Group Theory

Week 2, Lecture 1, 2 & 3

Dr Lubna Shaheen

Table of Contents

Examples of Groups

Symmetries of Geometric objects

D_{2n} = group of symetries of the regular n-polygon.

$$D_{2n} = \{1, r, \cdots, r^{n-1}, s, rs, r^2s, \cdots, r^{n-1}s\}$$

generated by rotations r, clockwise rotation by $2\pi/n$ and a reflection s about the y-axis, where $r^n = 1$ and $s^2 = 1$.This group is defined by

$$D_{2n} = \langle r, s | s^2 = e,\ r^n = e, srs = r^{-1} \rangle \text{ and } |D_{2n}| = 2n.$$

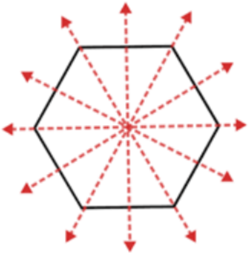
Examples of Groups

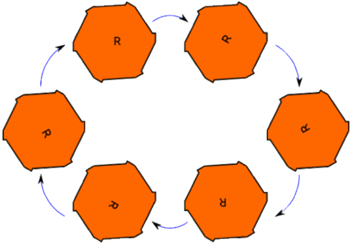
Example: The group of symmetries of a hexagon is known as the dihedral group, denoted as D_{12} consists of the symmetries that can map the hexagon onto itself. These symmetries include:

Rotational Symmetries: Rotation by $0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ$.

Reflective symmetries: There are 6 axes of symmetry for a regular hexagon, 3 axes passing through opposite vertices, 3 axes passing through midpiunts of opposite sides.

$$D_{12} = \{1, r, r^2, r^3, r^4, r^5, s, rs, r^2s, r^3s, r^4s, r^5s\}$$





Examples of Groups

Examples of Groups

The symmetry group of a subset $P \subseteq R^n$ depends on the geometric properties of P. It consists of all isometries that map P onto itself, preserving the distances between points in P. For finite sets, this often corresponds to a finite group of discrete symmetries (such as rotations and reflections), while for infinite or more structured sets like circles or spheres, the symmetry group can be continuous and infinite.

For any subset $P \subseteq R^n$, the symmetry group $\text{Sym}(P)$ is a subgroup of the isometry group of R^n, which consists of all distance-preserving transformations in $\mathbb{R}^n$.

Translations, Rotations, Reflections, Rotoreflections

Examples of Groups

Examples of Symmetry Groups for Specific Subsets P:

1. Points in $\mathbb{R}^n$
2. Line Segment in $\mathbb{R}^2$
3. Regular Polygon in $\mathbb{R}^2$
4. Circle in $\mathbb{R}^2$

Examples of Groups

Examples of Groups

Symmetric group: Group of all permutations on n symbols

Observation: Let X be a set, consider $f : X \to X$ the binary operation $\circ$

$$(f \circ g)(x) = f(g(x))$$

is associative $f \circ (g \circ h) = (f \circ g) \circ h$.

Proof:

Examples of Groups

Symmetric group: Group of all permutations on n symbols

X-set , Sym(X)= $\{$the collection of one-to-one and onto function $f : X \to X\}$

The symmetric group of degree n is the symmetric group on the set $X = \{1, 2, 3, \cdots, n\}$ will be denoted by S_n.

Claim

Claim: Sym(X) equipped with $\circ$ is a group.

Verification of group axioms

Symmetric group: Group of all permutations on n symbols

Disjoint cylce notation:

The group operation in a symmetric group is function composition, denoted by the symbol $\circ$ or simply by just a composition of the permutations.

$$f = (13)(2)(45) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

$$g = (125)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

We ll apply first g and then f.

$$fg = f \circ g = (124)(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

Verification of group axioms

Symmetric group: Group of all permutations on n symbols

Remarks:

1. Symmetric groups on infinite sets behave quite differently from symmetric groups on finite sets.
2. The symmetric group on a set of n elements has order $n!$.
3. It is abelian if and only if n is less than or equal to 2.
4. For $n = 0$ and $n = 1$ (the empty set and the singleton set), the symmetric groups are trivial (they have order 0! and 1!.

The symmetric group on a set of size n is the Galois group of the general polynomial of degree n and plays an important role in Galois theory.

Symmetric group

S_2, symmetric group of degree 2

This group consists of exactly two elements: the identity and the permutation swapping the two points. It is a cyclic group and is thus abelian.

S_3, symmetric group of degree 3, $S_3 \cong D_6$

S_3 is the first non-abelian symmetric group. This group is isomorphic to the dihedral group of order 6, (D_6) the group of reflection and rotation symmetries of an equilateral triangle, since these symmetries permute the three vertices of the triangle. Cycles of length two correspond to reflections, and cycles of length three are rotations.

Symmetric group

Symmetric group

Cyclic group

The cycic group of order n.

$\mathcal{C}_n = \{1, z_n, z_n^2, \cdots, z_n^{n-1}\}$ where z_n is an element of order n.

Example: $z_n = e^{2\pi i/n}$.

Another visualisation is

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \cdots, n-1\}$$

with addition.

Cyclic group

Cyclic Groups: The infinite cyclic group

$$\mathcal{C}_\infty = \{1, z, z^2, z^3, \cdots z^{-1}, z^{-2}, z^{-3}, \cdots\}$$

where z is an element of infinite order.

Example:

(i) $\mathbb{Z} = \{0, +1, -1, +2, -2, +3, -3, \cdots\}$
(ii) G-group, $g \in G$, $\langle g \rangle$ is a cyclic group.

Integer modulo n Group

Consider the multiplicative subgroup Integers module n,

$$\mathcal{U}_n = (\mathbb{Z}/n\mathbb{Z})^\times = \{1, 2, \cdots, n-1\} =$$

$$\{\text{numbers from } 1 \text{ to } n-1\text{, which are co-prime to n}\}.$$

$\mathcal{U}_{12} = \{1, 5, 7, 11\}$

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

This is essentially equal to $\mathcal{V}_4$.

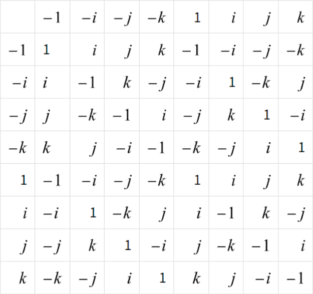
Integer modulo *n* Group

Result: $\mathcal{U}_n$ is a subgroup of $\mathrm{Sym}(\mathbb{Z}/n\mathbb{Z})$.

The Quaternion group

The quaternion group $\mathcal{Q}_8$ (sometimes just denoted by $\mathcal{Q}$) is a **non-abelian** group of order eight, isomorphic to the eight-element subset $\{1, i, j, k, -1, -i, -j, -k\}$ of the quaternions under multiplication.

Quaternion group multiplication table (simplified form)



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

$$i^2 = j^2 = k^2 = -1,$$
$$-1.i = -i, -1.j = -j,\ -1.k = -k$$
$$i.j = k,\ k.k = i,\ k.i = j$$
$$j.i = -k, k.j = -i, i.k = -j$$

The Quaternion group

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

$$j \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ k \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

1. $\mathcal{Q}_8$ is non-abelian.
2. Its subgroups are {1}, {-1,1}, {-1,1,-i,i}, {-1,1,-j,j}, {-1,1,-k,k}, and {-1,1,-i,i,-j,j,-k,k}.

Matrix group: General linear group, $\mathrm{GL}_n(\mathrm{R})$ or GL(n, R).

Definition

In mathematics, the general linear group of degree n is the set of n×n invertible matrices, together with the operation of ordinary matrix multiplication. This forms a group, because the product of two invertible matrices is again invertible, and the inverse of an invertible matrix is invertible, with the identity matrix as the identity element of the group.

Remark: A matrix is invertible iff its determinant is not 0.

Matrix group: General linear group, $\mathrm{GL}_n(\mathbb{R})$ or GL(n, $\mathbb{R}$).

Real numbers case: The general linear group GL(n, $\mathbb{R}$) over the field of real numbers is a real Lie group of dimension n^2. To see this, note that the set of all $n \times n$ real matrices, $\mathrm{M}_n(\mathbb{R})$, forms a real vector space of dimension n^2. The subset GL(n, $\mathbb{R}$) consists of those matrices whose determinant is non-zero.

Complex numbers case: The general linear group over the field of complex numbers, GL(n, $\mathbb{C}$), is a complex group of complex dimension n^2. As a real Lie group (through realification) it has dimension $2n^2$. The set of all real matrices forms a real Lie subgroup. These correspond to the inclusions

$$GL(n, \mathbb{R}) < GL(n, \mathbb{C}) < GL(2n, \mathbb{R})$$

which have real dimensions $n^2, 2n^2$, and $4n^2 = (2n)^2$.

Matrix group: General linear group, GL$_n(\mathbb{R})$ or GL(n, $\mathbb{R}$).

Finite field case: Let $\mathbb{F}$ be a field, then the general linear group $GL_n(\mathbb{F})$ consists of all the invertible $n \times n$ matrices over $\mathbb{F}$, the operation key matrix multiplication.

Exercise: $\mathbb{F}_2 = \{0, 1\}$.

$$GL_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 & \\ 0 & 1 & \end{pmatrix}, \begin{pmatrix} 1 & 1 & \\ 0 & 1 & \end{pmatrix} \begin{pmatrix} 1 & 0 & \\ 1 & 1 & \end{pmatrix}, \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \end{pmatrix} \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \end{pmatrix}, \begin{pmatrix} 0 & 1 & \\ 1 & 1 & \end{pmatrix} \right\}$$

Exercise: Comput $|GL_{100}(\mathbb{F}_2)|$.

Matrix group: General linear group, $\mathbf{GL}_n(\mathbb{R})$ or $\mathbf{GL}(n,\mathbb{R})$.

Definition: The speciall linear group $\mathrm{SL}_n(\mathbb{P})$ consists of $n \times n$ matrices with determinant 1.

Definition: The speciall linear group $\mathrm{SL}_2(\mathbb{R})$ is the group of 2×2 real matrices with determinant 1.

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, \text{ and } ad - bc = 1 \right\}$$

$|SL_2(\mathbb{R})|$ is infinite.

Upper traingular matrix

Subgroups of $\mathbf{SL}_2(\mathbb{R})$:

Cyclic Subgroups: Cyclic groups generated by one element of $\mathrm{SL}_2(\mathbb{R})$. If $A \in \mathrm{SL}_2(\mathbb{R})$, then $\langle A \rangle = \{A^n | n \in \mathbb{Z}\}$ forms a cyclic subgroups.

Diagonal Subgroups: The diagonal matrices with determinant 1 form a subgroup of $\mathrm{SL}_2(\mathbb{R})$. This subgroup is isomorphic to $\mathbb{R}^*$, the multiplicative group of non-zero real numbers:

$$= \left\{ \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} & \end{pmatrix} : a \in \mathbb{R} \right\}$$

Upper traingular matrix

Upper Triangular Subgroup (Borel Subgroup):
The set of upper triangular matrices with determinant 1 forms an important subgroup, called the Borel subgroup:

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} : a \in \mathbb{R}^*, b \in \mathbb{R} \right\}$$

Rotation Subgroup (SO(2))
The special group
SO(2) is a subgroup of $\mathrm{SL}_2(\mathbb{R})$, consisting of all rotations in $\mathbb{R}^2$:

$$SO(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}$$

Upper traingular matrix

Exercise: Consider the **Upper triangular matrix with 1 on the diagonals**. Check if this is subgroup of $\mathsf{SL}_2(\mathbb{R})$.

Upper traingular matrix

Definition: The upper triangular matrix has all the elements below the main diagonal as zero. Also, the matrix which has elements above the main diagonal as zero is called a lower triangular matrix, also, written in the form of;

$$U = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} & a_{1,r+1} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2r} & c_{2,r+1} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & \vdots & & \\ 0 & 0 & \cdots & a_{rr} & a_{r,r+1} & \cdots & \\ 0 & 0 & \cdots & 0 & a_{r+1,r+1} & \cdots & \\ \vdots & \vdots & & \vdots & \vdots & & \\ 0 & 0 & \cdots & 0 & 0 & \cdots & a_{m,n} \end{pmatrix}$$

Upper traingular matrix

Properties of Upper Triangular Matrix

1. If we add two upper triangular matrices, it will result in an upper triangular matrix itself.
2. If we multiply two upper triangular, it will result in an upper triangular matrix itself.
3. The inverse of the upper triangular matrix remains upper triangular.
4. The transpose of the upper triangular matrix is a lower triangular matrix, $U^T = L$.
5. If we multiply any scalar quantity to an upper triangular matrix, then the matrix still remains as upper triangular.

Exams Style Questions

Exam Year, 2024

Question 1

(a) For the following, either give an example or explain why no example can exist:

(i) A group with at least four elements in which every element has order either 1 or 2.

(ii) A group with at least four elements in which every element has order either 1 or 4.

(iii) Two groups of order 24 which are not isomorphic to one another.

(iv) Two countably infinite groups which are not isomorphic to each other.

(b) Let $G = \{x \in \mathbb{R} \colon x \geq 0\}$ and define a binary operation $\circ$ on G by $x \circ y := |x - y|$. Decide which of the four group axioms are satisfied by $(G, \circ)$ and which are not. For each axiom, give a brief justification for your answer.

Exams Style Questions

(c) Using Lagrange's theorem, or otherwise, show that if g is an element of a group G such that $|G| = n$, then g^n is the identity element of G.

(d) Using the result of (c) above, show that if p is a prime number and n is an integer in the range $1 \leq n \leq p$, then $n^{p-1} \equiv 1 \mod p$. (Hint: consider the group $\mathcal{U}_p$.)

(e) List all subgroups of the dihedral group $\mathcal{D}_{10}$ and indicate briefly why your list is complete.

Exams Style Questions

Question 2: Classify all groups of order 4 up to isomorphism.

Sol:Let G be a group with order $|G| = 4$. Then, we know by Lagrange's theorem that non-identity elements of G can have orders 2 or 4.

1. If G contains an element of order 4, then G is cyclic and therefore isomorphic to $\mathbb{Z}_4$.
2. If G does not contain an element of order 4, the only other possibility is that all 3 non-identity elements have order 2. If we let $G = \{e, b_1, b_2, b_3\}$, we consider the value of $b_1 b_2$. If $b_1 b_2 = e$, then $b_1 = b_2$, a contradiction. If $b_1 b_2 = b_1$ or $b_1 b_2 = b_2$, then we conclude one of b_1 and b_2 is the identity, again a contradiction. So, we must have $b_1 b_2 = b_3$. Then, we define a mapping $\varphi : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$:

$$\varphi : e \to (0,0)$$

$$\varphi : b_1 \to (0,1)$$

$$\varphi : b_2 \to (1,0)$$

$$\varphi : b_3 \to (1,1)$$

giving us an isomorphism from G to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Therefore, every group G of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Question 3: Classify all groups of order 8 up to isomorphism.

Exams Style Questions

Exam Year, 2022

Question: Give examples of
(a) A group of order 24 which is not abelian.

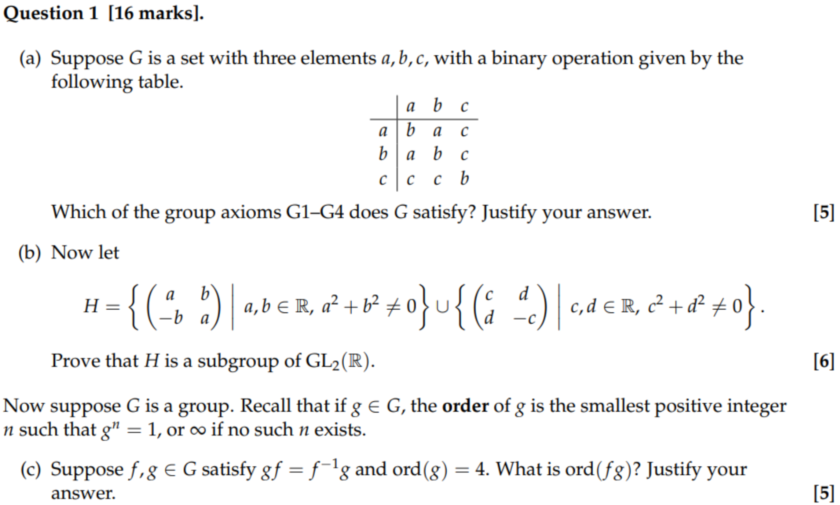
(b) A group of infinite order which is not abelian.

(c) A pair of abelian groups of the same order which are not isomorphic to one another.

(d) A group G and a two subgroups H_1, $H_2 \leq G$ such that $H_1 \cup H_2$ is npt a subgroup of G.

Exams Style Questions

Exam Year, 2021



Question 1 [16 marks].

(a) Suppose G is a set with three elements a, b, c, with a binary operation given by the following table.

	a	b	c
a	b	a	c
b	a	b	c
c	c	c	b

Which of the group axioms G1–G4 does G satisfy? Justify your answer. **[5]**

(b) Now let

$$H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R},\ a^2 + b^2 \neq 0 \right\} \cup \left\{ \begin{pmatrix} c & d \\ d & -c \end{pmatrix} \,\middle|\, c, d \in \mathbb{R},\ c^2 + d^2 \neq 0 \right\}.$$

Prove that H is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. **[6]**

Now suppose G is a group. Recall that if $g \in G$, the **order** of g is the smallest positive integer n such that $g^n = 1$, or ∞ if no such n exists.

(c) Suppose $f, g \in G$ satisfy $gf = f^{-1}g$ and $\mathrm{ord}(g) = 4$. What is $\mathrm{ord}(fg)$? Justify your answer. **[5]**

Exams Style Questions

Exams Question 2022

Recall that $GL_n(\mathbb{R})$ denotes the group of invertible $n \times n$ matrices with real entries. Let O(n) denote the set

$$O(n) = \{A \in GL_n(\mathbb{R}) : A^T A = I\}$$

where I denotes the $n \times n$ identity matrix and A^T denotes the transpose of the matrix A. Show that $O(n)$ is a subgroup of $GL_n(\mathbb{R})$.

Exams Style Questions

QMplus Quiz 2

Attempt Quiz 2 at QMplus page

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

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