A First Course in Group Theory

Aditi Kar

April 10, 2017

These are Lecture Notes for the course entitled ‘Groups and Group Actions’ aimed at 2nd and 3rd year undergraduate students of Mathematics in Royal Holloway University of London.

The course involves 33 hours of lectures and example classes.

Assessment. Cumulative End of Year Exam (100 %). Formative assessments are in the form of weekly problem sheets, released every Tuesday and due the following Tuesday. I will include important course material and examples in the Problem sheets. It is imperative therefore to think through/ solve the Problems on a regular basis.

Recommended Texts.
A First Course in Abstract Algebra, by John B. Fraleigh
Introduction to Algebra, PJ Cameron, OUP
Theory of Groups-An Introduction, JJ Rotmann, Springer.

Chapter 1

Groups

1.1 What is Group Theory?

Group Theory is the study of algebraic structures called groups; just as numbers represent 'how many', groups represent symmetries in the world around us. Groups are ubiquitous and arise in many different fields of human study: in diverse areas of mathematics, in physics, in the study of crystals and atoms, in public key cryptography and even in music theory.

Figure 1.1: Evariste Galois 1811-1832

The foundations of Group Theory were laid in the work of many - Cauchy, Langrange, Abel to name a few. The central figure was undoubtedly the dashing French mathematician Evariste Galois. Galois famously died fighting a duel at the premature age of 21. The mathematical doodles he left behind were invaluable. The adolescent Galois realised that the algebraic solution to a polynomial equation is related to the structure of a *group of permutations* associated with the roots of the polynomial, nowadays called the Galois group of the polynomial. *He found that an equation could be* *'solved by radicals' if one can find a series of subgroups of its Galois group, each one normal in its successor with abelian quotient, equivalently its Galois group is solvable.* This is formal jargon but what it means is, he'd discovered the necessary and sufficient conditions for a polynomial to be solvable by radicals, a problem that had stumped mathematicians for well over 350 years. Galois himself used the word 'group' as we understand it now.

Groups developed in parallel as part of number theoretic and geometric investigations due to Euler, Lagrange, Cauchy and Abel. Modern study of groups has evolved into the field of Geometric Group Theory which thrives on a dialogue between Algebra and Geometry. We may have occasion to see elementary versions of this theory later in the semester.

1.2 First Definitions

Groups are representatives of symmetry in nature. What is *symmetry*? We think objects, whether mathematical or otherwise, are symmetric if they look the same when viewed from different sides. The human body is symmetric about an axis that runs down its middle and you can reflect the left half onto the right half using this axis. Imagine the unit circle: if you rotate it in space about its centre, no matter what the angle (could be any $\theta \in \mathbb{R}$!), it ends up looking the same! Lets now consider an equilateral triangle in detail.

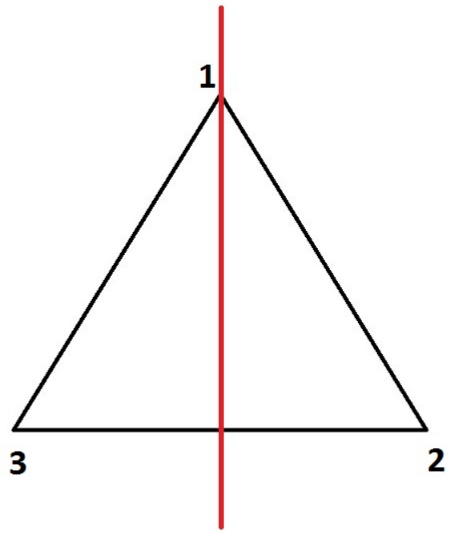

Figure 1.2: Equilateral Triangle: reflection in the red axis corresponds to the permutation (23) of the vertices.

Imagine an axis through the top vertex and passing through the midpoint of the base. The part of the triangle to the left of this line is an exact copy of the part of the triangle to the right of it : in other words, one is a reflection of the other and this reflection *permutes* the vertices sending $1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2$. This allows us to associate the permutation (23) with this reflection. Similarly the permutations (12) and (13) can be interpret as *symmetries* or transformations of the triangle. Also, you can imagine pivotting the triangle at its (circum)-centre and rotating it. A clockwise rotation of 120 degrees brings vertex 1 to vertex 2, 2 to 3 and 3 to 1. This rotation therefore is a realisation of the permutation (123) of a set of three elements.

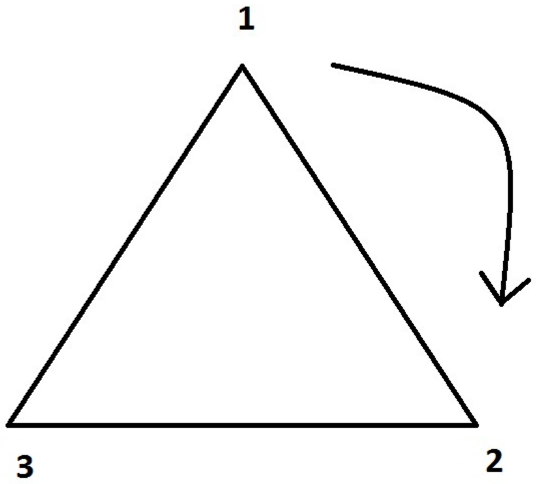

Figure 1.3: Equilateral Triangle: clockwise rotation by 120 degrees corresponds to the permutation (123) of the vertices.

You can follow up your first rotation with another, bringing your old vertex 1 to vertex 3 this time. Composing these two rotations gives rise to a rotation of 240 degrees which in terms of permutations is precisely the 3-cycle (132). Not only that, another iteration of the rotation brings you back to the original position. Observe that you could have inverted any of the transformations by rotating in the anti-clockwise direction. The equilateral triangle having symmetry is represented by the fact that the vertices may be permuted as we have done and the group of permutations of a set of 3 elements can be naturally identified as the group of symmetries of the triangle.

To summarise now, in each of the cases above, we took a symmetric object and associated with it, a set of transformations described as reflections or rotations. In case of the triangle we went on to compose some of these transformations and also invert them. As we will see later, this is a group of permutations in action. We have an underlying set; here, the set of transformations and just like we have composition of transformations we can put a binary operation on the set that satisfies some stipulated axioms or rules like existence of identity transformation and inverses for the elements.

Before we formalise the axioms or rules, let us investigate a dfferent mathematical scenario, that of solving a simple linear equation like $2x = 6$ over the real numbers $\mathbb{R}$. What properties of the real numbers that we take for granted get used in finding the solution to this equation.

First, in $\mathbb{R}$ we can invert 2. We left multiply by $1/2$ to transform the equation to $\frac{1}{2}(2x) = \frac{1}{2}6$. As multiplication in $\mathbb{R}$ is associative, we can rewrite our equation as $(\frac{1}{2}2)x = 3$. We use now that $\frac{1}{2}2 = 1$ and that $1.x = x$ for all x to get $x = 3$.

Likewise, suppose we have a set S with a binary operation $*$; let $a, b \in S$ and suppose we want to solve the equation $a * x = b$. In order to follow the same steps as before, we will need

- an identity element $e \in S$ such that $e * s = s * e = s$ for all $s \in S$.
- an inverse for a, that is, an element $a' \in S$ such that $a' * a = e$
- Associativity for $*$.

These turn out to be precisely the axioms we impose to define a group.

Definition 1. *A* ***binary operation*** $*$ *on a set* S *is a rule that assigns to each ordered pair of elements* (a, b) *of the set some element of the set that we write as* $a * b$.

Examples.

1. Addition in the set of integers: $(x, y) \mapsto x + y$ for all $x, y \in \mathbb{Z}$
2. Multiplication in the set of all real numbers $(x, y) \mapsto xy$ for all $x, y \in \mathbb{R}$.

Exercise 1. *Binary operations need not be associative. Check that* $\mathbb{R}$ *with the binary operation of division* $(a, b) \mapsto a/b$ *is not associative. Check also that the rational numbers* $\mathbb{Q}$ *endowed with the arithmetic mean* $(a, b) \mapsto \frac{a+b}{2}$ *is not associative.*

Definition 2. *A* ***group*** $(G, *)$ *is a set* G *together with a binary operation* $*$ *such that the following axioms are satisfied:*
$\mathcal{G}_1$: *the binary operation is associative i.e.* $a * (b * c) = (a * b) * c$ *for all* $a, b, c \in G$.

$\mathcal{G}_2$: *there is an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$. The element e is called the identity element of the group.*
$\mathcal{G}_3$: *For each $a \in G$ there is an element $a' \in G$, called the inverse of a, such that $a * a' = a' * a = e$.*

Remarks. It is customary to shorten $(G, *)$ to G and write ab for the element $a * b$.

Examples of Groups

1.) Integers with addition $(\mathbb{Z}, +)$. Similarly, the real numbers $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are groups.
2.) If $(\mathbb{F}, +, .)$ is a field then $(\mathbb{F}\backslash\{0\}, .)$ is a group. Here, one can take $\mathbb{F}$ to be $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Q}$.
3.) Let $M(2, \mathbb{R})$ be the set of all 2-by-2 matrices with real entries and consider the binary operation of matrix addition $(A, B) \mapsto A + B$. Then $(M(2, \mathbb{R}), +)$ is a group. However $M(2, \mathbb{R})$ is not a group with respect to matrix multiplication: the problem is that not all matrices are invertible.
4.) Let $GL(2, \mathbb{R}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0\}$ be the set of all 2-by-2 invertible matrices with real entries. Then $GL(2, \mathbb{R})$ is a group with respect to matrix multiplication.

Exercise 2. *Check that the axioms for a group hold in each of the examples above.*

Abelian Groups

A binary operation may not be commutative: recall that a binary operation $*$ defined on a set S is commutative if $a * b = b * a$ for all $a, b \in S$. A group whose associated operation is commutative is called an **Abelian group**. All the examples in (1)-(4) are Abelian except for $GL(2, \mathbb{R})$, the group of invertible matrices with respect to matrix multiplication. As we know, matrix multiplication is not commutative and so $GL(2, \mathbb{R})$ with matrix multiplication is a **non-Abelian** group.

Some preliminary results

Let us establish some simple results that follow from the defining axioms of a group.

Theorem 1 (Right and left cancellation laws hold in a group)**.** *Let G be a group. If $ab = ac$ for some $a, b, c \in G$ then $b = c$. Similarly, if $ab = cb$ for some $a, b, c \in G$, then $a = c$.*

Proof. The proof proceeds like our earlier solution to the linear equation. Suppose for some $a, b, c \in G$, $ab = ac$. If a' is an inverse for a, then we can left multiply to get $a'(ab) = a'(ac)$. By associativity, $(a'a)b = (a'a)c$. Finally, since $a'a = 1$ and $1.x = x$ for all $x \in G$, we conclude that $b = c$. This proves the left cancellation law in G. The proof of the right cancellation law is similar. □

Theorem 2. *Let G be a group and let $a, b \in G$. Let x represent a variable (unknown). Then, the linear equations $ax = b$ and $xa = b$ have unique solutions.*

Proof. Consider $ax = b$ and let a' be an inverse for a. Then $a'(ax) = a'b$ and using associativity, properties of inverses and the identity element, we can conclude as in the proof of Theorem 1 that $x = a'b$. To show that this solution is unique we argue by contradiction. Suppose x_1, x_2 are distinct solutions of the equation $ax = b$. Then $ax_1 = ax_2$. By Theorem 1, left cancellation holds, so $x_1 = x_2$. Similarly ba' is a solution of the equation $xa = b$ and moreover using the right cancellation law, we get that the solution is unique. □

Theorem 3. *Let G be a group. The following statements are true. 1.) Suppose e, e' both serve as identity elements in G so that $ae = ea = a$ and $ae' = e'a = a$ for all $a \in G$. Then $e = e'$.*

2.) Let $e \neq a \in G$. Suppose a_l is a left inverse for a and $a_l a = e$ while a_r is a right inverse for a. Then $a_l = a_r$.

3.) (Uniqueness of inverses) If a', a'' are both inverses for a, then $a' = a''$. From henceforth, we will write a^{-1} for the inverse of a.

Proof. 1.) Suppose $e, e' \in G$ are such that $ae = ea = a$ and $ae' = e'a = a$ for all $a \in G$. We play e, e' against each other as follows: $e = ee' = e'$.

2.) Similarly $a_l = a_l e = a_l(aa_r) = (a_l a)a_r = ea_r = a_r$.

3.) Left as exercise. □

Exercise 3. *Prove that we can weaken the axioms for a group $(G, *)$ as follows.*

1. *The binary operation is associative.*
2. *There exists a left identity e in G such that $ex = x$ for all $x \in G$.*
3. *For each $a \in G$ there exists a left inverse $a' \in G$ such that $a'a = e$.*

1.3 Finite groups and Group Tables

The cardinality of the underlying set is called the **order** of a group, written as $|G|$. Up till now, all our examples have infinite order. In this section we will build finite groups of small order using group tables.

Every group must have an identity element e, so $|G| \geq 1$. Can a singleton set $G = \{e\}$ be made into a group? Yes, this is called the trivial group. Here e is the identity element and the binary operation is specified by $ee = e$ which also means that e is its own inverse. In fact, in any group, the identity element is its own inverse.

We now take a set with two elements $\{e, a\}, a \neq e$ and try to put a group structure on it. We use a table where we put the set elements in the same order on the first row and first column with the identity element first, as below.

$*$	e	a
e		
a		

(1.1)

Then the entry in the i-th row and j-th column is (i-th entry on the left)(j-th entry on the top). The above table should be completed as follows

$*$	e	a
e	ee	ea
a	ae	aa

(1.2)

As e is the identity element in order to define the group structure, we need only decide $aa =$? Using the cancellation laws from earlier we know if $aa = a$ then $a = e$ which is not true. Therefore $aa = e$ making a its own inverse.

$*$	e	a
e	e	a
a	a	e

(1.3)

All group axioms hold except that we have not checked for associativity. This can be checked case by case and as there are only two elements of which one os the identity, this is not hard. Apparently, there is only one group of order 2: if the identity element is labelled e and the non-identity element is labelled a then the group table will look exactly like the one above. We can identify this group with integers modulo 2, namely $\mathbb{Z}_2$ under addition.

Observation 4 (Sudoku games). *An important consequence of the Right and Left Cancellation Laws is that every group element appears once and only once in each row and column.*

Consider now a set $\{e, a, b\}$ of size 3 and let us put a group structure on it.

$*$	e	a	b
e	e	a	b
a	a		
b	b		

(1.4)

If we set $aa = e$, then to avoid repetition in the a-th row, we will need to set $ab = b$ which would put two b's in the last column. So $aa = b$ and we can now complete the table as follows:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(1.5)

We can argue that the group given by the above table is *essentially* the additive group $\mathbb{Z}_3$ of integers modulo 3. Given that $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, match the elements of the group in the table with the elements of $\mathbb{Z}_3$ as follows: $e \mapsto \bar{0}, a \mapsto \bar{1}$ and $b \mapsto \bar{2}$. We see from the lack of choices in writing this table that there is essentially one group of order 3. Associativity can be checked element by element. Again, this is not hard, as there are only two non-identity elements a, b, where $b = a^2$.

When we come to groups of order 4, we see that there can be more than one group operation. Let us look at two possibilities taking $G_1 = \{e, a, b, c\}$ and $G_2 = \{e', a', b', c'\}$ as the underlying sets (e, e' are the identity elements of their the respective sets).

$*$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

$.$	e'	a'	b'	c'
e'	e'	a'	b'	c'
a'	a'			
b'	b'			
c'	c'			

(1.6)

We need to decide what aa and $a'a'$ can be. Two possibilities are e and b' and we proceed from there to complete the tables as follows.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$.$	e'	a'	b'	c'
e'	e'	a'	b'	c'
a'	a'	b'	c'	e'
b'	b'	c'	e'	a'
c'	c'	e'	a'	b'

(1.7)

In G_2, we see that $a'^4 = a'a'a'a' = e'$ and no smaller exponent of a' is the identity. On the other hand, all non-identity elements from G_1satisfy that $x^2 = e$. This tells us that the two groups G_1, G_2 are not the same.

Definition 3. *Let G be a group and a be an element of G. The smallest integer $n > 0$ such that $a^n = e$ is called the order of a.*

In this language, the element a has order 2 in G_1 and the element a' has order 4 in G_2.

Observe that our table for the group of order 2 is replicated in the top left corner of the first group we have of order 4. This is a case of a subset of a group being a group in its own right, with respect to the given binary operation. Such a set is called a **subgroup** and we will study this phenomenon in more detail.

Spotting Abelian Groups from the Tables. Note that all the groups we have drawn tables for, are Abelian. This is evident from the fact that all the tables are symmetric about the main diagonal. The smallest non-abelian group is of order 6 and we will encounter this in the next chapter.

1.3.1 More on Subgroups

We just encountered how one group can sit inside a larger group so that they share the same binary operation. In the ensuing paragraph we look at the notion of subgroups in detail. Recall that a set H is a subset of a set G, denoted $H \subseteq G$ if every element of H is already in G.

Definition 4. *Let G be a group and let S be a subset of G. We say that S is **closed** under the binary operation on G if for every pair s, t of elements of S, we have their product st also belongs to S.*

If a subset S is closed in the sense of the definition above, then the group operation on G induces (the same) binary operation on S.

Definition 5. *Let G be a group and let H be a subset of G. If H is closed under the binary operation on G and H is a group under this induced binary operation then H is called a **subgroup** of G; written $H \leq G$.*

Every group contains itself as a subgroup. It also contains the **trivial subgroup** $\{e\}$, the subgroup whose only element is the identity. A subgroup H which is neither the trivial subgroup nor equal to G is called a **proper subgroup**. For instance the additive group of integers is a proper subgroup in the additive group on the real numbers. The group $G_1 = \{e, a, b, c\}$ from 1.7, which is often called the Klein's 4-group, has 3 proper subgroups: $\{e, a\}$, $\{e, b\}$ and $\{e, c\}$. Incidentally the only proper subgroup of G_2 is $\{e', b'\}$.

We now give a criterion for checking when a subset of a group is a bona fide subgroup.

Theorem 5. *A subset H of a group G is a subgroup of G if and only if*

1. *H is closed under the binary operation on G*
2. *the identity e of G belongs to H*
3. *for every $a \in H$, the inverse a^{-1} of a also belongs to H.*

Proof. If $H \leq G$, then by defintion, H is closed under the binary operation on G. As H with the induced operation is a group in its own right, the defining axioms for a group hold in H and it must have an identity element call it e'. We claim that e' is equal to the identity e of G. By Theorem 2, an equation $ax = a$, where $a \in H$, must have a unique solution. In H, this is e'. However as $H \subset G$ and a also belongs to G itself, the equation has a unique solution in G. This solution must be e and as e, e' both belong to G, we conclude that $e = e'$.

We now verify condition (3). Let $a \in H$. So, a also belongs to G. Let a^{-1} be the inverse for a in G and a' be the inverse for a in H. We invoke Theorem 2 as before and argue that uniqueness of the solution of $ax = e$ implies $a^{-1} = a'$.

Conversely, if the three properties hold in H, then the only group axiom that needs checking is the associative law. But as $a(bc) = (ab)c$ for all elements in G, the same is true for all elements from H. □

You can find your favourite, perhaps more compact variation of the above criterion. Here is one:

Theorem 6. *Let H be a non-empty subset of a group G. Then H is a subgroup of G if and only if*
1.) $a, b \in H$ implies that $ab \in H$, and
2.) $a \in H$ implies $a^{-1} \in H$.

The proof of the Theorem is left to the reader.

1.4 Exercises

1.) Let G be a group. Show that for all $a, b \in G$, the inverse for ab is the element $b^{-1}a^{-1}$ where a^{-1}, b^{-1} represent the inverses for a, b respectively. What is the inverse of $ab^{-1}c$?

2.) In this exercise we will show that there are two possible different types of group structures on a set of 4 elements. We write the set as $\{e, a, b, c\}$ where e is the identity for the operation. So, we know that the group table will start as follows.

$*$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Now, we need to decide the value of $a^2 = a * a$. This cannot be a. It can be e and now there are 2 ways to complete the table.
a.) Find these two tables. You dont need to check the associative law.

b.) Show by matching elements or otherwise, that these two tables produce the same group structure.

c.) Assume now that $a^2 \neq e, a$. Find the table. Note that there is not much difference in choosing b or c as by swapping the roles of these two letters, you would get the same group structure. (Whats is a name?!)

3.) If $*$ is a binary operation on a set S then, we say $s \in S$ is an *idempotent* if $s * s = s$. Show that there is only one idempotent element in a group.

4.) Show that every group G with identity e and such that $g^2 = e$ for all $g \in G$ is Abelian. (Hint: consider $(ab)^2$.)

5.) Let S be the set of all real numbers except -1. Define a binary operation on S by

$$a * b = a + b + ab$$

a.) Check that $*$ is a binary operation. This means you have to verify that S is *closed* under this operation.
b.) Show that $(S, *)$ is a group. Is it abelian?
c.) Find the solution of the equation $2 * x * 3 = 7$.

6.) Which of the following subsets of the complex numbers are subgroups under addition of the group of complex numbers $(\mathbb{C}, +)$.
a.) $\mathbb{R}$
b.) $\mathbb{Q}^+ = \{r \in \mathbb{Q} \mid r > 0\}$

c.) $7\mathbb{Z} = \{7n \mid n \in \mathbb{Z}\}$
d.) The set of purely imaginary numbers.

7.) Let G be a finite group of even order. Then show that there is an element $g \in G$ such that $g^2 = e$.

8.)Let H and K be subsets of a group G. The intersection of H and K written $H \cap K$ is the set of all elements of G which are common to both H and K:

$$H \cap K = \{g \in G \mid g \in H,\ g \in K\}$$

a.) If $H \leq G$ and $K \leq G$, then which element of G can you always find in $H \cap K$?
b.) If $H \leq G$ and $K \leq G$, then show that $H \cap K$ is a subgroup of G.

9.) Let G be an abelian group, fix an integer $n > 0$. Let $H = \{g^n \mid g \in G\}$. Show that H is a subgroup of G.

10.) Let H be a non-empty finite subset of a group G. Show that if H is closed under the binary operation on G, then $H \leq G$.

11.) Let H be a subgroup of G. We define a relation $\approx$ on G as follows.

$$a \approx b \Leftrightarrow ab^{-1} \in H$$

Verify that $\approx$ is an equivalence relation.

Chapter 2

Cyclic groups and subgroups

Let G be a group and let a be an element of G. By definition, $a^2 = a.a$ belongs to G; similarly, $a^3 = a.a^2 \in G$ and indeed for any positive integer n, a^n which is the n-fold product of a with itself, belongs to G. Now, symbolically, we always think of $a^0 = e$. As G is a group, a^{-1}, the inverse of a is an element of G. Moreover, for any $n \in \mathbb{N}$, the n-fold product of a^{-1} with itself, written a^{-n}, is also in G. One can verify that the inverse of a^n is a^{-n}.

This discussion tells us that the set $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subset of G. However more is true.

Theorem 7. *Let G be a group, let $a \in G$ and let $H = \{a^n \mid n \in \mathbb{Z}\}$. Then H is a subgroup of G. Moreover, every subgroup that contains a contains H and so H is the smallest subgroup of G containing a.*

Proof. Let H be as in the statement of the theorem. Apparently H is nonempty (it contains a, by definition). By Theorem 6, it suffices to check closure and existence of inverses. Let $g, h \in H$. Then there exist integers k, l such that $g = a^k$ and $h = a^l$. So $gh = a^k a^l = a^{k+l}$ and clearly, gh belongs to H. For any element $a^n \in H$, its inverse is a^{-n}. Assuming without loss of generality that $n > 0$, we have

$$a^n a^{-n} = (\underbrace{a.a\ldots a}_{n})(\underbrace{a^{-1}.a^{-1}\ldots a^{-1}}_{n}) = (a(a\ldots(a(aa^{-1}).a^{-1})\ldots)a^{-1}) = e$$

By Theorem 3, a^{-n} is an inverse for a^n. This proves that H is a subgroup of G. As subgroups are closed under the group operation, any subgroup that contains a will also contain H. □

The above theorem motivates the definition of a cyclic subgroup and cyclic group.

Definition 6. *Let G be a group and $a \in G$. Then $\{a^n \mid n \in \mathbb{Z}\}$ is called the cyclic subgroup of G generated by a and denoted $\langle a \rangle$. A group G is said to be cyclic if there exists $a \in G$ such that $\langle a \rangle = G$. In this case we say G is generated by a or equivalently a is the generator for G.*

Examples

1.) The integers under addition $(\mathbb{Z}, +)$ is generated by 1.
2.) The integers modulo n under addition $(\mathbb{Z}_n, +)$ is generated by $\bar{1}$. See (Appendix, Example 29) for details. The addition is defined by $\overline{a} + \overline{b} = \overline{(a+b)}$
3.) If $G_1 = \{e, a, b, c\}$ is the Klein's 4-group from the previous chapter then $\langle a \rangle = \{e, a\}$ is a cyclic subgroup of G_1. However G_1 is not a cyclic group.

We now turn to some simple results about cyclic groups.

Theorem 8. *A cyclic group is Abelian.*

Proof. Let G be a cyclic group. By definition, there exists $a \in G$ such that $G = \langle a \rangle$. We need to show that $gh = hg$ for all $g, h \in G$. Now g, h are of the form a^n and a^m respectively. Moreover, $gh = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = hg$. □

Theorem 9. *Every subgroup of a cyclic group is also cyclic.*

Proof. The proof uses the Division algorithm, which says, given integers m, n with $m > 0$, there exists integers q and r such that $m = qn + r$ and $r \in \{0, 1, \ldots, n-1\}$.

Now let $G = \langle a \rangle$ be our cyclic group. Let $H \leq G$. If H is the trivial subgroup there is nothing to prove. Consider the set $S = \{s \in \mathbb{Z} \mid s > 0; a^s \in H\}$. If H is non-trivial, then $S \neq \emptyset$. But being a non-empty collection of positive integers, S must have a minimal element, call it k. We claim $H = \langle a^k \rangle$.

Let $h \in H$; as $h \in G$, replacing h by its inverse if necessary, we can write $h = a^m$ with $m > 0$. We now invoke the Division algorithm: there exist q, r such that $m = qk + r$, where $0 \leq r \leq k - 1$. Therefore, $h = a^m = a^{qk} a^r$. As a^k belongs to H, so does a^{qk}. By closure property of a subgroup, we know that $a^{qk} h^{-1} = a^r$ belongs to H. As r is strictly smaller than k, it contradicts the choice of k as the minimal element in S, unless $r = 0$. This proves that $h = a^{qk} = (a^k)^q$ and $H = \langle a^k \rangle$. □

Remark. The above theorem tells us that all subgroups of $(\mathbb{Z}, +)$ are of the form $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

The same strategy as in the proof of Theorem 9 gives us the Lemma below.

Lemma 10. *Let $a \neq e$ be an element of a group G. If n is the order of a and $a^k = e$ for some integer k then n divdes k.*

Proof. Let n be the order of the element $a \in G$. Recall that n is the smallest natural number such that $a^n = e$. Now suppose that for some integer k, we have $a^k = e$. We can assume by taking inverses if needed, that $k > 0$. We invoke the Division Algorithm: there exists therefore integers q, r such that $k = qn + r$ and r is strictly smaller than n. So,

$$e = a^k = a^{nq+r} = a^{nq}a^r.$$

As a has order n, $a^{nq} = (a^n)^q = e$. This implies $a^r = e$, which contradicts our choice of n as the smallest natural number for which a power of a is the identity, unless $r = 0$. In this case, $k = nq$ and we conclude n must divide k. □

Suppose now that we have a cyclic group G generated by an element a. If a has infinite order or equivalently, $a^n \neq e$ for all $n \in \mathbb{Z}$, then G is infinite, $G = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$ and for $n \neq m$, we know that $a^n \neq a^m$. In this case, we call G an infinite cyclic group and denote it by C_∞. By Theorem 9, all subgroups of C_∞ are cyclic and generated by some power a^k, and therefore also infinite cyclic.

We now discuss the case when G is finite and cyclic, with generator a. In this case $G = \langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$ but the list $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$ must have repetition. So for some integers h, k, we have $a^h = a^k$ and so $a^{h-k} = e$. Hence, a has finite order. Set $o(a) = n$.

We claim that $G = \{e, a, a^2, \ldots, a^{n-1}\}$. Observe that for $0 \leq h < k \leq n-1$, a^h and a^k are distinct as otherwise $a^{h-k} = e$ with $|h - k| < n$. Hence $\{e, a, a^2, \ldots, a^{n-1}\}$ is a *subgroup* of G containing n elements. On the other hand, if g is any element of G, then $g = a^p$ for some p. If $p > 0$ then applying the Division Algorithm, we can make $a^p = a^r$ where $0 \leq r < n-1$. If $p < 0$ and $P = -p$ then we can write $a^P = a^r$ for some $r < n$ and $a^p = a^{-P} = (a^P)^{-1} = (a^r)^{-1} = a^{n-r}$. This proves that $G = \{e, a, a^2, \ldots, a^{n-1}\}$ and hence, the cyclic group generated by an element of order n has precisely n elements. We denote a cyclic group of order n by C_n.

The preceeding paragraphs prove the following:

Theorem 11. *Let G be a finite cyclic group generated by a. Then,*
1.) The generator a has finite order.
2.) The elements a^h, with $h = 0, 1, \ldots, n-1$ are all distinct and $G = \{e, a, a^2, \ldots, a^{n-1}\}$.

Combining Theorems 9 and 11 we can find all the subgroups of a cyclic group of order n. Again, let G be a finite cyclic group of order n generated by a. Let H be a subgroup of G. By Theorem 9 H is cyclic. Suppose h is a generater for H. As $b \in G$, there is some integer s between 0 and $n-1$ such that $b = a^s$. The question now is whether we can say how large the subgroup H is. But we know that the order of H is equal to the order of b. We will now find the order of b. Set $k = o(b)$. Then $(a^s)^k = a^{ks} = e$. By Lemma 10, the order of a which is n must divide ks. To find the order of a^s, we thus have to find the smallest k such that $n|(sk)$.

Let d be the greatest common divisor of n and s. We use the Euclidean Algorithm to find integers p, q such that $np + qs = d$. Further $\frac{n}{d}p + q\frac{s}{d} = 1$ where n/d and s/d are both integers. This implies that n/d and s/d are co-prime. Moreover,

$$(a^s)^{\frac{n}{d}} = (a^n)^{\frac{s}{d}} = e.$$

We claim that $k = n/d$. We are searching for the smallest k such that $\frac{sk}{n}$ is an integer. But $\frac{sk}{n} = \frac{k(s/d)}{(n/d)}$. As n/d and s/d are co-prime, $\frac{k(s/d)}{(n/d)}$ will an integer if and only if n/d divides k. So the smallest value of k is n/d, as claimed. Hence a^s has order n/d and H is a subgroup of order n/d.

We have proved therefore

Theorem 12. *If $a \in G$ has order n then $o(a^s) = \frac{n}{gcd(n,s)}$.*

Exercise 4. *If G is a cyclic group generated by a and $o(a) = n$, then show that every element of G of the form a^s, where $1 \leq s \leq n-1$ and $gcd(n,s) = 1$ generates G.*

Exercise 5. *List all the subgroups of the cyclic group $\mathbb{Z}_n$.*

Chapter 3

Symmetric Groups

In this chapter we talk about groups that arise from permutations of sets. A permutation of a non-empty set A is a rearrangement of the elements of A; more formally, a permutation is a function $A \to A$ that is both onto and one-one.

We write S_A for the set of all permutations of the set A. If the cardinality of A is $n < \infty$ then, the elements of A are matched up with $\{1, 2, \ldots, n\}$ so that $S_A = S_{\{1,2,\ldots,n\}}$. To avoid cumbersome notation, we shorten $S_{\{1,2,\ldots,n\}}$ to S_n. Our job now is to make S_n into a group. We first need a binary operation. Functions from a set to itself may be composed with each other: given functions $f, g : A \to A$

$$f \circ g(a) = f(g(a)) \ \ \forall a \in A.$$

Theorem 13. *Endowed with the binary operation of composition, S_n is a group, called the symmetric group on n letters.*

3.1 Review of permutations

Consider the permutation $\sigma : 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$ from S_3. This is written as

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

or in cycle notation as $\sigma = (123)$. Similarly the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ can be written as $(124)(35)$.

We multiply permutations via composition. Treating them as functions we follow the convention that $(\sigma\tau)(k) = \sigma(\tau(k))$ and so we apply τ first and follow up with σ. In a product of several permutations we work our way from right to left!

For example if $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 3 \end{pmatrix} = (13)$$

Caveat. Composition of permutations is **non-commutative**. Indeed, $(123)(12) \neq (12)(123)$.

2-cycles are called **transpositions**. We will later come across a theorem saying that every permutation can be written as a product of transpositions. We now prove Theorem 13. The fact that composition of functions defines a binary operation on S_n follows from the fact that the composition of two bijections is again a bijection. For associativity, note that composition of functions, irrespective of whether we have bijections or not, is associative. Indeed, if f and g are two functions from a set to itself, then

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

On the other hand,

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

It remains to prove the existence of an identity and inverses. Here we freely use Exercise 3. The identity e in S_n is the identity permutation which sends each $k \in \{1, 2, \ldots, n\}$ to itself.

Finally, given a permutation σ, to find σ^{-1}, we simply *reverse the arrows*: if σ sends k to j, then its inverse sends j to k. The existence of the inverse completes the proof that all the group axioms hold.

There are $n!$ permutations of a set of n elements. Therefore, the group S_n defined in Theorem 13 has $n!$ elements. It is called the symmetric group on n elements. The symmetric group S_3 is the smallest non-Abelian group.

Exercise 6. *How many transpositions are there in S_n? How many k-cycles are there in S_n?*

Chapter 4

Telling groups apart

We will now embark on the long-overdue discussion of group homomorphisms which will eventually lead us to techniques for telling groups apart and transferring properties we know about one group to another.

4.1 Our world of groups so far

First let us list some of the groups we have encountered so far.

1. the trivial group, $\{e\}$
2. finite cyclic groups $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$
3. the infinite cyclic group $C_\infty = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots, \}$
4. Klein 4-group $V_4 = \{e, a, b, ab\}$, which is not cyclic, as each of a, b, ab has order 2.
5. the additive group of integers $(\mathbb{Z}, +)$ which is infinite cyclic and we suspect, it is essentially the same as C_∞
6. the additive group of integers modulo n, $(\mathbb{Z}_n, \oplus)$, which we suspect is essentially the same as C_n
7. permutation groups or subgroups of the symmetric groups S_n

Of course there are others like the additive group of reals, groups of $n \times n$ invertible matrices, the list is endless.

4.2 Direct products: an introduction

A class of groups that you would have seen in Linear Algebra involves the direct product. Consider for instance the Cartesian product of two copies of the integers $(\mathbb{Z}, +)$. Written $\mathbb{Z}^2$, as a set, this is the collection of all ordered pairs (n, m) such that n, m are both integers. But using addition in the integers, $\mathbb{Z}^2$ is easily made into a group:

$$(n, m) + (n', m') = (n + n', m + m') \ \forall \ (n, m), (n', m') \in \mathbb{Z}^2$$

Componentwise addition produces a binary operation which is associative.

Associativity is a direct consequence of associativity in $(\mathbb{Z}, +)$. The identity element is $(0, 0)$ and the inverse for (n, m) is $(-n, -m)$.

We generalise this construction to form direct products of groups; the groups involved do not have to be the same and one can combine as many copies as one likes (into n-fold direct products).

Definition 7 (Theorem/ Definition)**.** *Let G, H be groups. Let $G \times H = \{(g, h) \mid g \in G, h \in H\}$. Define the product of any $(g, h), (g', h') \in G \times H$ as*

$$(g, h)(g', h') = (gg', hh') \qquad (*)$$

This binary operation makes $G \times H$ into a group, called the direct product of G and H.

Let's check that the protagonist of Definition 7 is indeed a group. There is no doubt that the defined product is a binary operation.

Associativity follows from the associative law holding in both G and H. Let $(g_i, h_i), i = 1, 2, 3$ be elements of $G \times H$. Then

$$((g_1, h_1)(g_2, h_2))(g_3, h_3) = ((g_1 g_2) g_3, (h_1 h_2) h_3)$$

$$(g_1, h_1)((g_2, h_2)(g_3, h_3)) = (g_1(g_2 g_3), h_1(h_2 h_3))$$

But $(g_1 g_2) g_3 = g_1(g_2 g_3)$ in the group G and $(h_1 h_2) h_3 = h_1(h_2 h_3)$ in the group H and so the product is associative.

If e, e' are respectively the identity elements for G, H, then the identity for $G \times H$ is (e, e'). Finally for any $(g, h) \in G \times H$, the inverse is precisely (g^{-1}, h^{-1}).

Exercise 7. *If G and H are both Abelian, then $G \times H$ is Abelian. Is the converse true?*

The construction of the direct product enlarges our encyclopaedia of groups. We can take any pair of groups and form their direct product to form a new group. We now embark on developing the technology to tell groups apart. This calls for the notion of homomorphisms.

4.3 Homomorphisms

If we are to tell groups apart, we must have a way to map one group to another. However, a function with no additional properties is not good enough. We need the functions to somehow relate between the binary operations given on the groups and respect the group structure.

Suppose G, H are two groups with identity elements e, e' respectively. Let ϕ be a function from G to H. If g_1, g_2 are a pair of elements from G, we can form the product $g_1 g_2$ and then apply ϕ to get the element $\phi(g_1 g_2)$ of H. On the other hand, we can first apply ϕ to get the elements $\phi(g_i), i = 1, 2$; the product of these new elements in H is $\phi(g_1)\phi(g_2)$. For the function ϕ to have good structure preserving properties, we demand that the two products are the same. More precisely,

Definition 8. *Let G, H be groups. A function $\phi : G \to H$ is called a group homomorphism if $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$* ***for all*** *$g_1, g_2 \in G$.*

4.3.1 Examples of homomorphisms

1.) For any pair of groups, G, H, one can always define the **trivial homomorphism**. This is the rather uninteresting function that maps every element of the domain to the identity element in the range.

2.) If H is a subgroup of G, then one has the **canonical injection** of H into G that maps an element of h to its counterpart in G.

3.) **Evaluation homomorphism.** Let $\mathbb{F}$ be a field and let $\mathbb{F}[x]$ be the set of all polynomials over $\mathbb{F}$. Addition of polynomials makes $\mathbb{F}[x]$ into a group in which the zero polynomial is the identity and $-f(x)$ is the inverse of the polynomial $f(x)$. Fix $a \in \mathbb{F}$ and define $\eta_a : \mathbb{F}[x] \to \mathbb{F}$ as $f(x) \mapsto f(a)$. For instance $\eta_a(2x + 1) = 2a + 1$. Then η is a homomorphism. Evidently, evaluating a given polynomial $f(x)$ at a produces an element $f(a)$ of the field. Moreover, if f and f' are both elements of $\mathbb{F}[x]$, then

$$\eta_a(f + f') = f(a) + f'(a) = \eta_a(f) + \eta_a(f').$$

This shows that the defining property for a homomorphism holds. More generally, one can work with $H = Func(\mathbb{R}, \mathbb{R})$, the set of all functions from $\mathbb{R}$ to itself. As in the case of the polynomials, addition makes H into a group and for every real number r, there is a function $F_r : H \to \mathbb{R}$ which takes a function f to $f(r)$. For the same reasons as before F_r is a homomorphism.

4.) Let $GL(n, \mathbb{R})$ be the group of $n \times n$ invertible matrices under matrix multiplication. The determinant of matrices defines a homomorphism from $GL(n\mathbb{R})$ to the multiplicative group of $\mathbb{R}\backslash\{0\}$. For any invertible matrix A, $det(A) \neq 0$ and moreover, $det(AB) = det(A)det(B)$ for all $A, B \in GL(n, \mathbb{R})$.

5.) **Congruence modulo *n*.** Define $\rho_n : (\mathbb{Z}, +) \to (\mathbb{Z}_n, \oplus)$ by $\rho_n(k) = r$ where r is the remainder obtained on dividing k by n. We now need to verify that $\rho_n(k + k') = \rho_n(k) \oplus \rho_n(k')$ for all integers k, k'. Applying the division algorithm to k, k' we get

$$k = qn + r, \quad k' = q'n + r' \quad 0 \leq r, r' < n$$

So, $\rho_n(k) \oplus \rho_n(k') = r \oplus r'$, where $r \oplus r'$ is the remainder from dividing $r + r'$ by n. Applying the division algorithm again, we get $r + r' = q''n + r''$ with $0 \leq r'' < n$ and in $\mathbb{Z}_n$, $r \oplus r' = r''$. On the other hand, putting all of the above equations, we see

$$k + k' = (q + q' + q'')n + r''$$

Apparently $\rho_n(k + k') = r'' = \rho_n(k) + \rho_n(k')$ and therefore, ρ_n is a homomorphism.

Definition 9. *Let $\phi : G \to H$ be a group homomorphism.*
1.) The homomorphism ϕ is said to be surjective or onto, if for every $h \in H$, there exists $g \in G$ such that $\phi(g) = h$. If $\phi(G) = \{\phi(g) \mid g \in G\}$, then ϕ is surjective if and only if $\phi(G) = H$.
2.) The homomrphism ϕ is called injective if $\phi(g) = \phi(g')$ implies $g = g'$ in G.

Example 2 above is injective and all the others, (1) and (3)-(5) are surjective. For instance, ρ_n is surjective because for any integer $r \in \{0, 1, \ldots, n-1\}$, $\rho_n(r) = r$.

Exercise 8. *Show that η_a, F_r and det are surjective.*

4.3.2 Properties of Homomorphisms

The following Theorem elucidates how homomorphisms preserve the structure of the groups involved: it says, under a homomorphism, the identity maps to the identity, inverses get taken to inverses, subgroups to subgroups and finally, subgroups of the range come from subgroups of the domain. More precisely:

Theorem 14. *Let $\phi : G \to H$ be a homomorphism of groups. We write e for the identity element of G and e' for the identity element of H. The following hold:*

1. $\phi(e) = e'$

2. *For all $g \in G$, $\phi(g^{-1}) = \phi(g)^{-1}$. Moreover, $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{Z}$.*

3. *If $K \leq G$, then the image of K, $\phi(K) = \{\phi(x) \mid x \in K\}$ is a subgroup of H.*

4. *If $K' \leq H$, then $\phi^{-1}(K') = \{g \in G \mid \phi(g) \in K'\}$ is also a subgroup of G.*

Proof. Apply ϕ to both sides of $e.e = e$; then, $\phi(ee) = \phi(e)$ which implies $\phi(e)\phi(e) = \phi(e)$. Using the left or right cancellation law in H, we deduce that $\phi(e) = e'$.

For 2.) the argument similar. As $gg^{-1} = e$, the defining property of a homomorphism implies, $\phi(g)\phi(g^{-1}) = \phi(e) = e'$. But then, $\phi(g)^{-1} = \phi(g^{-1})$.

To prove 3.) we first observe that as the identity of G belongs to K, the identity $e' = \phi(e)$ (by (1)) also belongs to $\phi(K)$. Now suppose x, y are two arbitrary elements of $\phi(K)$, we need to show that xy and x^{-1} belong to $\phi(K)$. Now, there are elements g, g' such that $x = \phi(g)$ and $y = \phi(g')$. We can compute as follows,

$$xy = \phi(g)\phi(g') = \phi(gg'); \quad x^{-1} = \phi(g)^{-1} = \phi(g^{-1}).$$

Since $K \leq G$, K is closed under products and taking inverses. Hence, $gg', g^{-1} \in K$ and so $xy, x^{-1} \in \phi(K)$.

The proof of 4.) is similar. Let $L = \phi^{-1}(K')$. Once again, we can check that $e \in L$ as $e' \in K'$. Let $a, b \in L$. Then $\phi(a), \phi(b) \in K' \Rightarrow \phi(a)\phi(b) = \phi(ab) \in K'$ and $\phi(a)^{-1} = \phi(a^{-1}) \in K'$. Therefore by definition of L, we conclude that ab, a^{-1} belong to L and therefore it is a subgroup of G. □

4.3.3 The kernel of a homomorphism

Every group has the trivial subgroup, whose only element is the identity element. From property (4) above we see that for any homomorphism, $\phi : G \to H$, $\phi^{-1}(\{e'\})$ is a subgroup of G. It is called the **kernel** of ϕ and denoted as $\ker \phi$.

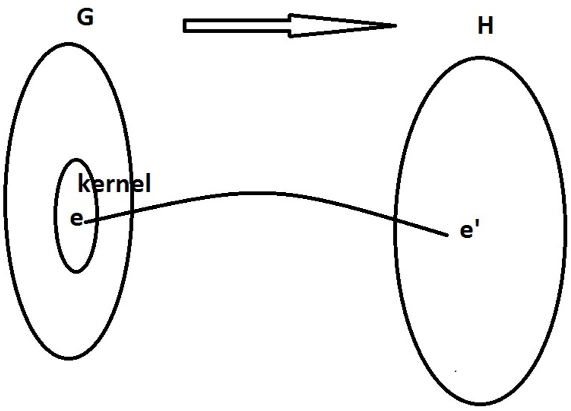

Figure 4.1: Kernel of a homomorphism

4.3.4 Examples of homomorphisms with non-trivial kernels.

1.) Let us revisit the homomorphism ρ_n from paragraph 4.3.1 above. An integer k lies in the kernel of ρ_n if and only if $\rho_n(k) = 0$ i.e. reducing k modulo n leaves a remainder of 0. This is equivalent to saying k is divisible by n. Therefore $k \in \ker(\rho_n) \Leftrightarrow k = nr$ for some integer r and so $\ker(\rho_n) = n\mathbb{Z}$, where $n\mathbb{Z} = \{nr \mid r \in \mathbb{Z}\}$.

2.) We now look at a homomorphism of a different kind. Consider the multiplicative group of the complex numbers $\mathbb{C}^\times$. As a set, this consists of all non-zero complex numbers. We denote the multiplicative group of all positive real numbers by $\mathbb{R}_{>0}$. Define now, $f(z) = |z|$. If z, z' are complex numbers, then $|zz'| = |z||z'|$ and so $f(zz') = f(z)f(z')$ for all $z, z' \in \mathbb{C}^x$. Hence f is a group homomorphism. Further, by definition, $\ker(f) = \{z \in \mathbb{C}^\times \mid f(z) = 1\}$. Now, $f(z) = 1$ if and only if $|z| = 1$ and therefore the kernel of this map is the unit circle.

The kernel helps us to detect one-one homomorphisms. As the identity e of G is always sent to the identity e' of H, if the homomorphism is one-one, no element distinct from e may be sent to e'. Formally,

Theorem 15. *Let $\phi : G \to H$ be a homomorphism. Then ϕ is one-one if and only if $\ker\phi = \{e\}$.*

Proof. Let ϕ be one-one and let $x \in \ker\phi$. Then $\phi(x) = e'$; but $\phi(e) = e'$ so $\phi(e) = \phi(x)$. As ϕ is one-one, $x = e$ and we conclude that $\ker\phi = \{e\}$.

Conversely let $\ker\phi = \{e\}$ and suppose $x, y \in G$ are such that $\phi(x) = \phi(y)$. Then

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

Clearly $xy^{-1} \in \ker\phi$. But then $xy^{-1} = e$ or equivalently $x = y$, as required. □

Exercise 9. *If the sets A and B both have n elements then show that the symmetric groups S_A and S_B are isomorphic.*

Hint: As the sets A and B have the same elements, you can choose a bijection ϕ between them. Use ϕ to define the map between their symmetric groups.

Chapter 5

Cosets and Lagrange's Theorem

We saw when we were studying cyclic groups that the order of subgroup divides the order of the ambient group. This is a more general phenomenon and is referred to in Group Theory as Lagrange's Theorem. The theorem, as we know it now was proved much later by Camille Jordan. To understand Lagrange's Theorem, one has to look at cosets of a subgroup.

5.1 Cosets

Let G be a group and $H \leq G$. We define an equivalence relation on the elements of G as follows:

$$a \sim b \ \Leftrightarrow \ ab^{-1} \in H.$$

Claim. $\sim$ is an equivalence relation.

1.) (reflexive) For any $a \in G$, $aa^{-1} = e$ and as H is a subgroup, $e \in H$. Therefore $a \sim a$ for all $a \in G$.

2.) (symmetric) Let $a, b \in G$ such that $a \sim b$. Then, by definition, $ab^{-1} \in H$. As H is a subgroup $(ab^{-1})^{-1} = ba^{-1}$ also belongs to H. Hence, $a \sim b \Leftrightarrow b \sim a$ for all $a, b \in G$.

3.)(transitive) Suppose $a, b, c \in G$ satisfy $a \sim b$ and $b \sim c$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$. As the subgroup H is closed under the binary operation, $(ab^{-1})(bc^{-1})$ belongs to H. But $(ab^{-1})(bc^{-1}) = ac^{-1}$ and so $a \sim c$.

As $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation on the elements of G. The upshot is that G can be partitioned into a **disjoint**

union of equivalence classes of $\sim$:

$$G = \cup_{g \in S} [g] \,,$$

where S is the set of equivalence classes. Choosing a representative from each class, one can identify S with the collection of all such representatives.

What do the equivalence classes of $\sim$ look like? Let $a, b \in G$; if $a \sim b$ then $ab^{-1} \in H$ and so, there exists $h \in H$ such that $ab^{-1} = h$ or equivalently, $b = h^{-1}a$. Conversely if $b = ha$ for some $h \in H$, then clearly $ab^{-1} \in H$ and so $a \sim b$. We have shown therefore that the equivalence class of a is given by

$$[a] = \{x \in G \mid a \sim x\} = \{ha \;:\; h \in H\}$$

and we write Ha for the set $\{ha \;:\; h \in H\}$.

Remark. As the Ha's are the equivalence classes of $\sim$, we know that for distinct a, b, either $Ha = Hb$ or else Ha and Hb are disjoint.

Definition 10. *The sets $Ha = \{ha \;:\; h \in H\}$ are called the* ***right cosets of*** *H* ***in*** *G. We write $H\backslash G$ for the set of all right cosets of H in G.*

Now, what can we say about the cardinality of each Ha? Notice that if a is the identity element then $Ha = H$ and moreover, $Ha = H$ if and only if $a \in H$. H is therefore referred to as the identity coset. Now for any a, b we can define a *set* map $Ha \to Hb$ by $ha \mapsto hb$, for $h \in H$. This map is one-one as $hb = h'b$ if and only if $h = h'$. The map is also onto as, given any element $x \in Hb$, $x(b^{-1}a)$ belongs to Ha. Any two Ha's are therefore in one-one correspondence with one another and so the cosets all have the same cardinality, namely, the cardinality of H itself.

We now return to the partition of G into right cosets: $G = \cup_{a \in S} Ha$. If G is finite then each Ha is also finite. Write $[G : H]$ for the number of equivalence classes of $\sim$; that is, $[G : H] = |S|$. Then, we have

$$|G| = \sum_{a \in S} |Ha| \; = \sum_{a \in S} |H| = \left(\sum_{a \in S} 1 \right) |H| = [G : H]|H|.$$

So $|G| = [G : H]|H|$ and we conclude that the order of H divides the order of G, which is precisely the statement of Lagrange's Theorem.

Theorem 16 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then the order of H divides the order of G.*

The quantity $[G : H]$, which is the number of right cosets of H in G is called **the index of H in G**.

Left cosets

Instead of defining $\sim$ as we did, we could have said that two elements $a, b \in G$ are related if and only if $a^{-1}b \in H$.

In this case, the entire discussion would have worked out (check it) and the only difference would have arisen in the nature of the equivalence classes: the equivalence class of an a would have been a **left coset** of H in G and a left coset is given by

$$aH = \{ah : h \in H\}.$$

The set of all left cosets of H in G are denoted by G/H.

Once again if we write G as a disjoint union of the left cosets of H, then we find that the number of left cosets turns out to be precisely $[G : H]$, the index of H in G. In regard to Lagrange's Theorem and the equation $|G| = [G : H]|H|$, it does not really matter whether we work with right or left cosets. *However, left and right cosets are very different in general and it is not true that $aH = Ha$ for all $a \in G$.*

For example, take G be the symmetric group S_3 and set H to be the cyclic group generated by the transposition (12). Then $(123)H = \{e, (13)\}$ while $H(123) = \{e, (23)\}$. So $(123)H \neq H(123)$.

Definition 11. *A subgroup H of G is said to be **normal** if $aH = Ha$ for all $a \in G$.*

Normal subgroups play a central role in Group Theory and we will study them in detail in a subsequent chapter. We will now look at some consequences of Lagrange's Theorem.

Consequences of Lagrange's Theorem

Corollary 17. *The order of any element a of in a finite group G divides the order of the group and consequently, $a^{|G|} = e$.*

Proof. Let G be a finite group and let $e \neq a$ be an element of G. Then the order n of the cyclic subgroup generated by a divides the order of G, by Lagrange's Theorem. But the order of $\langle a \rangle$ is precisely the order of a, by Theorem 11. Therefore the order of a divides the order of G. □

Corollary 18. *Every group of order p, a prime, is cyclic.*

Proof. Suppose a group G has order p, where p is a prime number. Let a be any non-identity element of G. The cyclic subgroup generated by a has size $o(a)$ and $o(a)$ divides $|G|$. As $|G|$ is prime, $o(a) = 1$ or p. As $a \neq e$,

$o(a) \neq 1$ and so $\langle a \rangle$ has order $o(a) = p$, thus making $\langle a \rangle = G$. This shows that G is cyclic. □

Chapter 6

Dihedral groups

The raison d'etre for groups really is their representation as symmetry groups of objects around us. The *objects* may be geometric figures, platonic solids or wallpaper patterns. Very loosely, a symmetry of an object $\mathbb{O}$ is a transformation that leaves $\mathbb{O}$ invariant and composition is the binary operation that makes the collection of all symmetries of $\mathbb{O}$ into a group.

The dihedral groups form an important infinite family of examples of groups. They arise as groups of symmetries of the regular n-gons. The regular n-gon is the convex figure which is formed of n sides, all of equal length and all of whose internal angles are equal. So, when $n = 3$, this is an equilateral triangle, for $n = 4$, it is a square, and so on. Regular polygons, like their three dimensional counterparts the platonic solids, have fascinated human beings through the ages. The ancient star of david sits on a regular hexagon while the regular octagon forms the basis of our familiar stop sign.

Figure 6.1: Regular Octagon

In a regular n-gon, the angle at the centre of the polygon is $2\pi/n$ and so the polygon has a rotational symmetry r of order n (see figure 6.2). This is the transformation that fixes the centre of the polygon and rotates the polygon clockwise by an angle of $2\pi/n$. If we label the vertices (corners) as 1,2,..., n, then we see that r corresponds to a permutation in S_n, namely the n-cycle $(123\ldots n)$. In particular, iterating this rotation n times means rotating the polygon through an angle of 2π and so each vertex returns to its original position. Thus, r has order n.

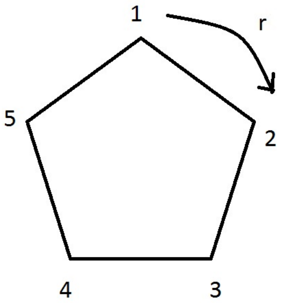

Figure 6.2: Regular pentagon: r rotates the pentagon clockwise through an angle of $2\pi/5$

What are the other symmetries of the polygon? The rotational symmetries leave neither the vertices nor the edges invariant. Let n be odd. Then, the n-gon has a symmetry s that flips it across the axis passing through a fixed vertex and bisecting the side opposite to this chosen vertex. As s is a reflection and its action is to interchange certain pairs of opposite vertices, it has order two and in the permutational representation of the symmetry, s corresponds to a product of disjoint transpositions. For instance, in figure 6.2, if the axis passes through vertex 1 and the mid-point of the side bounded by vertex 3 and vertex 4, then s is given by the permutation $(25)(34)$. One gets a reflectional symmetry for each of the vertices and each of these is conjugate to s, for example $rsr^{-1} = (13)(45)$.

If n is even there are 2 (conjugate) families of reflections that appear as symmetries of the polygon. In one, the axes pass through opposing vertices (and so correspond to diagonals). In the other family, the axes bisect two opposing edges and therefore pass through the mid-points of these edges. None of the symmetries, irrespective of the parity of n, described so far leave an edge invariant. In fact, a symmetry of a polygon that leaves an edge invariant must fix all vertices and hence be the identity transformation.

We conclude then that the regular polygon with n-sides has $2n$ symmetries, n rotational and n reflectional. These symmetries can be written as expressions in r and s and together, they constitute the n-th dihedral group

$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$.

The above expression for the dihedral group is easily explained with the language of group actions which we will do in a consequent chapter. The reflection s can be chosen so that $srs^{-1} = r^{-1}$. This implies that D_n's are all **non-abelian** and the cyclic subgroup generated by r is a normal subgroup of index 2.

For the moment, we will look at the cases when $n = 3, 4$.

6.1 $D_3 \cong S_3$

We saw this in the first chapter. The dihedral group D_3 is isomorphic to the symmetric group on 3 objects. Indeed the rotational symmetry r corresponds to the 3-cycle (123). The reflection s (see figure 1.2) that fixes vertex 3 exchanges vertices 1 and 2 is the permutation (12). Observe that $srs^{-1} = r^{-1}$ (which not only tells you that the group is not abelian) but also gives you a way to write out all the elements of $D_3 = \{e, r, r^2, s, sr, sr^2\}$.

Clearly D_3, given via this permutation representation is a subgroup of S_3. But as both D_3 and S_3 have size 6, we conclude they must be isomorphic.

The subgroup $\langle r \rangle$ is the cyclic subgroup of order 3 generated by (123). It is moreover a normal subgroup of D_3.

6.2 D_4

The dihedral group D_4 is the group of symmetries of the square. If we label the vertices of our square clockwise as 1,2,3,4 then the rotational symmetries are powers of the 4-cycle (1234). As $r^{-1} = (1432)$, the reflection s may be chosen to be (24). This is reflection about the axis that passes through the opposing vertices 1 and 3. So the 8 elements of D_4 are given below

- e, the identity transformation
- $r = (1234)$
- $r^2 = (13)(24)$
- $r^3 = r^{-1} = (1432)$
- $s = (24)$, reflection along the diagonal through vertices 1 and 3.
- $sr = (14)(23)$, reflection through the axis that passes through the opposing edges bounded by vertices 1 and 4 and by 2 and 3.

- $sr^2 = (13)$, another *diagonal* reflection
- $sr^3 = (12)(34)$, another *meridian* symmetry.

Again D_4 is a non-abelian group of order 8, having a normal subgroup (the cyclic subgroup generated by r) of index 2.

A different way of looking at dihedral groups

The dihedral groups can be realised as groups of matrices by viewing them as linear transformations that rotate and reflect in the complex plane where the vertices of a regular n-gon have been taken to be the n-th roots of unity.

6.3 Groups of order 8

We now have sufficient knowledge of group theory to describe all the non-isomorphic groups of order 8. However, we cannot yet prove there are precisely 5 of them and so, for the moment we will take that as a fact. The 5 non-isomorphic groups of order 8 are as follows.

- $\mathbb{Z}_8$
- $\mathbb{Z}_4 \times \mathbb{Z}_2$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- D_4, the dihedral group
- Q, the quaternions.

The first 3 groups in the list are all abelian. For this we need a lemma:

Lemma 19. *If G and H are abelian, then the direct product $G \times H$ is also abelian.*

Proof. Let $(g, h), (g', h') \in G \times H$. Then

$$(g, h).(g', h') = (gg', hh') = (g'g, h'h) = (g', h')(g, h)$$

. □

The last 2 groups are not abelian. We already discussed D_4.

The quaternions are a group arising from Hamilton's (one of the Cayley-Hamilton duo) extension of the complex numbers. The elements of the group include ±1, where 1 serves as the identity for the group. The other elements can be written in terms of i, j, k where the rules of multiplication follow: $ij = k$; $jk = i$; $ki = j$ and $i^2 = j^2 = -1 = ijk$. Therefore

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

Exercise 10. *Draw the Cayley table for the quaternions Q. What are the order of the elements of Q?*

Exercise 11. *Argue that any 2 groups from the following list are non-isomorphic.*

$$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ D_4,\ Q.$$

Some useful facts about direct products

1.) Let $G = H \times K$ be a direct product of 2 groups, not necessarily abelian. Show that for all $h \in H$ and $k \in K$, we have $(h, e_K)(e_H, k) = (h, k) = (e_H, k)(h, e_K)$ and the entire copy of K commutes with every $h\ inH$ and vice versa.

2.) Using 1.) above we know that $(h, k)^n = ((h, e_K)^n (e_H, k)^n$ for all n and therefore, the order of (h, k) is the least common multiple of $o_H(h)$ and $o_K(k)$.

The proof of (2) is left as an exercise.

Chapter 7

Normal subgroups

Recall that a subgroup H of a group G is said to be normal in G, written $H \trianglelefteq G$, if and only if $gH = Hg$ for all $g \in G$. In other words the right cosets of H coincide precisely with the left cosets of H in G.

We denote the set of all right cosets of H by $H\backslash G$ and the set of all left cosets by G/H. So $G/H = \{gH \mid g \in G\}$ where $gH = \{gh \mid h \in H\}$.

Lemma 20. *Let $H \leq G$. Then the following are equivalent.*

1. *$gH = Hg$ for all $g \in G$.*
2. *$ghg^{-1} \in H$ for all $h \in H$ and for all $g \in G$.*
3. *$gHg^{-1} = H$ for all $g \in G$.*

Proof. We will show that (1)⇒(2)⇒(3)⇒(1). Let (1) hold, let $h \in H$ and $g \in G$. Then $gh \in gH$ and as $gH = Hg$ there exists $h' \in H$ such that $gh = h'g$ or equivalently, $ghg^{-1} = h'$. Apparently $ghg^{-1} \in H$ as required and so (1)⇒(2).

Now let (2) hold. Note that (2) is equivalent to the statement that $gHg^{-1} \subseteq H$ for all $g \in G$. So to prove (3), we have to show that $H \subseteq gHg^{-1}$ for all $g \in G$. So let $x \in G$ and let $h \in H$. Then $x^{-1}hx \in H$ by (2). And so $h = x(x^{-1}hx)x^{-1}$ belongs to xHx^{-1}. Therefore (3) holds.

Finally (3) implies (1) is easy as $gH = Hg$ is equivalent to $gHg^{-1} = H$. □

Criterion 2 from Lemma 20 is perhaps the quickest way to establish that a subgroup is normal.

Examples.

1.) The kernel of a homomorphism $f : G \to H$ is normal in G. Let $g \in G$ and $x \in \ker(f)$. Then $f(gxg^{-1}) = f(g)f(x)f(g^{-1})$, where $f(x) = e$ and

$f(g^{-1}) = f(g)^{-1}$. Hence, $f(gxg^{-1}) = e$ and so $gxg^{-1} \in \ker(f)$ for all $x \in \ker(f)$ and for all $g \in G$. By Lemma 20, $\ker(f)$ is a normal subgroup of G.

2.) Let G be a group. Define the **centre of** G to be

$$Z(G) = \{x \in G \mid xg = gx \ \forall \ g \in G\}.$$

Then $Z(G)$ is a normal subgroup of G.

Exercise 12. *Show that $Z(G)$ is a normal subgroup of G. (You have to first check it is a subgroup). Show that the group G is abelian if and only if $G = Z(G)$. Find the centre of Q the group of quaternions. What is $Z(D_4)$?*

Exercise 13. *Show a subgroup H of lndex 2 in a group G must be a normal subgroup of G. Apply this to show that the Alternating Group A_n is normal in the symmetric group S_n.*

Suppose now that N is a normal subgroup of G. Recall that G/N is the collection of left cosets of G. Of course, these coincide with the right cosets and so, in the ensuing the paragraph, we will only work with left cosets, even though the whole discussion works for right cosets as well.

Observe that irrespective of whether N is normal or not, we have a set map $\pi : G \to G/N$ such that $\pi(g) = gN$. Under this map, the identity element of G maps to the identity coset N and so does every element of N. More precisely $\pi(g) = N \Leftrightarrow gN = N \Leftrightarrow g \in N$. To have any hope of making π into a homomorphism we must make G/N into a group. But is this always possible.

If $a, b \in G$, then the set $aNbN$ clearly contains the product ab whose coset must be abN. We would like therefore to define a binary operation on G/N such that $aN * bN = abN$. However this is not always a well-defined notion.

Lemma 21. *The binary operation on G/N given by $aN * bN = abN$ is well-defined if and only if N is normal in G.*

Proof. Any element of aN is of the form an and so if we take an to be a representative of aN instead of a then we have $anbN = abN$ iff $(ab)^{-1}anb$ belongs to N or equivalently, $b^{-1}nb \in N$, which holds if N is normal in G. Conversely suppose that the binary operation is well-defined. Let $g \in G$ and $n \in N$. Then $gng^{-1} = (gn)(g^{-1}e) \in gNg^{-1}N = N$. Then by Lemma 20, N is normal in G. □

So starting with a normal subgroup N, we can put a binary operation on G/N as above. Moreover, the associativity of the original binary operation on G implies that the induced binary operation on G/N is associative. Further, the identity element in G/N is the identity coset and $(gN)^{-1} = g^{-1}N$. Therefore the binary operation from Lemma 21 makes G/N into a group. Not only that, the group structure is such that the map π now becomes a surjective group homomorphism whose kernel is precisely N. We call π the canonical surjection from G to G/N.

Theorem 22 (**First Isomorphism Theorem of Group Theory**). *Let $\phi : G \to H$ be a surjective homomorphism. Then there exists a unique homomorphism making $G/\ker(\phi) \cong H$.*

Proof. Let $N = \ker(\phi)$ and let $\pi : G \to G/N$ be the canonical surjection as defined above. Define the induced map $\tilde{\phi}$ from G/N to H by setting $\tilde{\phi}(gN) = \phi(g)$. We will show that $\tilde{\phi}$ is an isomorphism and $\tilde{\phi} \circ \pi = \phi$.

$\tilde{\phi}$ **is well-defined and injective.** Let $g, g' \in G$. Then $gN = g'N \Leftrightarrow g^{-1}g' \in N \Leftrightarrow \phi(g^{-1}g') = e \Leftrightarrow \phi(g) = \phi(g') \Leftrightarrow \tilde{\phi}(gN) = \tilde{\phi}(g'N)$.

$\tilde{\phi}$ **is a homomorphism.** Let $gN, g'N \in G/N$. Then $\tilde{\phi}(gNg'N) = \tilde{\phi}(gg'N) = \phi(gg') = \phi(g)\phi(g') = \tilde{\phi}(gN)\tilde{\phi}(g'N)$.

$\tilde{\phi}$ **is surjective.** Let $h \in H$. As ϕ is surjective there exists a $g \in G$ such that $\phi(g) = h$. Now $\tilde{\phi}(gN) = \phi(g) = h$ thus proving that $\tilde{\phi}$ is also surjective. Therefore, $\tilde{\phi}$ is an isomorphism of groups. □

Remark. There is more to say about the scenario described in the First Isomorphism Theorem. In fact, given a surjective map from G to H, one gets a one-one correspondence between the normal subgroups of the two groups: if N is a normal subgroup of G then $\phi(N)$ is a normal subgroup of H. Conversely, if K is a normal subgroup of H, then $\phi^{-1}(K)$ is a normal subgroup of G containing the kernel of ϕ.

A simple illustraton of the First Isomorphism Theorem is $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ for any $n \in \mathbb{N}$.

One of the consequences is the Chinese Remainder Theorem:

Theorem 23 (**Chinese Remainder Theorem**). *Let m, n be positive integers such that their least common multiple is l. Then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_l$. In particular, if m, n are co-prime then $l = mn$ and so $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.*

Proof. Define $f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $f(k) = (k \mod m, k \mod n)$. One can check that f is a well-defined homomorphism and moreover that it is surjective.

The kernel of f consists of integers k that are divisible by both m and n. More precisely, $\ker f = m\mathbb{Z} \cap n\mathbb{Z}$. The subgroup $m\mathbb{Z} \cap n\mathbb{Z}$ is generated by the least common multiple of m, n, by Theorem 9. Using the First Isomorphism Theorem we deduce that $\mathbb{Z}/l\mathbb{Z} \cong \mathbb{Z}_l$ and hence $\mathbb{Z}_l \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Recall that for integers m, n, $\operatorname{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$. If m, n are co-prime then $l = mn$ and the final statement follows. □

Chapter 8

Group Actions

Definition 12. *Let X be a set and G be a group. An action of G on X is a map $* : G \times X \to X$ such that*

1.) $ex = x$ for all $x \in X$

2.) $(g_1 g_2)x = g_1(g_2 x)$ for all $g_1, g_2 \in G$ and for all $x \in X$.

In this case, X is called a G-set.

Examples

1.) For any set X, the symmetric group S_X on X acts on X, where the action of any $\sigma \in S_X$ is simply the effect of that permutation on each element of X. If n is a positive integer then using the parlance set up above, $\{1, 2, \ldots, n\}$ is an S_n-set.

2.) Every G is a G-set in many different ways but first and foremost, it is a G-set (recall Cayley's Theorem) as it acts on itself via left multiplication. A group also acts on itself by conjugation: that is the map $* : G \times G \to G$ in Definition 12 is given by $gx = gxg^{-1}$ for all $g \in G$ and for all $x \in G$ (here $X = G$).

3.) If H is a subgroup of G, then the set of all left cosets G/H of H in G is a G-set. Indeed, G acts on G/H again by *left multiplication* and $g(xH) = (gx)H$ for all $g \in G$ and $xH \in G/H$.

4.) The dihedral group D_n acts on the regular n-gon by permuting its vertices.

Orbit Stabiliser Theorem

8.0.1 Orbits

Let X be a G-set. We define a relation on X as follows.

$$x \sim y \;\Leftrightarrow\; \exists g \in G : gx = y.$$

Then $\sim$ defines an equivalence relation on X, as explained below:

1.) $\sim$ is reflexive, as $ex = x$ for all $x \in X$ and so $x \sim x \forall x \in X$.
2.) $\sim$ is symmetric. If $x \sim y$ then $gx = y$ for some $g \in G$ and so $g^{-1}y = x$, giving $y \sim x$.
3.) $\sim$ is transtive. If $x \sim y$ and $y \sim z$ then for some $g, g' \in G$, $gx = y$ and $g'y = z$. This implies that $(gg')x = z$ and so $x \sim z$.

The equivalence class $[x]$ of an $x \in X$ with respect to X is called an orbit of the action. Notice that $[x]$ consists of all the elements of X which arise as gx for some $g \in G$. Hence, we also write Gx for $[x]$.

As $\sim$ is an equivalence relation, X is a *disjoint* union of its equivalence classes: $X = \coprod Gx$ and in the case where G and X are both finite, this decomposition of X can be used for counting arguments.

For each $x \in X$, the **stabiliser** of x under the G-action, denoted as G_x or as $Stab_G(x)$, is defined as follows.

$$G_x = \{g \in G \mid gx = x\ \}$$

So, G_x is made up of all the elements of G which do not move the chosen point x at all.

Theorem 24 (Orbit Stabiliser Theorem)**.** *Let X be a G-set and let $x \in X$. Then the stabiliser G_x is a subgroup of G such that $[G : G_x] = |Gx|$. In other words, the index of the stabiliser of x under the G-action is equal to the size of the orbit of x.*

Proof. We will use the subgroup criterion as in earlier chapters. Clearly $e \in G_x$ as $ex = x$ and so G_x is non-empty. If $g, g' \in G_x$, then $gx = x$ and $g'x = x$, so $(gg')x = g(g'x) = gx = x$. Hence gg' belongs to G_x. For any $g \in G_x$, we have $gx = x$ and so $x = g^{-1}x$ which implies that g^{-1} also belongs to G_x. This proves that G_x is a subgroup of G.

We now define a map $s : Gx \to G/G_x$ by $gx \mapsto gG_x$. The map s is a well-defined bijection of *sets* which gives us the quantitative result that $|Gx| = [G : G_x]$. □

8.1 Applications

If X is a G-set then we will use the decomposition of X into disjoint orbits for quantitative arguments. Write S for the set of distinct orbits of the action of G on X. Then we have

$$(1) \qquad X = \coprod_{x \in S} Gx.$$

$$(2) \;\; |X| < \infty \Rightarrow \;\; |X| = \sum_{x \in S} |Gx|.$$

The Class Equation of a Group

Consider the action of a group on itself by conjugation. In this case, applying (1), we get that G is a union of its conjugacy classes: $Gx = \{gxg^{-1} \; : \; g \in G\}$. Further the stabiliser of an $x \in G$ under the conjugation action is precisely $G_x = \{g \in G \; : \; gxg^{-1} = x\}$. This is a subgroup of G by the Orbit Stabiliser Theorem, called the centraliser of x in G, and denoted $C_G(x)$.

Under the conjugation action, an elements $g \in G$ satisfies $|Gx| = 1$ if and only if every element of G fixes x or equivalently $G_x = G$. Evidently $Gx = \{x\}$. Now, under the conjugation action $G_x = G$ if and only if x is an element of the centre $Z(G)$.

So applying (2) in the case when G is a finite group acting on itself by conjugation, we get the *Class Equation*, which says,

$$|G| \; = \; |Z(G)| \; + \sum_{x \in S, \; |Gx|>1} |Gx|$$

One curious application of the Class Equation is to p-groups, the groups whose order if the power of a prime number.

Theorem 25. *Let G be a p-group with $|G| = p^n, n > 0$. Then,*

1.) $|Z(G)| > 1$

2.) If $|G| = p^2$ then G is abelian.

Proof. The proof uses the Class equation of G, the left-hand side of which is p^n and as $n \geq 1$ is clearly divisible by p. We claim that $\sum_{x \in S, \; |Gx|>1} |Gx|$ is also divisible by p. This'll show that p divides the order of $Z(G)$ and allows us to conclude that $Z(G)$ is non-trivial.

By the Orbit Stabiliser Theorem, for each x, $|Gx|$ is equal to the index of the centraliser of x in G. Lagrange's Theorem implies that the order of $C_G(x)$

divides the order of G, and so $|C_G(x)| = p^k$ for some k between 0 and n. But, for x such that $|Gx| \geq 2$, the centraliser is a proper subgroup of G: the centraliser must contain x itself and so $k \geq 1$. On the other hand, $G_x \neq G$ and so $k \leq n-1$. Hence for $x \in S$ with $|Gx| > 1$, $|Gx| = [G : C_G(x)] = p^{n-k}$ where $n - k \geq 1$. This implies that $\sum_{x\in S,\ |Gx|>1} |Gx|$ is also divisible by p, as required. This proves 1.

To prove 2.) we have that $|G| = p^2$. Now we know from 1. that $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$ then $Z(G) = G$ and so the group is abelian. So, we can assume that $|Z(G)| = p$. Recall that $Z(G)$ is a normal subgroup of G and so $G/Z(G)$ is a group. Moreover $|G/Z(G)| = [G : Z(G)] = \frac{p^2}{p} = p$. Every group of prime order is cyclic, so we know that $G/Z(G)$ is a cyclic group of order p. The Lemma below completes the proof of Case 2. □

Lemma 26. *If $G/Z(G)$ is cyclic then G is abelian.*

Proof. Let $G/Z(G)$ be cyclic generated by the coset of $g \in G$ with respect to the centre. Let $a, b \in G$, we claim $ab = ba$. If either a or b lie in the centre then the two elements evidently commute. So we may assume that both a and b are not in the centre.

Now $a \in g^n Z(G)$ and $b \in g^m Z(G)$ for some n, m and so, we can write $a = g^n z$ and $b = g^m z'$ for some $z, z' \in Z(G)$. This implies

$$ab = (g^n z)(g^m z') = g^n g^m z z' = g^m g^n z' z = (g^m z')(g^n z) = ba.$$

The equalities above follow from the fact that z, z' commute with all elements of the group. This completes the proof of 2. □

Cauchy's Theorem

Theorem 27 (Cauchy's Theorem)**.** *Let G be a finite group and let a prime p divide the order $|G|$. Then G contains an element of order p.*

Proof not examinable but I will add it for those who are interested in the near future.

Chapter 9

Appendix : Some Preliminary Material

You would have come across the concepts below in courses from your first year as an undergraduate in RHUL. Here, we will give a brief account.

Set Theory

Group Theory, as we will see, is the study of sets endowed with Binary Operations with specific properties. Recall that a **set** is a well-defined collection of objects. For instance, the horses grazing in Windsor Great Park form a set, as do the collection of all real numbers $\mathbb{R}$. A set is made of its **elements** and as its name suggests, the empty set $\emptyset$ has none.

What does the expression 'well-defined' mean in the above sentence? A given object is either an element of the set or it is not. There is no room for ambiguity. So, $\sqrt{2}$ is a real number (written, $\sqrt{2} \in \mathbb{R}$), as is 2, but $i = \sqrt{-1}$ is not an element of $\mathbb{R}$. This is our usual understanding as $\mathbb{R}$ represents the set of ALL real numbers and not of SOME real numbers. In mathematics, being well-defined is important as otherwise, we would all be constantly misunderstanding each other.

Well-defined sub-collections of a set are sets in their own right, and in this case, we call such a collection a subset of the original. For example, the set of all rational numbers $\mathbb{Q}$ is a subset of the real numbers $\mathbb{R}$, written $\mathbb{Q} \subset \mathbb{R}$.

Equivalence Relations and Partitions

A **partition** of a set S is a decomposition of S into subsets such that every elements of S is in one and exactly one of the subsets.

For example The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ can be *partitioned* into the subset of all odd numbers and the subset of all even numbers. No number is both even and odd, which makes this decomposition into a partition.

One way to get a partition of a given set is to define an equivalence relation on it.

Theorem 28. *Let S be a non-empty set. Let $\sim$ be a relation between elements of S that satisfies the following properties.*

1. *(Reflexive) $a \sim a$ for all $a \in S$.*
2. *(Symmetric) If $a \sim b$ then $b \sim a$.*
3. *(Transitive) If $a \sim b$ and $b \sim c$ then $a \sim c$.*

Then, $\sim$ is called an equivalence relation and it naturally divides S into classes $[a] = \{s \in S : a \sim s\}$ that constitute a partition of S. Conversely, every partition of S naturally gives rise to an equivalence relation.

Example 29. *For each positive integer k, we can put an equivalence relation on $\mathbb{Z}$: $m \sim n$ if and only if $m \equiv n (mod\ k)$ meaning $m - n$ is divisible by k. The equivalence classes form the integers modulo k, commonly denoted by $\mathbb{Z}_k$. Representatives of the equivalence classes are the remainders in division by n and so we may write $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \bar{(n-1)}\}$*