall deduce it from the First Isomorphism Theorem.

Define $\phi\colon G/K \to G/H$ by

$$(Kx)\phi = Hx.$$

Since the definition of ϕ appears to depend on the choice of representative x, we must first verify that it really is a function of the cosets.

Suppose $Kx = Ky$. Then $xy^{-1} \in K \leqslant H$, so $Hx = Hy$ and we do indeed have $(Kx)\phi = (Ky)\phi$. Hence ϕ is well-defined.

Next, ϕ is a homomorphism, since

$$(Kx \cdot Ky)\phi = (Kxy)\phi = Hxy = Hx \cdot Hy = (Kx)\phi \cdot (Ky)\phi.$$

Then

$$\ker\phi = \{\, Kx \mid Hx = H1 \,\} = \{\, Kx \mid x \in H \,\} = H/K$$

and

$$\operatorname{im}\phi = \{\, Hx \mid x \in G \,\} = G/H.$$

Now the First Isomorphism Theorem tells us that $H/K \trianglelefteqslant G/K$ and

$$\frac{G/K}{H/K} = \frac{G/K}{\ker\phi} \cong \operatorname{im}\phi = G/H,$$

as required. □

The content of this section provides us with crucial tools that will be used throughout this course and beyond whenever studying group theory.

Chapter 4

Cyclic Groups

In this short chapter, we shall perform a detailed analysis of cyclic groups. We shall be able to completely classify them up to isomorphism and provide a full description of the subgroup structure. The fact that we can so easily perform this indicates that cyclic groups are the most straightforward to understand. It is, however, necessary that we do fully understand them before moving on to more complicated groups.

Recall that a group G is cyclic if $G = \langle x \rangle$ for some $x \in G$. This means that the elements of G are the powers of the element x.

Proposition 4.1 *A cyclic group is abelian.*

PROOF: Let $G = \langle x \rangle$. If $g, h \in G$, then $g = x^m$ and $h = x^n$ for some $m, n \in \mathbb{Z}$. Then

$$gh = x^m x^n = x^{m+n} = x^n x^m = hg.$$

Hence G is abelian. □

We already know that every subgroup of an abelian group is normal, so this also applies to cyclic groups. However, the most significant observation to make based on the above proof is that in a cyclic group the multiplication is essentially determined by the *addition* of the exponents. This will be a feature of our analysis in this chapter (and will stand in sharp contrast to most other work conducted within groups).

We recall some standard examples of cyclic groups.

Example 4.2 (i) The integers under addition is an example of an infinite cyclic group: $\mathbb{Z} = \langle 1 \rangle$.

(ii) The set of complex nth roots of 1 is a multiplicative cyclic group of order n:

$$C_n = \{ \mathrm{e}^{2k\pi i/n} \mid k = 0, 1, 2, \ldots, n-1 \} = \langle \mathrm{e}^{2\pi i/n} \rangle.$$

(iii) The set of integers modulo n, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, is a group under addition performed modulo n. It is cyclic generated by 1: $\mathbb{Z}_n = \langle 1 \rangle$, since

$$k = \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} \in \langle 1 \rangle,$$

for each k.

Theorem 4.3 (i) *An infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$.*

(ii) *A cyclic group of order n is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.*

This theorem provides us with a complete classification of cyclic groups. It tells us, in particular, that the multiplicative group C_n is isomorphic to the additive group $\mathbb{Z}_n$. In view of this theorem, we often write C_∞ and C_n, respectively, to denote an arbitrary infinite cyclic group and an arbitrary cyclic group of order n. We now know these are essentially unique as groups.

We immediately deduce:

Corollary 4.4 *Let p be a prime. Up to isomorphism, there is exactly one group of order p.*

PROOF: If G is a group of order p, then G is cyclic by Corollary 2.23, so $G \cong \mathbb{Z}_p$ by Theorem 4.3(ii). □

PROOF OF THEOREM 4.3: (i) Let G be an infinite cyclic group, say $G = \langle x \rangle$. Then $o(x) = \infty$ and the powers of x are distinct. We may define a map $\phi\colon \mathbb{Z} \to G$ by

$$n\phi = x^n$$

and this is now a bijection. Then

$$(m+n)\phi = x^{m+n} = x^m x^n = (m\phi)(n\phi) \qquad \text{for all } m, n \in \mathbb{Z}.$$

Hence ϕ is an isomorphism and so $G \cong \mathbb{Z}$.

(ii) Let G be cyclic of order n, say $G = \langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\}$. Now define $\phi\colon \mathbb{Z}_n \to G$ by $i\phi = x^i$ and again ϕ is a bijection. As $o(x) = n$, if $i + j \equiv r \pmod{n}$, then

$$(i+j)\phi = r\phi = x^r = x^{i+j} = x^i x^j = (i\phi)(j\phi)$$

and again ϕ is an isomorphism and $G \cong \mathbb{Z}_n$. □

Subgroups of cyclic groups

Let us now attempt to describe the subgroups of a group G that is cyclic of (finite) order n. Suppose $G = \langle x \rangle$. Any subgroup of G has order dividing n by Lagrange's Theorem, so let us choose a divisor d of n. Write

$$n = dk$$

for some $k \in \mathbb{Z}$. Consider $y = x^k$. The powers of this element are

$$x^k, x^{2k}, x^{3k}, \ldots, x^{dk} = x^n = 1,$$

since $o(x) = n$. Therefore

$$o(y) = o(x^k) = d.$$

So G possesses a subgroup of order d, namely $\langle x^k \rangle = \langle x^{n/d} \rangle$.

Conversely, let H be any subgroup of G. We shall show that H has the form just described. For a start H consists of some powers of x and we note $x^n = 1 \in H$. It therefore makes sense to define m to be the smallest positive integer such that $x^m \in H$. Certainly $\langle x^m \rangle \leqslant H$. Let $i \in \mathbb{Z}$ with $x^i \in H$. Divide i by m to obtain a quotient and remainder:

$$i = qm + r \qquad \text{where } 0 \leqslant r < m.$$

Then $r = i - qm$ and

$$x^r = x^i(x^m)^{-q} \in H.$$

The minimality of m forces $r = 0$, so $x^i = x^{qm} = (x^m)^q \in \langle x^m \rangle$. Thus

$$H = \langle x^m \rangle$$

and in particular applying the above argument to $i = n$ (since $x^n = 1 \in H$) tells us that

$$m \text{ divides } n.$$

The powers of x^m are therefore x^m, x^{2m}, $\ldots$, $(x^m)^{n/m} = x^n = 1$ and $o(x) = n/m$. This shows that every subgroup has the form described above (namely our H is the subgroup of order $d = n/m$).

We have established:

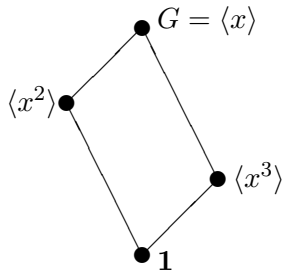
Theorem 4.5 *Let $G = \langle x \rangle$ be a finite cyclic group of order n. Then*

(i) *every subgroup of G is cyclic;*

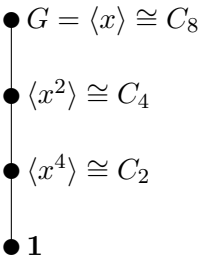
(ii) *the group G has a unique subgroup of order d for each divisor d of n, namely the subgroup $\langle x^{n/d} \rangle$.* □

Example 4.6 *Describe the subgroup structure of (i) a cyclic group of order 6, (ii) a cyclic group of order 8.*

SOLUTION: (i) Let $G = \langle x \rangle = C_6$. Then G has a unique subgroup of each order 1, 2, 3 and 6, which are $\mathbf{1}$, $\langle x^3 \rangle$, $\langle x^2 \rangle$ and G itself, respectively. Since any containment of one of these in another requires the corresponding orders to divide, we conclude the group structure is as follows:



(ii) Let $G = \langle y \rangle = C_8$. Then G has a unique subgroup of each order 1, 2, 4 and 8, namely $\mathbf{1}$, $\langle x^4 \rangle$, $\langle x^2 \rangle$ and $\langle x \rangle$. Since $x^4 \in \langle x^2 \rangle$, we deduce that there is an inclusion $\langle x^4 \rangle \leqslant \langle x^2 \rangle$. We conclude the subgroup structure is:



□

The analogue of Theorem 4.5 for infinite cyclic groups is the following, which is proved by similar arguments:

Theorem 4.7 *Let $G = \langle x \rangle$ be a cyclic group of infinite order. Then every non-trivial subgroup of G has the form $\langle x^m \rangle$ for some positive integer m and this is the unique subgroup of G of index m.*

PROOF: Omitted. See Problem Sheet IV. □

Chapter 5

Constructing Groups

Permutation Groups

In Chapter 2, we considered subgroups and, in particular, described an algorithm for computing the elements in the subgroup of a finite group G generated by a set X. We applied this algorithm in the case of a collection of permutations in a symmetric group (see Example 2.15). One natural question is whether we can build all groups in this way. In so doing we are asking which groups arise as "permutation groups".

A *permutation group* is a subgroup of some symmetric group S_X. What we shall observe is that every group is isomorphic to a permutation group. As a consequence every finite group can be built using our algorithm from a finite collection of permutations (at least up to isomorphism).

Theorem 5.1 (Cayley's Theorem) *Every group G is isomorphic to a subgroup of some symmetric group S_X (for some set X).*

PROOF: Let G be any group. Take $X = G$ and so consider the symmetric group S_G consisting of bijections $G \to G$. If $g \in G$, define a map

$$\begin{aligned} \sigma_g \colon G &\to G \\ x &\mapsto xg. \end{aligned}$$

Claim: σ_g is a bijection.

We establish this claim by providing an inverse for σ_g; specifically, we shall show $\sigma_{g^{-1}}$ is the inverse of σ_g:

$$x\sigma_g\sigma_{g^{-1}} = (xg)g^{-1} = x(gg^{-1}) = x1 = x$$

and

$$x\sigma_{g^{-1}}\sigma_g = (xg^{-1})g = x(g^{-1}g) = x1 = x.$$

Hence $\sigma_g\sigma_{g^{-1}} = \sigma_{g^{-1}}\sigma_g = \mathrm{id}$ (the identity map $G \to G$).

We conclude that $\sigma_g \in S_G$ for all $g \in G$.

We may now define a map $\phi \colon G \to S_G$ by

$$g\phi = \sigma_g \qquad \text{for each } g \in G.$$

Note that

$$x\sigma_g\sigma_h = (xg)h = x(gh) = x\sigma_{gh} \qquad \text{for } x, g, h \in G,$$

so

$$\sigma_g\sigma_h = \sigma_{gh} \qquad \text{for } g, h \in G,$$

that is,

$$(g\phi)(h\phi) = (gh)\phi \qquad \text{for } g, h \in G.$$

Thus ϕ is a homomorphism.

Now let $g \in \ker\phi$, so $\sigma_g = \mathrm{id}$, the identity map $G \to G$. Hence

$$x = x\sigma_g = xg \qquad \text{for all } x \in G.$$

Taking $x = 1$ (the identity element of G), we see that $g = 1$. Hence

$$\ker\phi = \mathbf{1}.$$

Lemma 3.12(i) now tells us that ϕ is an injective homomorphism.

Let $H = \mathrm{im}\,\phi$, which is a subgroup of S_G. Then ϕ is a bijective homomorphism $G \to H$, so $G \cong H$, as required. □

Remarks

(i) If we examine the proof, we see that it shows that if G is a finite group of order n, then G is isomorphic to a subgroup of $S_G \cong S_n$. For example, this tells us that A_5 (a group of order 60) is isomorphic to a subgroup of S_{60} (which is a group of order $60! \approx 8.3 \times 10^{81}$), whereas the very definition of the group concerned tells us that A_5 is actually a subgroup of S_5. This illustrates that although Cayley's Theorem tells us that every group is a subgroup of a symmetric group, this fact alone may not help us work well with the original group nor may the proof give us the most useful embedding. It is frequently useful to consider other ways to produce a homomorphism $G \to S_n$ to a symmetric group. The module *MT5824 Topics in Groups* discusses this and provides examples of how such homomorphisms may be constructed.

(ii) The theorem does justify the interest in permutations, subgroups of S_n, and our Example 2.15 where we applied the algorithm for generating subgroups to produce a subgroup of S_8 of order 8 (which happened to be isomorphic to Q_8). Actually the subgroup is precisely the one produced from Q_8 via Cayley's Theorem.

(iii) There are similar types of results for embedding in other types of groups. For example, we can produce a matrix corresponding to a permutation σ of $\{1, 2, \ldots, n\}$ and hence embed S_n in $\mathrm{GL}_n(F)$ (for any field F). Use of Cayley's Theorem then shows that every finite group is a subgroup of some general linear group $\mathrm{GL}_n(F)$. (See Problem Sheet V for more details.)

Direct Products

The other thing we shall do in this section is to give a construction that takes a number of groups and produces another group. There are many examples of such constructions in group theory and the one we give is just the most straightforward. Another more complicated construction is described in *MT5824*.

Definition 5.2 Let G and H be groups (both with multiplicatively written binary operations). The *direct product* of G and H is

$$G \times H = \{\, (g, h) \mid g \in G,\, h \in H \,\},$$

the set of ordered pairs of an element in G and an element in H, with multipication given by

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Theorem 5.3 *Let G and H be groups. Then the direct product $G \times H$ is a group and its order is given by*

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

PROOF: The formula for the group order is obvious. We need to verify the group axioms.

Associativity: Let $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$. Then

$$\begin{aligned}
\big((g_1, h_1)(g_2, h_2)\big)(g_3, h_3) &= (g_1 g_2, h_1 h_2)(g_3, h_3) \\
&= \big((g_1 g_2)g_3, (h_1 h_2)h_3\big) \\
&= \big(g_1(g_2 g_3), h_1(h_2 h_3)\big) \\
&= (g_1, h_1)(g_2 g_3, h_2 h_3) \\
&= (g_1, h_1)\big((g_2, h_2)(g_3, h_3)\big).
\end{aligned}$$

Hence the multiplication on $G \times H$ is associative.

Identity: If $(g, h) \in G \times H$, then

$$(g, h)(1, 1) = (g1, h1) = (g, h)$$

and

$$(1, 1)(g, h) = (1g, 1h) = (g, h).$$

Hence $(1, 1)$ $(= (1_G, 1_H))$ is the identity element in $G \times H$.

Inverses: We shall show that the inverse of (g, h) is (g^{-1}, h^{-1}):

$$(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (1, 1)$$

and

$$(g^{-1}, h^{-1})(g, h) = (g^{-1}g, h^{-1}h) = (1, 1).$$

Hence (g^{-1}, h^{-1}) is indeed the inverse of (g, h).

This completes the proof that the direct product $G \times H$ is indeed a group under the specified multiplication. □

We have now defined the direct product of two groups G and H and established that $G \times H$ is a group. What we should do is establish how the properties of this new group relate to the two groups G and H that we started with.

So let G and H be any groups and consider the direct product

$$G \times H = \{\, (g, h) \mid g \in G,\, h \in H \,\}$$

(where we multiply the elements of $G \times H$ componentwise, as described in Definition 5.2.) Define

$$\bar{G} = \{\, (g,1) \mid g \in G \,\} \qquad \text{and} \qquad \bar{H} = \{\, (1,h) \mid h \in H \,\}.$$

Also define $\alpha\colon G \to G \times H$ and $\beta\colon H \to G \times H$ by

$$g\alpha = (g,1) \qquad \text{and} \qquad h\beta = (1,h).$$

If $g_1, g_2 \in G$, then

$$(g_1g_2)\alpha = (g_1g_2, 1) = (g_1,1)(g_2,1) = (g_1\alpha)(g_2\alpha).$$

Hence α is a homomorphism. By construction

$$\operatorname{im}\alpha = \{\, (g,1) \mid g \in G \,\} = \bar{G},$$

so we conclude that $\bar{G}$ is a subgroup of $G \times H$ (by Lemma 3.11(ii)).

If $g \in \ker\alpha$, then $(g,1) = g\alpha = (1,1)$ and so we conclude that $\ker\alpha = \mathbf{1}$. Hence α is a bijective homomorphism from G to $\bar{G}$, so $\bar{G}$ is a subgroup of $G \times H$ isomorphic to G.

Theorem 5.4 *Let G and H be two groups and let $G \times H$ be their direct product. Define*

$$\bar{G} = \{\, (g,1) \mid g \in G \,\} = G \times \mathbf{1} \quad \textit{and} \quad \bar{H} = \{\, (1,h) \mid h \in H \,\} = \mathbf{1} \times H.$$

(i) *$\bar{G}$ and $\bar{H}$ are normal subgroup of $G \times H$.*

(ii) *$\bar{G} \cong G$ and $\bar{H} \cong H$.*

(iii) *$\bar{G} \cap \bar{H} = \mathbf{1}$.*

(iv) *$G \times H = \bar{G}\bar{H}$.*

Proof: (i), (ii) We have already shown that $\bar{G}$ is a subgroup of $G \times H$ isomorphic to G. The same argument applied to the map β above shows that $\bar{H}$ is a subgroup of $G \times H$ isomorphic to H. If

$$(x,1) \in \bar{G} \qquad \text{and} \qquad (g,h) \in G \times H,$$

then

$$\begin{aligned}(g,h)^{-1}(x,1)(g,h) &= (g^{-1}xg, h^{-1}h) \\ &= (g^{-1}xg, 1) \in \bar{G}.\end{aligned}$$

Hence $\bar{G} \trianglelefteq G \times H$. Similarly $\bar{H} \trianglelefteq G \times H$.

(iii) The form of the elements in $\bar{G}$ and $\bar{H}$ guarantees that $\bar{G} \cap \bar{H} = \{(1,1)\} = \mathbf{1}$.

(iv) If $(g,h) \in G \times H$, then

$$(g,h) = (g,1)(1,h) \in \bar{G}\bar{H}.$$

Thus $G \times H \subseteq \bar{G}\bar{H}$. However, the reverse inclusion $\bar{G}\bar{H} \subseteq G \times H$ is obvious since $\bar{G}$ and $\bar{H}$ are contained in the group $G \times H$ and this is closed under products. This establishes $G \times H = \bar{G}\bar{H}$. □

Since $\bar{G}, \bar{H} \trianglelefteqslant G \times H$, it is natural to ask what the quotient groups are. Define

$$\begin{aligned} \pi\colon G \times H &\to G & \qquad \rho\colon G \times H &\to H \\ (g,h) &\mapsto g & (g,h) &\mapsto h. \end{aligned}$$

Note

$$\big((g_1,h_1)(g_2,h_2)\big)\pi = (g_1g_2, h_1h_2)\pi = g_1g_2 = (g_1,h_1)\pi \cdot (g_2,h_2)\pi.$$

Hence π is a homomorphism. It is immediate that

$$\ker\pi = \{\,(1,h) \mid h \in H\,\} = \bar{H} \qquad \text{and} \qquad \operatorname{im}\pi = G.$$

The First Isomorphism Theorem (Theorem 3.14) now tells us that

$$\frac{G \times H}{\bar{H}} = \frac{G \times H}{\ker\pi} \cong \operatorname{im}\pi = G.$$

A similar argument using ρ shows

$$\frac{G \times H}{\bar{G}} \cong H.$$

Thus:

Theorem 5.5 *If G and H are any groups, then*

$$\frac{G \times H}{G \times \mathbf{1}} \cong H \qquad \text{and} \qquad \frac{G \times H}{\mathbf{1} \times H} \cong G.$$

□

In fact, the properties given in Theorem 5.4 characterise direct products.

Theorem 5.6 *Let G be a group and let M and N be normal subgroups of G such that* (i) $M \cap N = \mathbf{1}$ *and* (ii) $G = MN$. *Then $G \cong M \times N$.*

Proof: Define $\phi\colon M \times N \to G$ by

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

Hypothesis (ii) tells us that ϕ is surjective.

If $x \in M$ and $y \in N$, consider the element

$$x^{-1}y^{-1}xy.$$

(We shall meet such elements again later. It is called the *commutator* of x and y.) We use the fact that $M \trianglelefteqslant G$ and $N \trianglelefteqslant G$ to see

$$x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) \in M \qquad \text{and} \qquad x^{-1}y^{-1}xy = (x^{-1}y^{-1}x)y \in N.$$

Hence

$$x^{-1}y^{-1}xy \in M \cap N = \mathbf{1},$$

so $x^{-1}y^{-1}xy = 1$. Multiplying by x and then by y on the left gives:

$$xy = yx \qquad \text{for all } x \in M \text{ and } y \in N.$$

Hence, for $(x_1, y_1), (x_2, y_2) \in M \times N$, we calculate

$$(x_1, y_1)\phi \cdot (x_2, y_2)\phi = x_1 y_1 x_2 y_2 = x_1 x_2 y_1 y_2 = (x_1 x_2, y_1 y_2)\phi = \big((x_1, y_1)(x_2, y_2)\big)\phi.$$

Thus ϕ is a homomorphism.

If $(x, y) \in \ker \phi$, then $1 = (x, y)\phi = xy$, so

$$x = y^{-1} \in M \cap N = 1$$

and we deduce $(x, y) = (1, 1)$ and so $\ker \phi = \{(1, 1)\} = \mathbf{1}$.

It follows that ϕ is injective and we now conclude that it is an isomorphism. Thus $G \cong M \times N$. □

We can similarly construct a direct product of many groups. We briefly summarise the analogous definition and results.

Definition 5.7 Let G_1, G_2, …, G_k be groups. The *direct product* of these groups is

$$G_1 \times G_2 \times \cdots \times G_k = \{\, (x_1, x_2, \ldots, x_k) \mid x_i \in G_i \text{ for each } i \,\}$$

with componentwise multiplication

$$(x_1, x_2, \ldots, x_k)(y_1, y_2, \ldots, y_k) = (x_1 y_1, x_2 y_2, \ldots, x_k y_k).$$

Similar arguments (though a little more care is needed in a few places) establishes the following two results:

Theorem 5.8 *Let G_1, G_2, …, G_k be groups.*

(i) *The direct product $D = G_1 \times G_2 \times \cdots \times G_k$ is a group.*

(ii) *$\bar{G}_i = \{\, (1, \ldots, 1, g, 1, \ldots, 1) \mid g \in G_i \,\}$ is a normal subgroup of D isomorphic to G_i for each i. (Here the element g occurs in the ith entry of the sequence.)*

(iii) *$\bar{G}_i \cap (\bar{G}_1 \bar{G}_2 \cdots \bar{G}_{i-1} \bar{G}_{i+1} \cdots \bar{G}_k) = \mathbf{1}$.*

(iv) *$D = \bar{G}_1 \bar{G}_2 \cdots \bar{G}_k$.*

Theorem 5.9 *If G is a group and N_1, N_2, …, N_k are normal subgroups of G such that $G = N_1 N_2 \cdots N_k$ and $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_k) = \mathbf{1}$ for each i, then $G \cong N_1 \times N_2 \times \cdots \times N_k$.*

Finally we provide another (more general) way to find normal subgroups of direct products.

Proposition 5.10 *Let G_1, G_2, …, G_k be groups and $N_i \trianglelefteq G_i$ for each i. Then $N_1 \times N_2 \times \cdots \times N_k \trianglelefteq G_1 \times G_2 \times \cdots \times G_k$ and*

$$\frac{G_1 \times G_2 \times \cdots \times G_k}{N_1 \times N_2 \times \cdots \times N_k} \cong (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_k/N_k).$$

Proof: Define $\phi\colon G_1 \times G_2 \times \cdots \times G_k \to (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_k/N_k)$ by

$$(x_1, x_2, \ldots, x_k)\phi = (N_1 x_1, N_2 x_2, \ldots, N_k x_k).$$

It is straightforward to verify that ϕ is a homomorphism, that it is surjective and

$$\begin{aligned} \ker \phi &= \{\, (x_1, x_2, \ldots, x_k) \mid N_i x_i = N_i 1 \text{ for each } i \,\} \\ &= N_1 \times N_2 \times \cdots \times N_k. \end{aligned}$$

The result now follows by the First Isomorphism Theorem. □

We shall use direct products in the next chapter to classify finite abelian groups.

Chapter 6

Finite Abelian Groups

In this chapter, we shall give a complete classification of finite abelian groups. In so doing, we shall observe how the assumption that our binary operation is commutative brings considerable restriction and so makes abelian groups very tractible to study. We shall also observe how useful direct products are in our classification.

Before we describe the structure of finite abelian groups, we make a number of comments. The first is that when studying abelian groups it is common to use additive notation for the binary operation rather than multiplicative. The reason for this is that the cyclic groups $\mathbb{Z}$ of all integers and $\mathbb{Z}_n$ of integers modulo n are very important. Many textbooks make this change in notation and some previous exam papers have followed this convention. The author of these lecture notes has chosen, however, to continue to use multiplicative notation so as to maintain consistency with other chapters in the lecture course and not to introduce a whole new set of notation for everything we have covered so far.

We recall some facts that we need:

(i) In an abelian group, every subgroup is normal (Example 3.3).

(ii) As a consequence, if H and K are subgroups of an abelian group, then $HK = \{\, hk \mid h \in H,\, k \in K \,\}$ is also a subgroup (Problem Sheet III, Question 3).

(iii) If x and y are elements of a finite abelian group, then x and y commute, so

$$o(xy) \text{ divides } \operatorname{lcm}\big(o(x), o(y)\big)$$

(Problem Sheet II, Question 5).

In our classification of finite abelian groups, the constituents will turn out to be direct products and cyclic groups. We start by proving:

Lemma 6.1 *Let m and n be coprime positive integers. Then*

$$C_{mn} \cong C_m \times C_n.$$

(Recall that m and n are *coprime* if the only positive common divisor is 1. Also C_m continues to denote a multiplicatively written cyclic group of order m.)

PROOF: Let $C_m = \langle x \rangle$ and $C_n = \langle y \rangle$. We know that the direct product $C_m \times C_n$ is a group of order mn. Consider $g = (x, y) \in C_m \times C_n$. The kth power is given by

$$g^k = (x^k, y^k)$$

and this equals the identity if and only if $x^k = 1$ and $y^k = 1$; that is, when $m = o(x)$ and $n = o(y)$ both divide k. Since m and n are coprime, we conclude that $g^k = (1, 1)$ if and only if mn divides k. Thus

$$o(g) = mn.$$

Hence $\langle g \rangle$ is a subgroup of order mn. Therefore

$$C_m \times C_n = \langle g \rangle \cong C_{mn}$$

(using Theorem 4.3 to tell us that there is a unique cyclic group of any given order up to isomorphism). □

Repeated use of Lemma 6.1 tells us:

Corollary 6.2 *Let n be a positive integer and write $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ as a product of prime powers (where the prime numbers p_1, p_2, …, p_r are distinct). Then*

$$C_n \cong C_{p_1^{k_1}} \times C_{p_2^{k_2}} \times \cdots \times C_{p_r^{k_r}}.$$

□

This corollary gives some clue as to how our classification theorem works. It essentially says that all finite abelian groups are built from cyclic groups of prime-power order using direct products.

Theorem 6.3 (Fundamental Theorem of Finite Abelian Groups)
Any finite abelian group G is isomorphic to a direct product of cyclic groups of prime-power order. Moreover, this decomposition is essentially unique in that any two such decompositions for G have the same number of non-trivial factors of each order.

We already know that rearranging terms in a direct product gives an isomorphic group (see Problem Sheet V, Question 4(a)). The uniqueness of the decomposition says precisely that rearranging the terms in the direct decomposition is the only change that can be made. Before proving Theorem 6.3, we give some examples of its use.

Example 6.4 (i) *List the abelian group of order* 16 *and of order* 27*, up to isomorphism.*

(ii) *How many abelian groups of order* 432 *are there up to isomorphism?*

SOLUTION: (i) $16 = 2^4$, so we need to put together cyclic groups of 2-power order. Thus the abelian groups of order 16 are:

$$C_{16}, \quad C_2 \times C_8, \quad C_4 \times C_4, \quad C_2 \times C_2 \times C_4, \quad C_2 \times C_2 \times C_2 \times C_2.$$

The abelian groups of order $27 = 3^3$ are:

$$C_{27}, \quad C_3 \times C_9, \quad C_3 \times C_3 \times C_3.$$

(ii) $432 = 2^4 3^3 = 16 \times 27$, so we build an abelian group of order 432 by putting together an abelian group of order 16 and an abelian group of order 27 (both written as direct products of cyclic groups). Hence there are

$$5 \times 3 = 15 \text{ abelian groups of order } 432.$$

(These are $C_{16} \times C_{27}$, $C_2 \times C_8 \times C_{27}$, …, $C_2 \times C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_3$.) □

The next goal is to prove the Fundamental Theorem of Finite Abelian Groups. The proof is reasonably complicated and the first tool we shall need is the following lemma.

Lemma 6.5 *Let $G = \langle x_1, x_2, \ldots, x_d \rangle$ be an abelian group with specified generators. If*

$$y = x_1^{k_1} x_2^{k_2} \ldots x_d^{k_d}$$

with $\gcd(k_1, k_2, \ldots, k_d) = 1$, then there exists $y_2, \ldots, y_d \in G$ such that

$$G = \langle y, y_2, \ldots, y_d \rangle.$$

PROOF: We proceed by induction on d. If $d = 1$, then $k_1 = \pm 1$ and $\langle y \rangle = \langle x_1 \rangle = G$.

If $d = 2$, then as $\gcd(k_1, k_2) = 1$, there exist $u, v \in \mathbb{Z}$ such that

$$uk_1 + vk_2 = 1.$$

Set $y_2 = x_1^v x_2^{-u}$. Then

$$\begin{aligned} x_1 = x_1^{uk_1+vk_2} &= x_1^{uk_1} x_2^{uk_2} x_1^{vk_2} x_2^{-uk_2} \\ &= (x_1^{k_1} x_2^{k_2})^u (x_1^v x_2^{-u})^{k_2} \\ &= y^u y_2^{k_2} \in \langle y, y_2 \rangle \end{aligned}$$

and

$$\begin{aligned} x_2 = x_2^{uk_1+vk_2} &= x_1^{vk_1} x_2^{vk_2} x_1^{-vk_1} x_2^{uk_1} \\ &= (x_1^{k_1} x_2^{k_2})^v (x_1^v x_2^{-u})^{-k_1} \\ &= y^v y_2^{-k_1} \in \langle y, y_2 \rangle. \end{aligned}$$

Since x_1, x_2 generate G, we conclude $G = \langle y, y_2 \rangle$.

Now suppose $d \geqslant 3$. Let

$$t = \gcd(k_1, k_2, \ldots, k_{d-1})$$

and $m_i = k_i/t$ for $i = 1, 2, \ldots, d-1$. Set

$$z = x_1^{m_1} x_2^{m_2} \ldots x_{d-1}^{m_{d-1}}.$$

By induction, since $\gcd(m_1, m_2, \ldots, m_{d-1}) = 1$ by construction, there exist $y_2, \ldots, y_{d-1}$ such that

$$\langle x_1, x_2, \ldots, x_{d-1} \rangle = \langle z, y_2, \ldots, y_{d-1} \rangle.$$

Notice

$$y = x_1^{k_1} x_2^{k_2} \ldots x_d^{k_d} = z^t x_d^{k_d}$$

and

$$\gcd(t, k_d) = \gcd(k_1, k_2, \ldots, k_d) = 1.$$

Hence by the Case $d = 2$, there exists y_d such that

$$\langle z, x_d \rangle = \langle y, y_d \rangle.$$

Now

$$\begin{aligned} G &= \langle x_1, x_2, \ldots, x_{d-1}, x_d \rangle \\ &= \langle x_1, x_2, \ldots, x_{d-1} \rangle \langle x_d \rangle \\ &= \langle z, y_2, \ldots, y_{d-1} \rangle \langle x_d \rangle \\ &= \langle z, y_2, \ldots, y_{d-1}, x_d \rangle \\ &= \langle z, x_d \rangle \langle y_2, \ldots, y_{d-1} \rangle \\ &= \langle y, y_d \rangle \langle y_2, \ldots, y_{d-1} \rangle \\ &= \langle y, y_2, \ldots, y_d \rangle. \end{aligned}$$

This completes the induction step and hence the proof. □

We now prove the Fundamental Theorem of Finite Abelian Groups.

Proof of Theorem 6.3: Let G be a finite abelian group. We start by establishing that G has the claimed direct product decomposition.

Claim 1: G is isomorphic to a direct product of cyclic groups of prime-power order.

Let $G = \langle x_1, x_2, \ldots, x_d \rangle$. We proceed by induction on d. If $d = 1$, then $G = \langle x_1 \rangle$ is cyclic and Corollary 6.2 tells us that G is a direct product of cyclic groups of prime-power order.

So suppose $d > 1$. We shall also suppose that d is as small as possible amongst all generating sets for G and, having fixed this d, that $o(x_1)$ is as small as possible amongst all generating sets for G of size d.

Let

$$H = \langle x_1 \rangle \qquad \text{and} \qquad K = \langle x_2, x_3, \ldots, x_d \rangle.$$

Since G is abelian, $H, K \trianglelefteq G$ and

$$HK = \langle x_1 \rangle \langle x_2, x_3, \ldots, x_d \rangle = \langle x_1, x_2, \ldots, x_d \rangle = G.$$

Subclaim: $G \cong H \times K$

Suppose $H \cap K \neq \mathbf{1}$, so there exists some non-identity element

$$g = x_1^{m_1} = x_2^{m_2} x_3^{m_3} \ldots x_d^{m_d}$$

in $H \cap K$ with $1 \leqslant m_1 < o(x_1)$. Let $t = \gcd(m_1, m_2, \ldots, m_d)$ and set $k_i = m_i/t$ for $i = 1, 2, \ldots, d$. Define

$$y = x_1^{-k_1} x_2^{k_2} x_3^{k_3} \ldots x_d^{k_d}.$$

Note by construction, $\gcd(-k_1, k_2, k_3, \ldots, k_d) = 1$ and Lemma 6.5 produces $y_2, \ldots, y_d$ such that $G = \langle y, y_2, \ldots, y_d \rangle$. Also

$$y^t = x_1^{-m_1} x_2^{m_2} x_3^{m_3} \ldots x_d^{m_d} = 1,$$

so $o(y) \leqslant t \leqslant m_1 < o(x_1)$. This contradicts our original choice of the generating set $\{x_1, x_2, \ldots, x_d\}$.

Hence $H \cap K = \mathbf{1}$. By Theorem 5.6, this is all that remains to show $G \cong H \times K$.

Now H is cyclic, so is a direct product of cyclic groups of prime-power order by Corollary 6.2. By induction, K is a direct product of cyclic groups of prime-power order. Hence, putting these together, $G \cong H \times K$ is a product of cyclic groups of prime-power order. This completes the proof of Claim 1, the existence of our claimed direct product decomposition.

Claim 2: The decomposition of G into a direct product of cyclic groups of prime-power order is essentially unique.

Let p be any prime dividing the order of G. Suppose that the largest cyclic group of p-power order occurring in the direct product decomposition of G is C_{p^t} and, for $i = 1, 2, \ldots, t$, let α_i be the number of factors occurring isomorphic to C_{p^i}.

Subclaim: $\alpha_1, \alpha_2, \ldots, \alpha_t$ are uniquely determined by G.

If the decomposition of G is

$$G \cong G_1 \times G_2 \times \cdots \times G_k,$$

where each G_i is a cyclic group of prime-power order, then an element

$$x = (x_1, x_2, \ldots, x_k) \in G_1 \times G_2 \times \cdots \times G_k$$

has order dividing p (our fixed prime), that is $x^p = 1$, if and only if each x_i has order dividing p. For such an x, if G_i has order that is not a power of p, we must select $x_i = 1$. If $G_i \cong C_{p^m}$ for some m, then x_i must be selected from the unique subgroup of G_i of order p (see Theorem 4.5). Hence

$$\text{the number of elements of order dividing } p \text{ in } G \text{ is} \quad p^{\alpha_1} p^{\alpha_2} \ldots p^{\alpha_t} = p^{\alpha_1+\alpha_2+\cdots+\alpha_t}$$

(and one of these is the identity element).

If we count the number of elements of order dividing p^2 in G, we can take our x_i to be any element when $G_i \cong C_p$, but when $G \cong C_{p^m}$ for $m \geqslant 2$, we can take x_i to be from the unique subgroup of G_i of order p^2. Hence

the number of elements of order p^2 in G is

$$p^{\alpha_1} (p^2)^{\alpha_2} (p^2)^{\alpha_3} \ldots (p^2)^{\alpha_t} = p^{\alpha_1+2\alpha_2+2\alpha_3+\cdots+2\alpha_t}.$$

In general, if $1 \leqslant j \leqslant t$, the number of elements of order dividing p^j in G is

$$p^{\alpha_1} (p^2)^{\alpha_2} (p^3)^{\alpha_3} \ldots (p^j)^{\alpha_j} (p^j)^{\alpha_{j+1}} \ldots (p^j)^{\alpha_t} = p^{\alpha_1+2\alpha_2+3\alpha_3+\cdots+j\alpha_j+j\alpha_{j+1}+\cdots+j\alpha_t}.$$

These numbers are therefore completely determined by G and so we conclude that

$$\begin{gathered}
\alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_t \\
\alpha_1 + 2\alpha_2 + 2\alpha_3 + \cdots + 2\alpha_t \\
\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + 3\alpha_t \\
\vdots \\
\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + t\alpha_t
\end{gathered}$$

and hence, upon subtracting each sum from the subsequent sum,

$$\begin{aligned} &\alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_t \\ &\alpha_2 + \alpha_3 + \cdots + \alpha_t \\ &\alpha_3 + \cdots + \alpha_t \\ &\vdots \\ &\alpha_t \end{aligned}$$

are uniquely determined by G. Therefore α_t, α_{t-1}, ..., α_1 are uniquely determined by G. This establishes the subclaim for each prime p dividing $|G|$, and this is enough to prove Claim 2 and hence complete the proof of the theorem. □

To finish the section, two final comments can be made. The first is to draw attention to the argument used in the uniqueness part of the proof. It is used in the following example.

Example 6.6 *Let $G = C_5 \times C_{25} \times C_{625} = C_5 \times C_{5^2} \times C_{5^4}$. Determine the number of elements of each order in G.*

SOLUTION: The identity element is the unique element of order 1. An element of order *dividing* 5 has the form (x_1, x_2, x_3) where x_i is selected from the unique subgroup of order 5 in the ith factor. Hence there are

$$5^3 \text{ elements of order diving } 5$$

and so

$$5^3 - 1 = 124 \text{ elements of order } 5.$$

An element of order dividing 5^2 has the form (x_1, x_2, x_3) where x_1, x_2 are arbitrary but x_3 is selected from the unique subgroup of order 5^2 in C_{5^4}. Hence there are

$$5 \times 5^2 \times 5^2 = 5^5 \text{ elements of order dividing } 5^2,$$

and so

$$5^5 - 5^3 = 3000 \text{ elements of order precisely } 5^2.$$

There are $5 \times 5^2 \times 5^3 = 5^6$ elements of order dividing 5^3, so

$$5^6 - 5^5 = 12\,500 \text{ elements of order precisely } 5^3.$$

This leaves

$$5^7 - 5^6 = 62\,500 \text{ elements of order precisely } 5^4.$$

□

The second comment is that given a decomposition for an abelian group as a direct product of cyclic groups of prime-power order, we can apply Corollary 6.2 to put the largest factors for each prime together, and then the next largest factors, and so on. In doing this, we can deduce the following alternative statement of the classification theorem:

Theorem 6.7 (Fundamental Theorem of Finite Abelian Group, II) *Let G be a finite abelian group. Then G can be uniquely expressed as a direct product*

$$G \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_t}$$

where $m_1, m_2, \ldots, m_t$ are positive integers such that m_i divides m_{i+1} for $i = 1, 2, \ldots, t-1$.

Example 6.8 Consider $G = C_2 \times C_4 \times C_3 \times C_9 \times C_9 \times C_5$. Putting together the largest factors for each prime in turn, we see:

$$\begin{aligned} C_4 \times C_9 \times C_5 &\cong C_{180} \\ C_2 \times C_9 &\cong C_{18} \\ C_3 &\cong C_3, \end{aligned}$$

so

$$G \cong C_3 \times C_{18} \times C_{180},$$

which is the unique form for G as described in Theorem 6.7.

Chapter 7

Simple Groups

The process of forming a quotient group of G by a normal subgroup N can be thought of as analogous to factorisation of integers. By using this quotient process, we move from considering a group G to considering two smaller groups N and G/N. Provided $N \neq 1$ and G, these are genuinely smaller than the original group G (at least in the case when G is a finite group, where the concept of "smaller" makes some sense). There is a class of groups therefore where quotient groups do not help us: the "simple" groups where only trivial quotients can be formed.

Definition 7.1 A group G is called *simple* if it is non-trivial and its only normal subgroups are $\mathbf{1}$ and G.

In this section, we shall establish two classes of finite simple group.

Proposition 7.2 *A cyclic group of prime order is simple.*

This result is simply another variant of Corollary 2.23.

Proof: Let G be a cyclic group of order p where p is prime. If H is any subgroup of G, then $|H|$ divides $|G| = p$, by Lagrange's Theorem (2.21). Hence $|H| = 1$ or p, so $H = \mathbf{1}$ or G. So the only subgroups, and certainly then the only normal subgroups, of G are $\mathbf{1}$ and G. □

In fact it is quite easy to see that any abelian simple group has to be cyclic of prime order. We leave the proof to Problem Sheet VII, but state here:

Theorem 7.3 *An abelian group is simple if and only if it is cyclic of prime order.*

Simplicity of the alternating groups

The main result of this section which provides us with a family of non-abelian simple groups.

Theorem 7.4 *The alternating group A_n is simple for $n \geqslant 5$.*

The structure of the proof is pretty much the standard one for proofs of simplicity:

Step 1: Find a set A of generators for the group G (see Lemma 7.5).

Step 2: Show any two elements of A are conjugate in G (see Lemma 7.6).

Step 3: Show any non-trivial normal N of G contains an element of A (see Lemma 7.7).

We then put these together to see that any non-trivial normal subgroup N of G contains one (by Step 3) and hence all (by Step 2) elements from A and therefore $N = G$ (by Step 1).

Lemma 7.5 *Let $n \geqslant 3$. The alternating group A_n is generated by its set of 3-cycles.*

(We assume that $n \geqslant 3$ simply to ensure A_n is non-trivial. When $n \leqslant 2$, A_n is the trivial group.)

PROOF: First note that a 3-cycle is even, since $(i\ j\ k) = (i\ j)(i\ k)$, a product of two transpositions.

Let σ be any element of A_n, that is, any even permutation of $X = \{1, 2, \ldots, n\}$. Then σ is a product of an even number of transpositions. We shall show that every product of two transpositions is a product of 3-cycles, for it will then follow that σ is also a product of 3-cycles.

Suppose i, j, k and ℓ are distinct points in X. Then

$$\begin{aligned}(i\ j)(i\ j) &= 1\\ (i\ j)(i\ k) &= (i\ j\ k)\\ (i\ j)(k\ \ell) &= (i\ j)(i\ k)(i\ k)(k\ \ell)\\ &= (i\ j\ k)(i\ \ell\ k).\end{aligned}$$

Thus every product of two transpositions, and hence every even permutation, is a product of 3-cycles. Therefore the alternating group is generated by its 3-cycles. □

Lemma 7.6 *Let $n \geqslant 5$. Then any two 3-cycles are conjugate in A_n.*

PROOF: Let $\sigma = (i_1\ i_2\ i_3)$ and $\tau = (j_1\ j_2\ j_3)$ be arbitrary 3-cycles in A_n. Define a permutation α by

$$i_1\alpha = j_1, \qquad i_2\alpha = j_2, \qquad i_3\alpha = j_3$$

and completing α to a permutation of $X = \{1, 2, \ldots, n\}$ by any appropriate selection of images for the remaining points in X. Then

$$\alpha^{-1}\sigma\alpha = (i_1\alpha\ \ i_2\alpha\ \ i_3\alpha) = \tau$$

(see Problem Sheet III, Question 4). This shows that σ and τ are conjugate in the symmetric group S_n. If it happens that α is an element of A_n, then in fact our 3-cycles σ and τ are conjugate in A_n.

Suppose that α is an odd permutation. Since $n \geqslant 5$, there exist at least two points $k, \ell \in X \setminus \{i_1, i_2, i_3\}$. Let $\beta = (k\ \ell)\alpha \in A_n$. We calculate

$$\begin{aligned}\beta^{-1}\sigma\beta &= \alpha^{-1}(k\ \ell)(i_1\ i_2\ i_3)(k\ \ell)\alpha\\ &= \alpha^{-1}(i_1\ i_2\ i_3)\alpha\\ &= \tau,\end{aligned}$$

since $(k\ \ell)$ commutes with $(i_1\ i_2\ i_3)$. Hence σ and τ are conjugate in A_n. □

Lemma 7.7 *Let $n \geqslant 5$ and N be a non-trivial normal subgroup of the alternating group A_n. Then N contains some 3-cycle.*

PROOF: Let σ be a non-identity element in N and let us choose σ to be a permutation of $X = \{1, 2, \ldots, n\}$ that moves the fewest possible points amongst all non-identity elements in N. Let r be the number of points moved by σ. Since σ cannot be a transposition (which would be an odd permutation), we know $r \geqslant 3$.

Let $i \in X$ be a point that is moves by σ. Choose $j \in X \setminus \{i, i\sigma, i\sigma^2\}$ (which is possible since $n > 3$). Let

$$\alpha = (i \;\; i\sigma \;\; j) \in A_n.$$

Then

$$\tau = \alpha^{-1}\sigma^{-1}\alpha\sigma = (\alpha^{-1}\sigma^{-1}\alpha)\sigma \in N,$$

since $N \trianglelefteqslant A_n$. But

$$\begin{aligned}\tau &= \alpha^{-1} \cdot \sigma^{-1}\alpha\sigma \\ &= (i \;\; j \;\; i\sigma)(i\sigma \;\; i\sigma^2 \;\; j\sigma)\end{aligned}$$

and this is a non-identity element in N since $j\tau = i\sigma^2 \neq j$. The points moved by τ are amongst

$$i, i\sigma, i\sigma^2, j, j\sigma$$

which tells us that an element of N which moves the fewest points in X can move at most five points. Thus

$$3 \leqslant r \leqslant 5.$$

We consider each possibility in order:

Case 1: $r = 5$.

Then σ must be a 5-cycle (as it cannot be a product of a 3-cycle and a 2-cycle), so

$$\sigma = (i \;\; i\sigma \;\; i\sigma^2 \;\; i\sigma^3 \;\; i\sigma^4).$$

Take $j = i\sigma^4$ in the above argument, so our element τ is

$$\tau = (i \;\; i\sigma^4 \;\; i\sigma)(i\sigma \;\; i\sigma^2 \;\; i) = (i \;\; i\sigma^4 \;\; i\sigma^2),$$

which moves three points. This contradicts $r = 5$ being the fewest number of points moved by a non-identity element of N.

Case 2: $r = 4$.

Then σ must be a product of two transpositions (as it cannot be a 4-cycle, which is odd), so

$$\sigma = (i \;\; i\sigma)(k \;\; k\sigma)$$

for some i and k. Take $j \in X \setminus \{i, i\sigma, k, k\sigma\}$ in the above argument (which is possible since $n \geqslant 5$). Then $j\sigma = j$ and $i\sigma^2 = i$, so

$$\tau = (i \;\; j \;\; i\sigma)(i\sigma \;\; i \;\; j) = (i \;\; i\sigma \;\; j),$$

which moves three points. This contradicts $r = 4$ being the fewest number of points moved by a non-identity element of N.

Case 3: $r = 3$.

It now follows that σ is 3-cycle and we have established the lemma. $\square$

PROOF OF THEOREM 7.4: Let $n \geqslant 5$ and suppose that N is a normal subgroup of A_n. We wish to prove $N = \mathbf{1}$ or A_n. If $N \neq \mathbf{1}$, then by Lemma 7.7, N contains some 3-cycle σ. Since $N \trianglelefteq G$, it contains all conjugates $\alpha^{-1}\sigma\alpha$ for $\alpha \in A_n$ and hence it contains all 3-cycles by Lemma 7.6. We then apply Lemma 7.5 to conclude $N = A_n$.

Hence A_n is simple if $n \geqslant 5$. $\square$

We finish this section by briefly mentioning that one of the crowning achievements of 20th century group theory was the completion of the Classification of Finite Simple Groups. This very long and difficult theorem, proved between the 1950s and the 1980s and featuring the efforts of many mathematicians, specifies a complete list of all the finite simple groups. It states that a finite simple group is either cyclic of prime order, an alternating group of degree $n \geqslant 5$, a group of Lie type (essentially constructed via matrices in a specific manner), or one of 26 so-called sporadic simple groups. The largest of the sporadic simple groups is called the Monster and it has order

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.

Chapter 8

Further Tools: The centre, commutators and conjugation

In this chapter, we develop a number of tools which are useful when making further progress in group theory. We shall use them in the remaining chapters of the course. They all relate in some way to the extent to which elements of a group do or do not commute.

The centre

Definition 8.1 Let G be any group. The *centre* of G is denoted by $\mathrm{Z}(G)$ and is defined by

$$\mathrm{Z}(G) = \{\, x \in G \mid xg = gx \text{ for all } g \in G \,\}.$$

Thus the centre of G consists of all those elements of G which commute with every element of G.

Theorem 8.2 *Let G be any group.*

(i) *The centre $\mathrm{Z}(G)$ is a normal subgroup of G.*

(ii) *G is abelian if and only if $\mathrm{Z}(G) = G$.*

Proof: (i) We first show that $\mathrm{Z}(G)$ is a subgroup of G. First

$$1g = g = g1 \qquad \text{for all } g \in G,$$

so $1 \in \mathrm{Z}(G)$. If $x, y \in \mathrm{Z}(G)$, then

$$xyg = xgy = gxy \qquad \text{for all } g \in G,$$

so $xy \in \mathrm{Z}(G)$. Multiplying the equation $xg = gx$ on the left and on the right by x^{-1} gives

$$gx^{-1} = x^{-1}g \qquad \text{for all } g \in G,$$

so $x^{-1} \in \mathrm{Z}(G)$. Hence $\mathrm{Z}(G)$ is a subgroup of G.

Finally if $x \in \mathrm{Z}(G)$ and $g \in G$, then

$$g^{-1}xg = g^{-1}gx = 1x = x \in \mathrm{Z}(G).$$

Thus $\mathrm{Z}(G) \trianglelefteqslant G$.

(ii) is immediate from the definition. □

Example 8.3 Consider the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. We calculate

$$(-1)i = -i = i(-1),$$

etc., and so deduce $-1 \in \mathrm{Z}(Q_8)$. Certainly $1 \in \mathrm{Z}(Q_8)$. However

$$ij = k \qquad \text{and} \qquad ji = -k \neq ij,$$

so $i, j \notin \mathrm{Z}(Q_8)$. Similar calculations apply to the other elements of order 4 in Q_8, so we conclude

$$\mathrm{Z}(Q_8) = \{\pm 1\} = \langle -1 \rangle.$$

Commutators and the derived subgroup

Definition 8.4 Let G be any group. If x and y are elements of G, the *commutator* of x and y is

$$[x, y] = x^{-1}y^{-1}xy.$$

The *derived subgroup* of G is denoted by G' and is defined to be the subgroup generated by all the commutators in G:

$$G' = \langle\, [x, y] \mid x, y \in G \,\rangle.$$

Remark: Observe

$$[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y, x],$$

so the inverse of a commutator is again a commutator. However, the product of two commutators need not be a commutator, though finding an example of a group where this happens is rather tricky. The smallest finite group where the derived subgroup and the *set* of commutators are different has order 96. However, note that as a consequence, in general, the elements of the derived subgroup are *products* of commutators.

By definition

$$xy = yx\,[x, y],$$

so $[x, y] = 1$ if and only if $xy = yx$. In this sense commutators measure "by how much" two elements fail to commute. Hence:

Lemma 8.5 *Let G be a group. If $x, y \in G$, then $[x, y] = 1$ if and only if x and y commute. In particular, $G' = \mathbf{1}$ if and only if G is abelian.* □

The process of determining the derived subgroup can appear at first sight to be somewhat cumbersome. Calculating all commutators and then calculating the subgroup they generated appears to be a rather time-consuming process. Fortunately the following characterisation is very useful in enabling us to find the derived subgroup.

Theorem 8.6 *Let G be a group. The derived subgroup of G is the smallest normal subgroup N of G such that the quotient group G/N is abelian.*

This is "smallest" in the sense that if N is *any* normal subgroup such that the quotient G/N is abelian, then $G' \leqslant N$.

PROOF: We must first verify that G' satisfies the stated property. First, by definition, G' is a subgroup of G. Let us show that G' is a normal subgroup of G. If $x, y, g \in G$, then

$$\begin{aligned} g^{-1}[x,y]g &= g^{-1}x^{-1}y^{-1}xyg \\ &= (g^{-1}x^{-1}g)(g^{-1}y^{-1}g)(g^{-1}xg)(g^{-1}yg) \\ &= (g^{-1}xg)^{-1}(g^{-1}yg)^{-1})(g^{-1}xg)(g^{-1}yg) \\ &= [g^{-1}xg, g^{-1}yg]. \end{aligned}$$

So any conjugate of a commutator is also a commutator. Now if $x \in G'$, write $x = c_1c_2 \dots c_k$ as a product of commutators. Then

$$g^{-1}xg = (g^{-1}c_1g)(g^{-1}c_2g) \dots (g^{-1}c_kg)$$

is also a product of commutators (from what we have just observed), so we conclude $g^{-1}xg \in G'$ whenever $x \in G'$ and $g \in G$. Thus $G' \trianglelefteqslant G$.

We now show that G/G' is abelian. Consider the product of two cosets $G'x$ and $G'y$ in this quotient group:

$$(G'x)(G'y) = G'xy \qquad \text{and} \qquad (G'y)(G'x) = G'yx.$$

Now

$$(xy)(yx)^{-1} = xyx^{-1}y^{-1} = [x^{-1}, y^{-1}] \in G',$$

so $G'xy = G'yx$. Hence

$$(G'x)(G'y) = (G'y)(G'x) \qquad \text{for all } x, y \in G$$

and we conclude G/G' is abelian.

Now suppose N is any normal subgroup of G such that G/N is abelian. If $x, y \in G$, then

$$N[x,y] = Nx^{-1}y^{-1}xy = (Nx)^{-1}(Ny)^{-1}(Nx)(Ny) = N1,$$

since we can rearrange the terms in the above product as G/N is abelian. Hence $[x, y] \in N$ for all $x, y \in G$. It follows that G', the subgroup generated by all such commutators, is contained in N. □

Example 8.7 Consider the quaternion group Q_8. In Question 8 on Problem Sheet III we showed that $N = \langle -1 \rangle \trianglelefteqslant Q_8$ and

$$Q_8/\langle -1 \rangle \cong V_4,$$

which is an abelian group. Hence by Theorem 8.6,

$$Q_8' \leqslant \langle -1 \rangle.$$

But $|\langle -1 \rangle| = 2$, so there remain only two possibilities $Q_8' = \mathbf{1}$ or $\langle -1 \rangle$. However, Q_8 is non-abelian, so $Q_8' \neq \mathbf{1}$. Therefore

$$Q_8' = \langle -1 \rangle.$$

Soluble groups

If G is any group, we can repeatedly take derived subgroups:

$$G^{(1)} = G', \qquad G^{(2)} = (G')', \qquad G^{(3)} = (G^{(2)})', \quad \ldots$$

A group G is called *soluble* if $G^{(n)} = \mathbf{1}$ for some n. The idea here is that the group G has a chain of subgroups

$$G \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots \geqslant G^{(n)} = \mathbf{1}$$

and, by Theorem 8.6, each quotient $G^{(i)}/G^{(i+1)}$ is abelian. Thus G is built, in some sense, from abelian groups and it turns out that these soluble groups have a more tractible structure than arbitrary groups. They are considered in more detail in *MT5824 Topics in Groups*.

Conjugacy classes

We now wish to study the conjugation property that has already arisen in the context of normal subgroups.

Definition 8.8 Let G be a group. Two elements x and y are said to be *conjugate* in G if there exists $g \in G$ such that $y = g^{-1}xg$.

Theorem 8.9 *Let G be a group. Define a relation $\sim$ on G by*

$$x \sim y \qquad \text{if and only if} \qquad y = g^{-1}xg \text{ for some } g \in G.$$

Then $\sim$ is an equivalence relation on G.

Proof: We check the conditions for an equivalence relation:

Reflexivity: If $x \in G$, then $x = 1^{-1}x1$, so $x \sim x$. Hence $\sim$ is reflexive.

Symmetry: Let $x, y \in G$ and suppose $x \sim y$. Then $y = g^{-1}xg$ for some $g \in G$. Then $x = gyg^{-1} = (g^{-1})^{-1}yg^{-1}$, so $y \sim x$. Hence $\sim$ is symmetric.

Transitivity: Let $x, y, z \in G$ and suppose $x \sim y$ and $y \sim z$. Then $y = g^{-1}xg$ and $z = h^{-1}yh$ for some $g, h \in G$. Then

$$z = h^{-1}yh = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh)$$

and so $x \sim z$. Hence $\sim$ is transitive.

This establishes that the relation of being conjugate is an equivalence relation on G. □

The standard facts about equivalence relations can be applied to conjugacy: specifically, that the group G is the disjoint union of the equivalence classes. We give the following name to the equivalence classes:

Definition 8.10 Let G be a group and x be an element of G. The *conjugacy class* of x in G is the $\sim$-equivalence class of x, that is,

$$\{\, y \in G \mid y \sim x \,\} = \{\, g^{-1}xg \mid g \in G \,\},$$

the set of all conjugates of x in G.

Example 8.11 (i) In an abelian group G, $g^{-1}xg = g^{-1}gx = x$, so two elements x and y in G are conjugate if and only if $x = y$. So the conjugacy classes in an abelian group are singletons $\{x\}$ as x ranges over G.

(ii) In Question 4 on Problem Sheet III, we observed that two permutations σ and τ in S_n are conjugate if and only if they have the same structure when factorised into products of disjoint cycles. So this cycle structure determines the conjugacy classes in S_n.

In particular, the conjugacy classes in S_4 are:

- the identity element,
- the transpositions,
- the 3-cycles,
- the 4-cycles,
- the permutations of the form $(i\ j)(k\ \ell)$.

(iii) In any group, $g^{-1}1g = 1$, so the identity element always forms a conjugacy class on its own.

Proposition 8.12 *A subgroup N of a group G is normal if and only if it is a union of conjugacy classes.*

PROOF: As N is a subgroup by assumption, it is normal if and only if it contains every conjugate of its elements, that is, if and only if it contains the whole conjugacy classes of every element. □

Centralisers

To describe the size of a conjugacy class, we make use of the following:

Definition 8.13 Let G be a group and $x \in G$. The *centraliser* of x in G is

$$\mathrm{C}_G(x) = \{\, g \in G \mid xg = gx \,\},$$

the set of all elements in G that commute with x.

Lemma 8.14 *Let G be a group and $x \in G$. The centraliser $\mathrm{C}_G(x)$ of x is a subgroup of G. It always contains the element x.*

PROOF: From $x1 = x = 1x$, we conclude $1 \in \mathrm{C}_G(x)$. We can also use the equation $xx = xx$ to conclude $x \in \mathrm{C}_G(x)$, which is the last assertion. Both facts ensure that $\mathrm{C}_G(x)$ is non-empty.

If $g, h \in \mathrm{C}_G(x)$, then

$$xgh = gxh = ghx$$

so $gh \in \mathrm{C}_G(x)$. Also multiplying $xg = gx$ on both sides by g^{-1} gives $g^{-1}x = xg^{-1}$, so $g^{-1} \in \mathrm{C}_G(x)$.

Hence $\mathrm{C}_G(x)$ is a subgroup of G. □

The following theorem then contains all the basic information we require concerning conjugacy classes:

Theorem 8.15 *Let G be a group.*

(i) *G is the disjoint union of its conjugacy classes.*

(ii) *If $x \in G$, there is a bijection between the conjugacy class of x and the cosets of the centraliser $\mathrm{C}_G(x)$. Thus the number of conjugates of x equals the index $|G : \mathrm{C}_G(x)|$.*

PROOF: (i) We have already established this is true (it follows from Theorem 8.9).

(ii) Define a map ϕ from the set of cosets of $\mathrm{C}_G(x)$ to the conjugacy class of x by

$$\phi\colon \mathrm{C}_G(x)g \mapsto g^{-1}xg.$$

First note that if $\mathrm{C}_G(x)g = \mathrm{C}_G(x)h$, then $gh^{-1} \in \mathrm{C}_G(x)$, so

$$xgh^{-1} = gh^{-1}x$$

and multiplying on the left by g^{-1} and on the right by h gives

$$g^{-1}xg = h^{-1}xh.$$

Hence ϕ is well-defined.

Clearly ϕ is surjective: the conjugate $g^{-1}xg$ is the image of the coset $\mathrm{C}_G(x)g$ under ϕ.

Finally suppose $(\mathrm{C}_G(x)g)\phi = (\mathrm{C}_G(x)h)\phi$; that is,

$$g^{-1}xg = h^{-1}xh.$$

Hence $xgh^{-1} = gh^{-1}x$, so $gh^{-1} \in \mathrm{C}_G(x)$ and therefore $\mathrm{C}_G(x)g = \mathrm{C}_G(x)h$. This shows that ϕ is injective.

We have shown that ϕ is indeed a bijection from the set of cosets of $\mathrm{C}_G(x)$ to the set of conjugates of x (that is, the conjugacy class of x). In particular, the number of conjugates of x equals the index $|G : \mathrm{C}_G(x)|$. □

Lemma 8.16 *An element x lies in a conjugacy class of size 1 if and only if $x \in \mathrm{Z}(G)$.*

PROOF: An element x has one conjugate if and only if $g^{-1}xg = x$ for all $g \in G$; that is, $xg = gx$ for all $g \in G$; that is, $x \in \mathrm{Z}(G)$. □

Now consider an arbitrary finite group G. Suppose that $\mathscr{C}_1$, $\mathscr{C}_2$, …, $\mathscr{C}_m$ are the conjugacy classes of G. Let us suppose that $\mathscr{C}_{k+1}$, …, $\mathscr{C}_m$ are the conjugacy classes of size 1, so

$$\mathscr{C}_{k+1} \cup \cdots \cup \mathscr{C}_m = \mathrm{Z}(G)$$

by Lemma 8.16. For $i = 1, 2, \ldots, k$, pick an element x_i in $\mathscr{C}_i$. Theorem 8.15(ii) tells us

$$|\mathscr{C}_i| = |G : \mathrm{C}_G(x_i)|.$$

Moreover, Theorem 8.15(i) says that G is the disjoint union of its conjugacy classes, so

$$\begin{aligned} |G| &= |\mathscr{C}_1| + |\mathscr{C}_2| + \cdots + |\mathscr{C}_k| + |\mathscr{C}_{k+1}| + \cdots + |\mathscr{C}_m| \\ &= \sum_{i=1}^{k} |G : \mathrm{C}_G(x_i)| + |\mathrm{Z}(G)|. \end{aligned}$$

Thus we have established:

Theorem 8.17 (Class Equation) *Let G be a finite group. Suppose that $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_k$ are the conjugacy classes of size $\geqslant 2$ and that x_i is an element of $\mathscr{C}_i$ for $i = 1, 2, \ldots, k$. Then*

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} |G : \mathrm{C}_G(x_i)|.$$

□

Conjugation of subgroups

We finish this chapter by considering how conjugation affects subgroups of a group.

First fix a group G and an element $g \in G$. Let $\tau_g \colon G \to G$ denote the map

$$\tau_g \colon x \mapsto g^{-1}xg$$

(that is, τ_g is the effect of conjugating by g).

Lemma 8.18 *If G is a group and $g \in G$, the map $\tau_g \colon G \to G$, given by $\tau_g \colon x \mapsto g^{-1}xg$, is a bijective homomorphism (that is, τ_g is an isomorphism $G \to G$).*

We give a special name to this sort of isomorphism.

Definition 8.19 Let G be a group. A map $\phi \colon G \to G$ that is an isomorphism is called an *automorphism* of G.

If $g \in G$, the automorphism τ_g given by $\tau_g \colon x \mapsto g^{-1}xg$ is called an *inner automorphism* of G.

Proof of Lemma 8.18: We first show that τ_g is a homomorphism:

$$(xy)\tau_g = g^{-1}xyg = (g^{-1}xg)(g^{-1}yg) = (x\tau_g)(y\tau_g) \qquad \text{for all } x, y \in G.$$

Then we show that τ_g is bijective by showing it is invertible:

$$x\tau_g\tau_{g^{-1}} = g(g^{-1}xg)g^{-1} = gg^{-1}xgg^{-1} = x$$

and

$$x\tau_{g^{-1}}\tau_g = g^{-1}(gxg^{-1})g = x$$

for all $x \in G$. Hence $\tau_g\tau_{g^{-1}} = \tau_{g^{-1}}\tau_g = \mathrm{id}$, the identity map $G \to G$. Hence τ_g is invertible; that is, it is a bijection. □

The crucial point about automorphisms is not that they tell us that G is isomorphic to G (which is, after all, obvious). Instead, applying an automorphism preserves all the structure present in the original group. In particular, an automorphism ϕ of G maps a subgroup H to a subgroup $H\phi$ (see Lemma 3.11(ii)) and ϕ induces a bijective homomorphism from H to $H\phi$. Hence $H\phi$ is a subgroup of G that is isomorphic to the original subgroup H.

Specialising to our inner automorphism τ_g, we conclude:

Corollary 8.20 *Let G be a group, $g \in G$ and H be a subgroup of G. Then the conjugate*

$$g^{-1}Hg = \{\, g^{-1}hg \mid h \in H \,\}$$

is a subgroup of G that is isomorphic to H. □

Normalisers

We finish by describing how many conjugates a subgroup has, using a tool very similar to the centraliser (which was defined in Definition 8.13).

Definition 8.21 Let G be a group and H be a subgroup of G. The *normaliser* of H in G is

$$\mathrm{N}_G(H) = \{\, g \in G \mid g^{-1}Hg = H \,\}.$$

Theorem 8.22 *Let G be a group and H be a subgroup of G.*

(i) *The normaliser $\mathrm{N}_G(H)$ is a subgroup of G.*

(ii) *H is contained in $\mathrm{N}_G(H)$.*

(iii) *$H \trianglelefteqslant G$ if and only if $\mathrm{N}_G(H) = G$.*

(iv) *The number of conjugates of H in G equals the index $|G : \mathrm{N}_G(H)|$ of the normaliser of H.*

Proof: (i) First note that

$$1^{-1}H1 = \{\, 1^{-1}h1 \mid h \in H \,\} = H,$$

so $1 \in \mathrm{N}_G(H)$. Now let $g, h \in \mathrm{N}_G(H)$. Then

$$(gh)^{-1}H(gh) = h^{-1}(g^{-1}Hg)h = h^{-1}Hh = H,$$

since $g^{-1}Hg = h^{-1}Hh = H$, and therefore $gh \in \mathrm{N}_G(H)$. Also conjugating the equation $H = g^{-1}Hg$ by g^{-1} gives

$$gHg^{-1} = g(g^{-1}Hg)g^{-1} = H,$$

so $g^{-1} \in \mathrm{N}_G(H)$. Thus $\mathrm{N}_G(H)$ is a subgroup of G.

(ii) If $h \in H$, then $h^{-1}Hh \leqslant H$, since H is a subgroup so closed under products and inverses. Equally $hHh^{-1} \leqslant H$ and conjugating by h now yields $H \leqslant h^{-1}Hh$. Hence $h^{-1}Hh = H$ for all $h \in H$ and therefore $h \in \mathrm{N}_G(H)$ for all $h \in H$.

(iii) This follows almost immediately from the definitions; note that $H \trianglelefteqslant G$ if and only if $g^{-1}Hg = H$ for all $g \in G$, as observed in Question 1 on Problem Sheet III.

(iv) Define a map ϕ from the set of cosets of $\mathrm{N}_G(H)$ to the set of conjugates of H by

$$\phi\colon \mathrm{N}_G(H)g \mapsto g^{-1}Hg.$$

Now

$$\begin{aligned} \mathrm{N}_G(H)g = \mathrm{N}_G(H)h \qquad & \text{if and only if} \qquad gh^{-1} \in \mathrm{N}_G(H) \\ & \text{if and only if} \qquad (gh^{-1})^{-1}H(gh^{-1}) = H \\ & \text{if and only if} \qquad hg^{-1}Hgh^{-1} = H \end{aligned}$$

and applying the bijection τ_h (conjugating by h) to the last equation, we conclude

$$\mathrm{N}_G(H)g = \mathrm{N}_G(H)h \qquad \text{if and only if} \qquad g^{-1}Hg = h^{-1}Hh.$$

Thus ϕ is both well-defined and injective. It is obvious that ϕ is surjective.

Hence ϕ is a bijection and we conclude that the number of conjugates of H equals the number of cosets of $\mathrm{N}_G(H)$, that is, the index $|G : \mathrm{N}_G(H)|$. □

Example 8.23 (i) Consider the dihedral group of order 8, $D_8 = \langle \alpha, \beta \rangle$, where $\alpha = (1\ 2\ 3\ 4)$ and $\beta = (2\ 4)$, with $\alpha^4 = 1$, $\beta^2 = 1$ and $\beta\alpha = \alpha^{-1}\beta$ (as described in Theorem 2.17). We know that a subgroup of order 1, 4 or 8 is normal in D_8 (since a subgroup of index 2 is always normal), so we shall concentrate on some of the subgroups of order 2. These are cyclic generated by one of the (five) elements of order 2 in D_8.

Consider first $K = \langle \alpha^2 \rangle = \{1, \alpha^2\}$. We calculate

$$\alpha^{-1}K\alpha = \{\alpha^{-1}1\alpha, \alpha^{-1}\alpha^2\alpha\} = \{1, \alpha^2\} = K$$

and, since $\beta^{-1}\alpha^2\beta = (2\ 4)(1\ 3)(2\ 4)(2\ 4) = (1\ 3)(2\ 4) = \alpha^2$,

$$\beta^{-1}K\beta = \{1, \alpha^2\} = K.$$

Hence $\alpha, \beta \in \mathrm{N}_{D_8}(K)$. Since α and β generate D_8 and the normaliser is a subgroup, we conclude that

$$\mathrm{N}_{D_8}(K) = D_8$$

and hence $K \trianglelefteq D_8$.

Now consider $H = \langle \beta \rangle = \{1, \beta\}$. We know that $H \leqslant \mathrm{N}_{D_8}(H)$ and as $\beta^{-1}\alpha^2\beta = \alpha^2$, we see α^2 and β commute, so

$$(\alpha^2)^{-1}H\alpha^2 = \{1, \beta\} = H.$$

On the other hand,

$$\alpha^{-1}\beta\alpha = \alpha^{-2}\beta = \alpha^2\beta \notin H.$$

This tells us $\langle \beta, \alpha^2 \rangle \leqslant \mathrm{N}_{D_8}(H) < D_8$. As subgroups of D_8 have order dividing 8, we conclude

$$\mathrm{N}_{D_8}(H) = \langle \beta, \alpha^2 \rangle = \{1, \beta, \alpha^2, \alpha^2\beta\}.$$

It follows that $H = \langle \beta \rangle$ has two conjugates in D_8 (as $|D_8 : \mathrm{N}_{D_8}(H)| = 2$), and these are H and $\alpha^{-1}H\alpha = \{1, \alpha^2\beta\} = \langle \alpha^2\beta \rangle$.

(ii) $D_8 = \langle \alpha, \beta \rangle$ is a subgroup of S_4, by its construction. The elements of D_8 are

$$D_8 = \{1, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (2\ 4), (1\ 4)(2\ 3), (1\ 3), (1\ 2)(3\ 4)\}.$$

Now $(1\ 2)^{-1}(1\ 3)(1\ 2) = (2\ 3) \notin D_8$, so $(1\ 2) \notin \mathrm{N}_{S_4}(D_8)$. We therefore deduce

$$D_8 \leqslant \mathrm{N}_{S_4}(D_8) < S_4,$$

so $\mathrm{N}_{S_4}(D_8)$ is a proper subgroup whose order is divisible by 8. Therefore

$$\mathrm{N}_{S_4}(D_8) = D_8$$

and D_8 has $|S_4 : D_8| = 3$ conjugates in S_4.

Chapter 9

Sylow's Theorem

One tool that has been applied throughout the course is Lagrange's Theorem (2.21). However, the information it tells us (that the orders of subgroups, and hence also of elements, divides the order of a finite group) mostly tells us about the non-existence of subgroups or at best restrictions upon their existence. It does not provide us with the existence of any subgroups. Indeed we know that the alternating group A_4 of degree 4 (of order 12) does not have a subgroup of order 6 (see Question 8 on Problem Sheet III), so there is no direct converse to Lagrange's Theorem. The purpose of this chapter is to provide a partial converse, but this is still a very strong result that has had profound impact on the study of group theory.

Definition 9.1 Let p be a prime number. A finite group is called a *p-group* if its order is a power of p.

A subgroup of a finite group is a *p-subgroup* if its order is a power of p.

So a p-subgroup of G is a subgroup that happens to be a p-group.

We are interested in a very special type of p-subgroup:

Definition 9.2 Let p be a prime number. Let G be a finite group and suppose $|G| = p^n m$ where p does not divide m. A *Sylow p-subgroup* of G is a subgroup of order p^n.

So a Sylow p-subgroup of G is a p-subgroup whose order is the largest power of p that divides $|G|$. Of course, Lagrange's Theorem tells us that there cannot be any larger p-subgroup of G.

Example 9.3 (i) $|S_4| = 24 = 2^3 \cdot 3$. A Sylow 2-subgroup of S_4 would be a subgroup of order $2^3 = 8$, so the dihedral group D_8 of order 8 is an example of a Sylow 2-subgroup of S_4.

A Sylow 3-subgroup of S_4, would be a subgroup of order 3, so $\langle (1\ 2\ 3) \rangle$ is an example of a Sylow 3-subgroup of S_4.

(ii) $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. The subgroup

$$H = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong V_4$$

is a Sylow 2-subgroup of A_5, $\langle (1\ 2\ 3) \rangle$ is a Sylow 3-subgroups of A_5, and $\langle (1\ 2\ 3\ 4\ 5) \rangle$ is a Sylow 5-subgroup of A_5.

(iii) $|A_6| = 360 = 2^3 \cdot 3^2 \cdot 5$. The subgroup

$$\langle (1\ 2\ 3), (4\ 5\ 6) \rangle \cong C_3 \times C_3$$

is a Sylow 3-subgroup of A_6.

Theorem 9.4 (Sylow's Theorem) *Let p be a prime number and G be a finite group of order $p^n m$ where p does not divide m. Then*

(i) *G has a Sylow p-subgroup;*

(ii) *any two Sylow p-subgroups of G are conjugate;*

(iii) *the number of Sylow p-subgroups of G is congruent to 1 (mod p) and divides m;*

(iv) *any p-subgroup of G is contained in a Sylow p-subgroup.*

Remarks If P is a Sylow p-subgroup of G and $g \in G$, then the conjugate $g^{-1}Pg$ is also a subgroup of G and, since the conjugation map $x \mapsto g^{-1}xg$ is a bijection, we know $|g^{-1}Pg| = |P|$. Thus $g^{-1}Pg$ is also a Sylow p-subgroup. Part (ii) of Sylow's Theorem tells us that every Sylow p-subgroup of G arises in this manner.

The first half of part (iii) of the theorem says that the total number of Sylow p-subgroups in G has the form $1 + kp$ for some $k \geqslant 0$.

We shall now embark on the lengthy process of proving the theorem. We shall then see many ways in which Sylow's Theorem can be used.

Proof: (i) We proceed by induction on $|G|$.

If $p^n = 1$, then the trivial subgroup is the required Sylow p-subgroup. In particular, this deals with the case when $|G| = 1$, for then $n = 0$, $p^n = 1$ and $m = 1$.

Now suppose that $|G| > 1$ and that all finite groups of smaller order possess Sylow p-subgroups. We can moreover assume that $p^n > 1$. We apply the Class Equation (Theorem 8.17). Let $\mathscr{C}_1$, $\mathscr{C}_2$, ..., $\mathscr{C}_k$ be the conjugacy classes of size greater than 1 and let $x_i \in \mathscr{C}_i$ for each i. Then

$$|\mathscr{C}_i| = |G : \mathrm{C}_G(x_i)| > 1$$

(by Theorem 8.15(ii)), so $|\mathrm{C}_G(x_i)| < |G|$ and

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} |G : \mathrm{C}_G(x_i)|. \tag{9.1}$$

If p^n divides one of $|\mathrm{C}_G(x_i)|$, then by induction $\mathrm{C}_G(x_i)$ contains a subgroup of order p^n and this is then a Sylow p-subgroup of G.

Otherwise p^n does not divide any of the $|\mathrm{C}_G(x_i)|$ and hence (using the fact that $p^n > 1$) p divides the index $|G : \mathrm{C}_G(x_i)|$ for $1 \leqslant i \leqslant k$. It then follows from Equation (9.1) that p divides $|\mathrm{Z}(G)|$. Now the centre $\mathrm{Z}(G)$ consists of those elements of G which commute with all elements of G, so in particular $\mathrm{Z}(G)$ is an abelian group. The Fundamental Theorem of Finite Abelian Groups (6.3) tells us that $\mathrm{Z}(G)$ is a direct product of cyclic groups and so, as p divides $|\mathrm{Z}(G)|$, there is at least one cyclic group of p-power order and hence, upon taking a generator for the unique subgroup of order p, we see that $\mathrm{Z}(G)$ contains an element g of order p.

Let $N = \langle g \rangle$. Since $N \leqslant \mathrm{Z}(G)$, then $N \trianglelefteqslant G$ (see Question 1 on Problem Sheet VIII). As $|N| = o(g) = p$, the quotient group G/N has order $p^{n-1}m$. By induction, G/N has a Sylow p-subgroup and this has order p^{n-1}. By the Correspondence Theorem, this Sylow p-subgroup has the form H/N where H is a subgroup of G with $N \leqslant H \leqslant G$. As

$$|H/N| = p^{n-1} \qquad \text{and} \qquad |N| = p,$$

we conclude $|H| = p^n$ and so H is a Sylow p-subgroup of G.

This completes the induction step and hence part (i) of Sylow's Theorem is established.

To establish parts (ii)–(iv) of Sylow's Theorem, we shall need a number of intermediate results.

Lemma 9.5 *Let p be a prime number, P be a Sylow p-subgroup of a finite group G and Q be any p-subgroup of G. Then*

$$Q \leqslant \mathrm{N}_G(P) \qquad \textit{if and only if} \qquad Q \leqslant P.$$

Recall that the normaliser $\mathrm{N}_G(P)$ is the set of all $x \in G$ such that $x^{-1}Px = P$.

Proof: Since $P \leqslant \mathrm{N}_G(P)$, if $Q \leqslant P$ then certainly $Q \leqslant \mathrm{N}_G(P)$.

Conversely, suppose $Q \leqslant \mathrm{N}_G(P)$. Since $x^{-1}Px = P$ for all $x \in \mathrm{N}_G(P)$, by definition, this means $P \trianglelefteqslant \mathrm{N}_G(P)$. We may now apply the Second Isomorphism Theorem to the normal subgroup P and the subgroup Q of $\mathrm{N}_G(P)$: it tells us that $P \cap Q \trianglelefteqslant Q$, $PQ \leqslant G$ and

$$PQ/P \cong Q/(P \cap Q).$$

Since Q is a p-group, we conclude $|PQ/P|$ is a power of p. As $|P|$ is a power of p, it follows that $|PQ|$ is a power of p; that is, PQ is a p-subgroup of G. But as $P \leqslant PQ$ and P is a Sylow p-subgroup (a p-subgroup of largest possible order), we conclude $PQ = P$. Therefore

$$Q \leqslant PQ = P.$$

□

Lemma 9.6 *Let G be a group and H and K be subgroups of G. Then the number of conjugates of H of the form $x^{-1}Hx$ where $x \in K$ equals $|K : K \cap \mathrm{N}_G(H)|$.*

This lemma is simply a variant of Theorem 8.22(iv). Indeed that result can be retrieved from this lemma by taking $K = G$. We merely give a sketch proof since it is basically the same as that part of the theorem.

Proof: If $x, y \in K$, then

$$\begin{aligned} x^{-1}Hx = y^{-1}Hy \quad &\iff \quad yx^{-1}Hxy^{-1} = H \\ &\iff \quad (xy^{-1})^{-1}H(xy^{-1}) = H \\ &\iff \quad xy^{-1} \in \mathrm{N}_G(H) \\ &\iff \quad xy^{-1} \in K \cap \mathrm{N}_G(H) \\ &\iff \quad (K \cap \mathrm{N}_G(H))x = (K \cap \mathrm{N}_G(H))y, \end{aligned}$$

and it follows

$$(K \cap \mathrm{N}_G(H))x \mapsto x^{-1}Hx$$

is a bijection from the cosets of $K \cap \mathrm{N}_G(H)$ in K to the set of conjugates $x^{-1}Hx$ with $x \in K$. □

We have established that our finite group G (of order $p^n m$ where p does not divide m) has at least one Sylow p-subgroup P (of order p^n). Let

$$\Sigma = \{\, g^{-1}Pg \mid g \in G \,\},$$

the set of all conjugates of P in G. This consists of *some* of the Sylow p-subgroups of G. In establishing part (ii) of Sylow's Theorem, we shall show that it is, in fact, the set of *all* the Sylow p-subgroups of G. Most of parts (ii)–(iv) are established by the same method, which we shall now describe.

Method: Let Q be any p-subgroup of G. If $R \in \Sigma$, let

$$\Gamma_R = \{\, x^{-1}Rx \mid x \in Q \,\} \subseteq \Sigma,$$

the set of conjugates of R by elements of Q. Then Lemma 9.6 says

$$|\Gamma_R| = |Q : Q \cap \mathrm{N}_G(R)|. \tag{9.2}$$

Note that $|\Gamma_R| = 1$ if and only if $Q \cap \mathrm{N}_G(R) = Q$; that is, $Q \leqslant \mathrm{N}_G(R)$. Since R is a Sylow p-subgroup of G, Lemma 9.5 tells us that $|\Gamma_R| = 1$ if and only if $Q \leqslant R$. Since $|Q|$ is a power of p, we may therefore record the following:

Observation 1: *For any p-subgroup Q of G, $|\Gamma_R|$ is a power of p and it equals 1 if and only if $Q \leqslant R$.*

Claim: If $R, S \in \Sigma$, then either $\Gamma_R = \Gamma_S$ or $\Gamma_R \cap \Gamma_S = \varnothing$.

Suppose $\Gamma_R \cap \Gamma_S \neq \varnothing$. This means $x^{-1}Rx = y^{-1}Sy$ for some $x, y \in Q$. Then $R = xy^{-1}Syx^{-1}$ and if $z \in Q$, then

$$z^{-1}Rz = z^{-1}xy^{-1}Syx^{-1}z = (yx^{-1}z)^{-1}S(yx^{-1}z) \in \Gamma_S.$$

It follows that $\Gamma_R \subseteq \Gamma_S$ and therefore, by symmetry, the two sets of conjugates are equal: $\Gamma_R = \Gamma_S$.

We can therefore partition Σ into the sets Γ_R for various $R \in \Sigma$, so we record:

Observation 2: *For each p-subgroup Q of G, there exist $R_1, R_2, \ldots, R_k \in \Sigma$ such that Σ is the disjoint union*

$$\Sigma = \Gamma_{R_1} \cup \Gamma_{R_2} \cup \cdots \cup \Gamma_{R_k}.$$

We now apply these observations for various choices of Q.

Application 1: Take $Q = P$ (our original Sylow p-subgroup). Since each member of Σ has order p^n, precisely one of them contains P, namely P itself. Hence, by Observation 1, there is a single choice of R such that $|\Gamma_R| = 1$ and for all other choices of R, $|\Gamma_R|$ is a power of p. Therefore when we partition Σ as

$$\Sigma = \Gamma_{R_1} \cup \Gamma_{R_2} \cup \cdots \cup \Gamma_{R_k},$$

exactly one of the sets has size 1 and the others have order divisible by p, so

$$|\Sigma| = |\Gamma_{R_1}| + |\Gamma_{R_2}| + \cdots + |\Gamma_{R_k}| = 1 + mp$$

for some m. Thus $|\Sigma| \equiv 1 \pmod{p}$.

Application 2: Take Q to be any Sylow p-subgroup of G. There exist R_1, R_2, …, R_k (depending on Q) such that

$$\Sigma = \Gamma_{R_1} \cup \Gamma_{R_2} \cup \cdots \cup \Gamma_{R_k},$$

a disjoint union, and hence

$$|\Gamma_{R_1}| + |\Gamma_{R_2}| + \cdots + |\Gamma_{R_k}| = |\Sigma| \equiv 1 \pmod{p}.$$

Therefore some $|\Gamma_{R_i}|$ is not divisible by p and so, by Observation 1, $|\Gamma_{R_i}| = 1$ and $Q \leqslant R_i$. But Q and R_i are Sylow p-subgroups of G, that is, $|Q| = p^n = |R_i|$, so we conclude

$$Q = R_i \in \Sigma.$$

Hence

every Sylow p-subgroup of G is a conjugate of P;

that is, part (ii) of Sylow's Theorem holds.

This tells us that Σ is the set of all Sylow p-subgroups of G. As we have shown $|\Sigma| \equiv 1 \pmod{p}$ (in Application 1), we have shown that the number of Sylow p-subgroups of G is congruent to 1 (mod p).

Also, by Theorem 8.22(iv),

$$|\Sigma| = |G : \mathrm{N}_G(P)| = \frac{|G|/|P|}{|\mathrm{N}_G(P)|/|P|} = \frac{|G : P|}{|\mathrm{N}_G(P) : P|} = \frac{m}{|\mathrm{N}_G(P) : P|}.$$

Hence the number of Sylow p-subgroups of G divides m.

Thus part (iii) of Sylow's Theorem holds.

Application 3: Now take Q to be any p-subgroup of G (not necessarily a Sylow subgroup). There exist R_1, R_2, …, R_k such that we have a disjoint union

$$\Sigma = \Gamma_{R_1} \cup \Gamma_{R_2} \cup \cdots \cup \Gamma_{R_k}.$$

Since $|\Sigma| \equiv 1 \pmod{p}$, as least one $|\Gamma_{R_i}|$ is not divisible by p. Therefore, by Observation 1, $Q \leqslant R_i$ for this value of i. Thus, Q is contained in the Sylow p-subgroup R_i, which establishes part (iv) of Sylow's Theorem.

This completes the proof of the theorem. □

We shall now illustrate some applications of Sylow's Theorem. Note that if a group G has a unique Sylow p-subgroup P, then

$$x^{-1}Px = P \qquad \text{for all } x \in G$$

and therefore

$$P \trianglelefteq G.$$

Thus one common application of Sylow's Theorem is to find normal subgroups and hence show that certain types of group are not simple.

Example 9.7 *Show that there is no simple group of order* 40.

SOLUTION: Let G be a group of order $40 = 2^3 \cdot 5$. The number of Sylow 5-subgroups of G is congruent to 1 (mod 5) and divides 8. Hence there is one Sylow 5-subgroup in G and this is therefore a normal subgroup of G of order 5. Hence G is not simple. □

Example 9.8 *Show that there is no simple group of order* 70.

SOLUTION: Let G be a group of order $70 = 2 \cdot 5 \cdot 7$. The number of Sylow 5-subgroups of G is congruent to 1 (mod 5) and divides 14. Hence there is one Sylow 5-subgroup in G.

In the same way, the number of Sylow 7-subgroups of G is congruent to 1 (mod 7) and divides 10. Hence there is one Sylow 7-subgroup in G.

Thus G has both a normal subgroup of order 5 and a normal subgroup of order 7. We conclude that G is not simple. □

Example 9.9 *Show that there is no simple group of order* 56.

SOLUTION: Let G be a group of order $56 = 2^3 \cdot 7$. Let n_2 and n_7 denote the number of Sylow 2-subgroups and the number of Sylow 7-subgroups of G, respectively.

Sylow's Theorem tells us that $n_7 \equiv 1 \pmod 7$ and that n_7 divides 8. Hence there are two possibilities: either $n_7 = 1$ or $n_7 = 8$. If $n_7 = 1$, then there is a unique Sylow 7-subgroup and this is a normal subgroup of order 7. In this case, G is not simple.

Suppose then that $n_7 = 8$. Let $S_1, S_2, \ldots, S_8$ denote the eight Sylow 7-subgroups. Note that each S_i contains the identity element and six elements of order 7 (since $S_i \cong C_7$). Now if $i \neq j$, the intersection $S_i \cap S_j$ is a proper subgroup of both S_i and S_j, and Lagrange's Theorem tells us that $S_i \cap S_j = \mathbf{1}$.

Hence each S_i contains six elements of order 7 that lie in no other Sylow 7-subgroup of G and we conclude that between them the eight Sylow 7-subgroups contain $8 \times 6 = 48$ elements of order 7.

There are only 8 remaining elements in G which do not have order 7 (including the identity element in these eight) and any Sylow 2-subgroup must therefore consist of some of these eight elements not of order 7. However, a Sylow 2-subgroup of G has order $2^3 = 8$ and we therefore conclude that there is exactly one Sylow 2-subgroup of G consisting of these eight elements. Hence, if $n_7 = 8$, then $n_2 = 1$ and G has a normal subgroup of order 8.

Thus in either case, G is not simple. □

Example 9.10 *For each prime p dividing* 60*, determine the number of Sylow p-subgroups of the alternating group A_5 of degree* 5.

SOLUTION: $|A_5| = 60 = 2^2 3 \cdot 5$. Let n_2, n_3 and n_5 denote the number of Sylow 2-, 3- and 5-subgroups in A_5. Then

$$\begin{aligned} n_2 &\equiv 1 \pmod 2, & n_2 &\mid 15 \\ n_3 &\equiv 1 \pmod 3, & n_3 &\mid 20 \\ n_5 &\equiv 1 \pmod 5, & n_5 &\mid 12. \end{aligned}$$

Hence

$$\begin{aligned} n_2 &= 1, 3, 5 \text{ or } 15 \\ n_3 &= 1, 4 \text{ or } 10 \\ n_5 &= 1 \text{ or } 6. \end{aligned}$$

Since A_5 is simple, none of the Sylow subgroups can be normal in A_5 and so we conclude $n_p \neq 1$ for $p = 2$, 3 and 5. Hence

there are six Sylow 5-subgroups in A_5.

For the others, recall that if P is a Sylow p-subgroup of a group G, then the set of all Sylow p-subgroups is the set of conjugates of P and hence the number of them equals the index of the normaliser $\mathrm{N}_G(P)$.

In Example 9.3(ii), we showed that

$$H = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

is a Sylow 2-subgroup of A_5. Now we know $H \trianglelefteqslant A_4$, so the normaliser $\mathrm{N}_{A_5}(H)$ contains A_4. Thus $1 < |A_5 : \mathrm{N}_{A_5}(H)| \leqslant 5$. But Question 3(c) on Problem Sheet VII tells us that A_5 has no proper subgroup of index less than 5. Hence

$$n_2 = |A_5 : \mathrm{N}_{A_5}(H)| = 5;$$

that is,

there are five Sylow 2-subgroups in A_5.

Similarly, if $T = \langle(1\ 2\ 3)\rangle$, then $|A_5 : \mathrm{N}_{A_5}(T)| \neq 4$, and therefore

$$n_3 = |A_5 : \mathrm{N}_{A_5}(T)| = 10;$$

that is,

there are ten Sylow 3-subgroups in A_5.

□

Chapter 10

Classification of Groups of Small Order

We finish the course by applying the methods we have developed to provide a classification or groups of small order. We intend to specify a list of groups of order n such that every group of order n is isomorphic to one on the list. We do this for $1 \leqslant n \leqslant 15$.

A group of order 1 *is trivial.*

Up to isomorphism there is one group of order 1.

Corollary 2.23 tells us:

If p is prime, then any group of order p is isomorphic to C_p, a cyclic group of order p.

Up to isomorphism there is one group of order p.

This deals with groups of order 2, 3, 5, 7, 11, 13, ...

Groups of order p^2

Lemma 10.1 *Let G be a group such that $G/\mathrm{Z}(G)$ is cyclic. Then G is abelian.*

Proof: Suppose $G/\mathrm{Z}(G) = \langle \mathrm{Z}(G)x \rangle$ for some $x \in G$. Then, as G is the union of the cosets of $\mathrm{Z}(G)$,

$$G = \bigcup_{n \in \mathbb{Z}} \mathrm{Z}(G)x^n,$$

so every element of G has the form zx^n for some $z \in \mathrm{Z}(G)$ and $n \in \mathbb{Z}$. Thus

$$G = \langle \mathrm{Z}(G), x \rangle.$$

Consider the centraliser $\mathrm{C}_G(x)$. Certainly x commutes with itself, while, by definition, every element of $\mathrm{Z}(G)$ commutes with every element in G and so in particular with x. Thus

$$\mathrm{Z}(G) \leqslant \mathrm{C}_G(x) \qquad \text{and} \qquad x \in \mathrm{C}_G(x),$$

so

$$G = \langle \mathrm{Z}(G), x \rangle \leqslant \mathrm{C}_G(x).$$

Hence every element of G commutes with x, so $x \in \mathrm{Z}(G)$. Therefore

$$G = \langle \mathrm{Z}(G), x \rangle = \mathrm{Z}(G)$$

and so G is abelian. □

Theorem 10.2 *Let p be prime. Any group of order p^2 is abelian and so is isomorphic to C_{p^2} or $C_p \times C_p$.*

PROOF: Let G be a group of order p^2. It then follows from the Class Equation that, since G is a p-group, then $\mathrm{Z}(G) \neq \mathbf{1}$ (see Question 11 on Problem Sheet VIII). Hence either

$$|\mathrm{Z}(G)| = p \text{ or } p^2.$$

But if $|G/\mathrm{Z}(G)| = p$, then $G/\mathrm{Z}(G)$ is cyclic, so $G = \mathrm{Z}(G)$, contrary to assumption. Therefore $|\mathrm{Z}(G)| = p^2$ and $G = \mathrm{Z}(G)$ is abelian. Therefore, by the Fundamental Theorem of Finite Abelian Groups, either

$$G \cong C_{p^2} \quad \text{or} \quad G \cong C_p \times C_p.$$

□

In conclusion,

Up to isomorphism there are two groups of order p^2 (for p prime).

This deals with groups of order 4, 9, 25, ...

Groups of order $2p$

Let p be an odd prime and consider groups of order $2p$. By the Fundamental Theorem of Finite Abelian Groups, an abelian group of order $2p$ is isomorphic to

$$C_2 \times C_p \cong C_{2p}.$$

Theorem 10.3 *Let G be a group of order $2p$ where p is an odd prime. Then $G \cong C_{2p}$ or D_{2p}, depending upon whether G is abelian or non-abelian.*

PROOF: The number of Sylow p-subgroups of G is congruent to 1 (mod p) and divides 2. Therefore G has precisely one Sylow p-subgroup P. As $|P| = p$, we know $P \cong C_p$.

If $x \in G \setminus P$, then $o(x) \neq p$, since an element of order p must generate the Sylow p-subgroup P. If G contains an element of order $2p$, then $G \cong C_{2p}$. So suppose that G is non-abelian and therefore

$$o(x) = 2 \qquad \text{for all } x \in G \setminus P.$$

(Note the identity lies in P.)

Fix a generator a for P and an element $b \in G \setminus P$. So $o(a) = p$ and $o(b) = 2$. The elements of P are $1, a, \ldots, a^{p-1}$ and the elements of the coset Pb are $b, ab, \ldots, a^{p-1}b$, so

$$G = \{1, a, \ldots, a^{p-1}, b, ab, \ldots, a^{p-1}b\} = \langle a, b \rangle.$$

Now $(a^i b)^2 = 1$ for all i, so $a^i b a^i b = 1$. Therefore

$$ba^i = a^{-i}b^{-1} = a^{-i}b.$$

We are now able to completely specify the multiplication in G:

$$(a^ib^j)(a^kb^\ell) = \begin{cases} a^{i+k}b^\ell & \text{if } j = 0 \\ a^{i-k}b^{j+\ell} & \text{if } j = 1. \end{cases}$$

Hence, up to isomorphism, there is at most one non-abelian group of order $2p$. (In theory, at this stage in our calculations, we do not know that the above multiplication actually does define a group.) However, the dihedral group D_{2p} is a non-abelian group of order $2p$ and therefore our G must be isomorphic to D_{2p}. □

If p is an odd prime, there are two groups of order $2p$ up to isomorphism.

This deals with groups of order 6, 10, 14, 22, ... Note $D_6 = S_3$.

Groups of order 8

By the Fundamental Theorem of Finite Abelian Groups, an abelian group of order 8 is isomorphic to one of

$$C_8, \qquad C_2 \times C_4 \qquad \text{or} \qquad C_2 \times C_2 \times C_2.$$

Let G be a non-abelian group of order 8. An element in G has order 1, 2, 4 or 8. If G contains an element of order 8, then $G \cong C_8$ and it would be abelian. If $x^2 = 1$ for all $x \in G$, then G would be abelian (see Question 11 on Problem Sheet I). Hence G contains at least one element a of order 4.

Let $N = \langle a \rangle$, a subgroup of order 4 in G, so $N \trianglelefteq G$ (as it has index 2. Choose $b \in G \setminus N$. Then either $o(b) = 2$ or $o(b) = 4$. Since $G/N \cong C_2$, we know $Nb^2 = N1$ and therefore $b^2 \in N$ in either case. As a^2 is the unique element of order 2 in N, we conclude either

$$b^2 = 1 \qquad \text{or} \qquad b^2 = a^2.$$

The elements of N are 1, a, a^2, a^3 and the elements of the coset Nb are b, ab, a^2b, a^3b, so

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

Now $b^{-1}ab \in N$ and $o(b^{-1}ab) = o(a) = 4$, so

$$b^{-1}ab = a \text{ or } a^3.$$

If $b^{-1}ab = a$, then $ab = ba$ and it would follow that $G = \langle a, b \rangle$ is abelian. Therefore

$$b^{-1}ab = a^3 = a^{-1},$$

so

$$b^{-1}a^{-i}b = (b^{-1}ab)^{-i} = (a^{-1})^{-i} = a^i$$

and we deduce

$$ba^i = a^{-i}b = a^{3i}b.$$

Hence

$$(a^ib^j)(a^kb^\ell) = \begin{cases} a^{i+k}b^\ell & \text{if } j = 0 \\ a^{i+3k}b & \text{if } j = 1,\ \ell = 0 \\ a^{i+3k}b^2 & \text{if } j = \ell = 1. \end{cases}$$

So we would have completely determined the multiplication in G once we knew whether $b^2 = 1$ or a^2. Therefore, there are, up to isomorphism, at most two non-abelian group of order 8. We already know two such groups, namely D_8 and Q_8, so these two must be the only two that exist.

This establishes:

Theorem 10.4 *Any group of order* 8 *is isomorphic to one of*

$$C_8, \qquad C_2 \times C_4, \qquad C_2 \times C_2 \times C_2, \qquad D_8 \qquad \text{or} \qquad Q_8.$$

□

There are five groups of order 8 *up to isomorphism.*

Groups of order pq

We shall consider groups of order pq where $p < q$ are distinct primes. We shall actually only consider a special case, namely

$$p \text{ does } \textit{not} \text{ divide } q - 1.$$

Let G be a group of order pq where p and q are distinct primes with $p < q$ and such that p does not divide $q - 1$. Let n_p and n_q denote the number of Sylow p- and Sylow q-subgroups in G, respectively. Then, by Sylow's Theorem,

$$n_p \equiv 1 \pmod{p} \qquad \text{and} \qquad n_p \text{ divides } q$$

and

$$n_q \equiv 1 \pmod{q} \qquad \text{and} \qquad n_q \text{ divides } p.$$

The first of these tells us that $n_p = 1$, since $n_p = q$ is impossible since $q \not\equiv 1 \pmod{p}$ by assumption. The second tells us that $n_q = 1$, since $p < q$, so certainly $p \not\equiv 1 \pmod{q}$.

Let P be the unique Sylow p-subgroup and Q be the unique Sylow q-subgroup of G. Then $P \trianglelefteq G$ and $Q \trianglelefteq G$. As they have coprime order, Lagrange's Theorem tells us $P \cap Q = \mathbf{1}$. Consider PQ. It is a subgroup of G, since both P and Q are normal, and it contains both P and Q. Therefore both p and q divide $|PQ|$, so we conclude $G = PQ$. This checks all conditions for a direct product in Theorem 5.6 and we have shown

$$G \cong P \times Q \cong C_p \times C_q \cong C_{pq}.$$

Theorem 10.5 *Let G be a group of order pq where p and q are distinct primes with $1 < p < q$. Suppose that p does not divide $q - 1$. Then $G \cong C_{pq}$.* □

Up to isomorphism, there is one group of order pq when $1 < p < q$ and p does not divide $q - 1$.

This deals with groups of order 15, 33, 35, ...

Groups of order 12

An abelian group of order 12 is isomorphic to either

$$C_2 \times C_2 \times C_3 \cong C_2 \times C_6 \qquad \text{or} \qquad C_4 \times C_3 \cong C_{12}.$$

We already know two non-abelian groups of order 12, namely the dihedral group D_{12} of order 12 and the alternating group A_4 of degree 4. There is actually one more.

Example 10.6 Let T be the subgroup of S_{12} generated by the permutations

$$\alpha = (1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9\ 10\ 11\ 12) \quad \text{and} \quad \beta = (1\ 7\ 4\ 10)(2\ 12\ 5\ 9)(3\ 11\ 6\ 8).$$

If we apply the generation algorithm (see Chapter 2) to T we find that its elements are:

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

Here $\alpha\beta \neq \beta\alpha$, so T is non-abelian. From the cycle structure, we see that T has one element of order 2. We know A_4 has three elements of order 2 and D_{12} has seven elements of order 2. Therefore

$$T \ncong A_4 \qquad \text{and} \qquad T \ncong D_{12}.$$

Theorem 10.7 *If G is a group of order 12, then G is isomorphic to one of*

$$C_2 \times C_6, \qquad C_{12}, \qquad A_4, \qquad D_{12} \qquad \text{or} \qquad T.$$

Up to isomorphism, there are five groups of order 12.

PROOF: Let G be a non-abelian group of order 12. Let n_2 and n_3 be the number of Sylow 2- and Sylow 3-subgroups respectively in G. Then, by Sylow's Theorem,

$$n_2 \equiv 1 \pmod 2, \quad n_2 \mid 3 \qquad \text{and} \qquad n_3 \equiv 1 \pmod 3, \quad n_3 \mid 4.$$

Therefore

$$n_2 = 1 \text{ or } 3, \qquad n_3 = 1 \text{ or } 4.$$

Suppose $n_3 = 4$. We then count elements in the Sylow 3-subgroups (any pair of which must intersect trivially by Lagrange's Theorem) to see that G contains $4 \times 2 = 8$ elements of order 3. This only leaves four elements of other orders, so we conclude there must be a unique Sylow 2-subgroup (of order 4); that is, $n_2 = 1$. Hence it is not possible that $n_2 = 3$ and $n_3 = 4$ and we consider three cases.

Case 1: $n_2 = n_3 = 1$.

There are unique Sylow 2- and 3-subgroups P and Q (respectively) in G which are normal in G. Here $P \cong C_4$ or $C_2 \times C_2$ (from the classification of groups of order p^2) and $Q \cong C_3$. As in the classification of groups of order pq, by Lagrange's Theorem, $P \cap Q = \mathbf{1}$ and $G = PQ$. Hence, by Theorem 5.6

$$G \cong P \times Q \cong C_4 \times C_3 \quad \text{or} \quad C_2 \times C_2 \times C_3.$$

Hence in this case, G is isomorphic to one of C_{12} or $C_2 \times C_6$.

Case 2: $n_2 = 1$ and $n_3 = 4$.

Let N be the unique Sylow 2-subgroups, so $N \trianglelefteqslant G$ and $N \cong C_4$ or $N \cong C_2 \times C_2 \cong V_4$.

Subcase 2a: $N \cong C_4$.

Let $N = \langle a \rangle$ and $H = \langle b \rangle$ be a Sylow 3-subgroup of G. Then $b^{-1}ab = a^i$ for some i. Then

$$a = b^{-3}ab^3 = b^{-2}a^ib^2 = b^{-1}(b^{-1}ab)^ib = b^{-1}a^{i^2}b = a^{i^3},$$

so $4 \mid (i^3 - 1)$. The only possibility is $i = 1$ (as $i = 2$ and $i = 3$ do not satisfy this condition). This means that $ab = ba$, so $G = \langle a, b \rangle$ is abelian, which contradicts $n_3 = 4$.

Subcase 2b: $N \cong C_2 \times C_2 \cong V_4$.

If $H = \langle d \rangle$ is a Sylow 3-subgroup of G, then when we conjugate the elements of order 2 in N by d, we must permute them as a 3-cycle (since $o(d) = 3$). Hence we can assume $N = \{1, a, b, c\}$, where

$$d^{-1}ad = b, \qquad d^{-1}bd = c, \qquad d^{-1}cd = a.$$

Hence we determine that $da = cd$, $db = ad$ and $dc = bd$. Hence any product $(xd^i)(yd^j)$ where $x, y \in \{1, a, b, c\}$ is now uniquely specified. We conclude that there is at most one group of order 12 with $n_2 = 1$ and $n_3 = 4$. But we already know that the alternating group A_4 is a non-abelian group of order 12 and it has a unique Sylow 2-subgroup and four Sylow 3-subgroups, therefore $G \cong A_4$ in this cases.

Case 3: $n_2 = 3$ and $n_3 = 1$.

Let N be the unique Sylow 3-subgroup of G, so $N = \langle a \rangle$ for some a of order 3 and $N \trianglelefteqslant G$. Let H be a Sylow 2-subgroup. Every element of G can be expressed as a^ix where $0 \leqslant i \leqslant 2$ and $x \in H$. As in the classification of groups of order 8 and in Subcase 2, to determine the multiplication in G it is enough to establish that conjugation of elements in N by elements in H are essentially uniquely determined.

If $H \cong C_4$, the generator b for H cannot commute with a (as G is non-abelian), so $b^{-1}ab = a^2 = a^{-1}$. From this we conclude $b^{-1}a^{-1}b = a$ and $ba = a^{-1}b$. Hence all products $(a^ib^j)(a^kb^\ell)$ are uniquely determined. This shows that there is at most one group of order 12 with $n_2 = 3$, $n_3 = 1$ and cyclic Sylow 2-subgroup. However, T is one such group and we deduce $G \cong T$. (Indeed, it is this line of argument that enables us to go searching for such a group of order 12 and hence determine that T exists.)

If $H \cong C_2 \times C_2$, them at least one element x in H which satisfies $x^{-1}ax = a^{-1}$. Suppose $H = \{1, x, y, z\}$. If $y^{-1}ay = a^{-1}$, then $z = xy$ actually commutes with a:

$$z^{-1}az = y^{-1}x^{-1}axy = y^{-1}a^{-1}y = (y^{-1}ay)^{-1} = (a^{-1})^{-1} = a.$$

Similarly if y commutes with a, then $z^{-1}az = a^{-1}$. Hence, without loss of generatity, we can assume $y^{-1}ay = a^{-1}$ and $z^{-1}az = a$. In this way, all products $(a^i h)(a^j k)$ with $h, k \in H$ are determined and we deduce that there is at most one such group. However, D_{12} does satisfy the hypotheses, so we conclude $G \cong D_{12}$ in this case.

This completes the proof. $\square$