Group Theory

Week 1, Lecture 1, 2 & 3

Dr Lubna Shaheen

How this module run

Lectures (3 hours) + Tutorials (1 hours): All lectures and tutorials will take place at MB-203 (Friday 9:00–11:00) and Arts Two 2.17 (Fridays 2:00–4:00pm).

Online Quizzes: There will be Quizzes in the form of online questions. There is no Quiz in Weeks 7. Each Quiz consists of 5-7 questions. These Quizzes DO NOT contribute to your final mark for this module.

Midterm Assessments: There will be one in-term assessment, in Weeks 7 with weightage 20% towards your final mark for this module. There will be no lectures or tutorials during Week 7.

Exams: There will be a final exam in Jan 2025 (details tbd). The contribution of the final exam to the module mark is 80%. The further details of the exam to be announce in due time.

Lecture Notes, Online Quizzes, Lecture slides, Tutorials (informal discussions of weekly material)

Table of Contents

Informal Preliminaries

In old days there was no concept of abstract groups, only thet consider a set X and a collection of operations on X such that these operations could be composed and inverting

Groups appear naturally, for example symmetries of geometric objects.

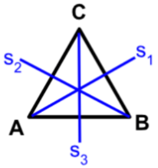
The operations that can be performed on a loose square tile: 0° (do nothing), 90° (rotate counterclockwise by 90°), 180°, 270°. Each of these operations can be inverted, e.g. the inverse of $270^\circ$is 90°, and one can compose them, e.g. $270 \circ 180^\circ = 90^\circ$.
Together, these four operations form a group called C_4 (the cyclic group of order 4).

Symmetries: mathematical object remain unchanged under a set of operations

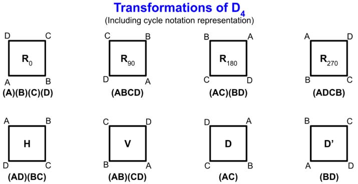
Natural groups: Symmetries of a regular polygon

Consider the symmetries of a regular polygon with n sides, where n is a positive integer. The dihedral group of order $2n$, denoted by D_n, is the group of all possible rotations and reflections of the regular polygon.

- **D_3**



- **D_4**



The group D_n consists of $2n$ elements.

Groups: Definition

Definition. A **group** is a set G, together with a binary operation $\circ$ on G, satisfying the following axioms.

G1 (closure): for every $g, h \in G$ we have $g \circ h \in G$.

G2 (associativity): for every $g, h, k \in G$ we have $(g \circ h) \circ k = g \circ (h \circ k)$.

G3 (identity): there is an element $1 \in G$ such that $1 \circ g = g = g \circ 1$ for every $g \in G$.

G4 (inverse): for every $g \in G$, there is an element g^{-1} such that $g^{-1} \circ g = 1 = g \circ g^{-1}$.

Groups: Examples

Important examples will be highlighted as easy (green), harder (blue) and very hard as exercises.

Example

(i) The set of all functions $\mathbb{R} \to \mathbb{R}$ with $\circ$ being the composition is not a group (no inverse). The set of all invertible functions (bijections) is a group.
(ii) $(\mathbb{R}, +)$ is a group; $(\mathbb{R}, \times)$ is not (0 does not have an inverse).

Example

D_3 Dihedral group of order 6 and D_4 Dihedral group of order 8.

Exercise

The group of symmetries of my IPAd (rectangle) is known as the dihedral group (D_2). This group consists of four elements:

Examples

Example

(i) $(\mathbb{Z}, +)$, non-negative integers is not a group. This set does not have inverses.
(ii) $(\mathbb{R}, +)$ is a group; $(\mathbb{R}, \times)$ is not (0 does not have an inverse).
(iii) A group with 2 elements, $\{1, \times\}$, $1.1 = 1, 1.x = x.1 = x$, the common name for x is -1. This make it the $\mathcal{C}_2 = \{1, -1\}$.

Exercise

D_5 dihedral group of order 10, is the group of symmetries of a regular pentagon. It is composed of 10 elements, which can be represented as rotations and reflections of the pentagon.

Some Useful Notations

Throughout this course, we use the following notation.

- $\mathcal{C}_n$ denotes the cyclic group of order n.
- Klein group often symbolized by the letter $\mathcal{V}_4$ or as $K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ denotes the group $\{1, a, b, c\}$, with group operation given by

$$a^2 = b^2 = c^2 = 1, \qquad ab = ba = c, \ ac = ca = b, \ bc = cb = a.$$

- $\mathcal{U}_n$ is the set of integers between 0 and n which are prime to n, with the group operation being multiplication modulo n.

Examples

Klein four-group $\mathcal{V}_4$

The Klein four-group $\mathcal{V}_4$, has elements $1, a, b, c$ and the group operation given by the table.

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

The Klein four-group is also defined by the group presentation

$$V =< a, b \,|\, a^2 = b^2 = (ab)^2 = 1 >$$

Examples

Klein four-group $\mathcal{V}_4$

It is, however, an abelian group, and isomorphic to D_2

1. All non-identity elements of the Klein group have order 2, so any two non-identity elements can serve as generators in the above presentation.
2. The Klein four-group is the smallest non-cyclic group.
3. is isomorphic to the dihedral group of order (cardinality) 4, symbolized as D_2 (using the geometric convention);
4. other than the group of order 2, it is the only dihedral group that is abelian.

Exercise

The Klein four-group also has a representation as 2×2 real matrices with the operation being matrix multiplication. Can you find the matrix elements of this group.

Definition: Calay Table

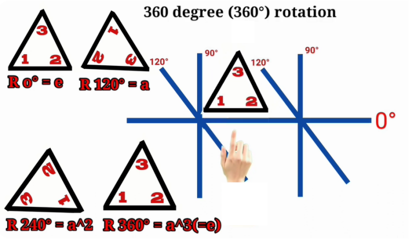
By organising all potential products of all group elements in a table that resembles an addition or multiplication table, a Cayley table describes the structure of a finite group.

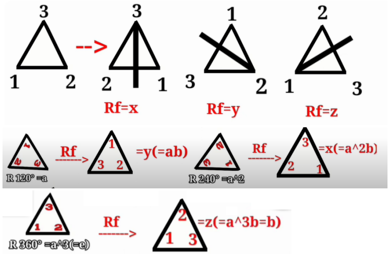
Properties of a Cayley Table:

Closure: Every entry in the table must be an element of the group.
Associativity: The operation must be associative, but this property is not directly visible in the table. It is a requirement for the structure to be a group.
Identity Element: Each row and each column must contain the identity element exactly once.
Inverses: Each row and each column must contain each element of the group exactly once (this implies that each element has an inverse).

Calylay table of Dihedral Group: D_3

The dihedral group D_6 is the symmetry group of an equilateral triangle, that is, it is the set of all transformations (reflections, rotations, and combinations of these) that leave the shape and position of this triangle fixed.





Calylay table of Dihedral Group: D_3

D_3, the group of symmetries of the equilateral triangle

	R_0	R_{120}	R_{240}	V	D	D'
R_0	R_0	R_{120}	R_{240}	V	D	D'
R_{120}	R_{120}	R_{240}	R_0	D	D'	V
R_{240}	R_{240}	R_0	R_{120}	D'	V	D
V	V	D'	D	R_0	R_{240}	R_{120}
D	D	V	D'	R_{120}	R_0	R_{240}
D'	D'	D	V	R_{240}	R_{120}	R_0

Calylay table of Dihedral Group: D_4

Exercise: Can you write down the rotations and reflections of a square such that the following calay table make sense.

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

Definition: Abelian groups

Definition: A group G is called abelian if for any $g, h \in G$

$$g \circ h = h \circ g$$

Example

(i) D_8, Dihedral group of order 8 is a non-abelian group.
(ii) Functions (bijections) of $\mathbb{R}$ is a non-abelian group.

Remarks and Notations:

(i) We write gh in place of $g \circ h$.
(ii) $g^5 = g \circ g \circ g \circ g \circ g$.
(iii) $g^0 = 1$
(iv) $g^{-1} =$ inverse of g, $g^{-2} = g^{-1} \circ g^{-1}$
(v) $g^n \circ g^m = g^{n+m}$, $g^{n^m} = g^{nm}$.

Definition: Abelian groups

Lemma

Suppose G is a group.
(i) The identity element of G is unique.
(ii) The inverse of any element is unique.
(iii) for any $g \in G$, $(g^{-1})^{-1} = g$.
(iv) for any $g, h \in G$

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

Definition: Order of a group

Definition: Let G be a group and $g \in G$.

1. The order of G, $|G|$ is the number of elements of G (possibly ∞).
2. The order of $g \in G$ is the smallest $n \geq 1$ such that $g^n = 1$ or ∞, if there is no such n.

Subgroup of a group

Definition: If $H \subseteq G$, where G is a group, then H is a subgroup if and only if
(i) $H \neq \emptyset$
(ii) $H \subset G$
(ii) H is itself a group with the same operation as of G.
We denote $H \leq G$ if H is a subgroup of G.

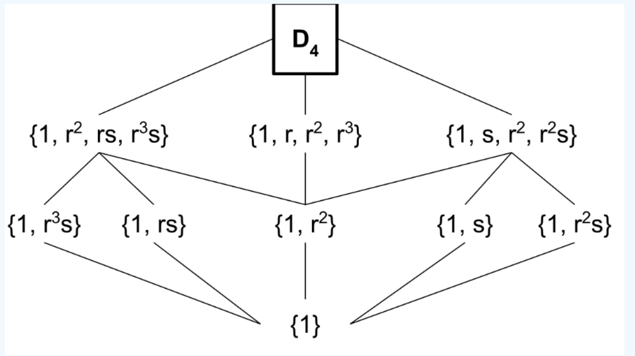
Example

(i) $G \leq G$
(ii) $\{1\} \leq G$
(iii) $\mathcal{V}_4 = \{1, a, b, c\}$, the Klein four-group. The set $\{1, a\} \leq \mathcal{V}_4$.
(iv) $\mathbb{R}^\times \leq \mathbb{C}^\times$.

Subgroup of D_4

Example

Find all the subgroups lattice of D_4.
Prove that every subgroup of D_4 of odd order is cyclic.



Subgroup of a group

Subgroup Test: If $H \subseteq G$, G is a group and H is a subgroup if and only if
(i) $H \neq \emptyset$
(ii) for any $g, h \in H$, $g \circ h^{-1} \in H$.

Exercise

(i) $(\mathbb{Z}_{+}, +)$ is not a subgroup.
(ii) Which subgroups of $(\mathbb{Z}, +)$ do you know?
(iii) Even integers $2\mathbb{Z} \leq \mathbb{Z}$.

Generators of a group

Definition: Let G be a group, $g \in G$, the subgroup generated by g is the set of all powers if g, i.e

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

$$= \{1, g, g^{-1}, g^2, g^{-2}, \cdots\}$$

Example

(i) $G = \mathcal{V}_4$, $\langle a \rangle = \{1, a\}$
(ii) $G = \mathbb{C}^\times$, $\langle i \rangle = \{1, i, -i, -1\}$
(iii) $G = \mathbb{R}^\times$, $\langle 2 \rangle = \{1, 2, 4, 8, 16, \cdots, \frac{1}{2}, \frac{1}{4}, \frac{1}{8} \cdots\}$

Generators of a group

Lemma

Let G be a group and $g \in G$, then $\langle g \rangle$ is a subgroup of G.

Lemma

Let G be a group, and $g \in G$, then $|\langle g \rangle| =$ ord(g)

Generators of a group

Subgroup generators by a set of elements

Definition: Let G be a group and $g_1, g_2, \cdots, g_r \in G$, the subgroup of G generated by $g_1, \cdots, g_r$ (notation $\langle g_1, \cdots, g_r \rangle$) is a subgroup of G. This will be the set of all elements which can be written as product of elements of $\{g_1, \cdots g_r, g_1^{-1}, \cdots, g_r^{-1}\}$.
If $G = \langle g_1, \cdots, g_r \rangle$ we say that $g_1, \cdots, g_r$ generate G.

Example:
Let $G = \mathbb{C}^{\times}$, the multiplicative group of nonzero complex numbers. You're given an element $g = \frac{1}{2}(1 + i\sqrt{3})$, and let $H = \langle g \rangle$. What is the order of H?
Solution: The first step is to write $g = \frac{1}{2}(1 + i\sqrt{3})$ in polar form, $re^{i\theta}$, where r is the modulus and θ is the argument.
Magnitude r of g is

$$r = |g| = |\frac{1}{2}(1 + i\sqrt{3})| = \frac{1}{2}|1 + i\sqrt{3}| = \frac{1}{2}\sqrt{1^2 + (\sqrt{3})^2} = \frac{1}{2} \times 2 = 1$$

Subgroup generators by a set of elements

Example

Thus, $r = 1$ so g lies on teh unit circle.

The argument θ is the angle whose tangent is $\frac{\sqrt{3}}{1}$ which is

$$\theta = arg(g) = tan^{-1}(\frac{\sqrt{3}}{1}) = \frac{\pi}{3}$$

Since $g = e^{i\pi/3}$ it is a root of unity. The order of g is the smallest positive integer n such that

$$g^n = e^{in\frac{\pi}{3}} = 1$$

For this to be true, $n\frac{\pi}{3}$ must be integer multiple of 2π. We solve and get $n\frac{\pi}{3} = 2\pi \Rightarrow n = 6$.

Generators of a subgroup

Example: Suppose G is a group and $f, g \in G$ with ord(f) $=$ 3, ord(g) $=$ 2 and gf $=$ fg. What is ord(fg)?

Solution: For fg to have order n we need $(fg)^n = e$, which implies $f^n g^n = e$. This can happen if both $f^n = e$ and $g^n = e$. From the orders of f and g we know
$f^3 = e$ so $f^n = e$, if and only if n is a multiple of 3.
$g^2 = e$ so $g^n = e$, if and only if n is a multiple of 2.
Thus, n must be the smallest number that is a multiple of both 2 and 3, which is the least common multiple LCM of 2 and 3. Thus $(fg)^6 = f^6 g^6 = e$, and the smallest such n is 6.

Generators of a subgroup

Exercise

Suppose G is a group and $g \in G$ with ord(g)=6. What is ord(g^4)?

Exercise

Suppose G is a group and $f, g \in G$ with $ord(f) = 3$, $ord(g) = 2$ and $gf = f^2 g$. What is $ord(fg)$?

Exercise

Let H be the subgroup of $\mathbb{Q}^{\times}$ generated by 2 and -3. Write down few elements belong to H.

Generators of a group

Exercise

Let H be the subgroup of $\mathbb{Q}_+^\times$ generated by 9 and 20^{-1}. Write down few elements of H.

Exercise

Let G be an abelian group and n a positive integer, and let

$$H = \left\{ x \in G : \ x^n = e \right\}$$

Prove that the set H is a subgroup of G. Give an example to show that this conclusion may not be true if G is a non-abelian group.

Exams Style Questions

Exam Year, 2022

Question 1 [21 marks].

(a) Give the definition of a **group**. **[3]**

(b) Give the definition of a **subgroup**. **[2]**

(c) Let

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \,\middle|\, a + c = b + d \right\}.$$

Prove that H is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. **[5]**

Suppose G is a group and $f, g \in G$.

(d) Prove that the inverse of g is unique. **[4]**

(e) Give the definition of the **order** of g. **[2]**

(f) Suppose g has order 4, and $gf = f^{-1}g$. What is the order of fg? *[Show your working.]* **[5]**

Exams Style Questions

Exam Year, 2023

(b) Complete the following table in a way which results in the Cayley table of a group.

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

[5]

(c) The following table is **not** the Cayley table of a group. Indicate which group axioms are inconsistent with the operation defined by this table. For each group axiom which is inconsistent with the table, give an example of where in the table the inconsistency occurs.

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

[5]

QMplus Quiz 1

Attempt Quiz 1 at QMplus page

References: (i) Lior Silberman, "Introduction to Group Theory Lecture Notes", Available online.
(ii) Humphreys, John F, "A Course in Group Theory" (Oxford Science Publications) ISBN 10: 0198534590 / ISBN 13: 9780198534594 Published by Oxford University Press, USA, 1996

Some Useful Notations

Throughout this course, we use the following notation.

- $\mathcal{C}_n$ denotes the cyclic group of order n.
- Klein group often symbolized by the letter $\mathcal{V}_4$ or as $K_4 = \mathbb{Z}_4 \times \mathbb{Z}_4$ denotes the group $\{1, a, b, c\}$, with group operation given by

$$a^2 = b^2 = c^2 = 1, \qquad ab = ba = c,\ ac = ca = b,\ bc = cb = a.$$

- $\mathcal{U}_n$ is the set of integers between 0 and n which are prime to n, with the group operation being multiplication modulo n.

Some Useful Notations

- $\mathcal{D}_{2n}$ is the group with $2n$ elements

$$1,\ r,\ r^2,\ \ldots,\ r^{n-1},\ s,\ rs,\ r^2s,\ \ldots,\ r^{n-1}s.$$

  The group operation is determined by the relations $r^n = s^2 = 1$ and $sr = r^{n-1}s$.
- $\mathcal{S}_n$ denotes the group of all permutations of $\{1, \ldots, n\}$, with the group operation being composition.
- $GL_n(\mathbb{R})$ is the group of $n \times n$ invertible matrices with entries in $\mathbb{R}$, with the group operation being matrix multiplication.
- $\mathcal{Q}_8$ is the group $\{1, -1, i, -i, j, -j, k, -k\}$, in which

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