

Group Theory

Week 1, Lecture 1, 2 & 3

Dr Lubna Shaheen

l.shaheen@qmul.ac.uk

ahw811@qmul.ac.uk

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

1 Informal Preliminaries

- Natural groups: Symmetries of a regular polygon
- Klein four-group \mathcal{V}_4

2 Definition: Groups

- Cayley table
- Abelian groups
- Order of a group and an element
- Subgroup of a group
- Generators of a group
- Subgroup generated by a set of element

3 Exams Style Questions

Informal Preliminaries

Regular polygons.

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

Regular means equal side.

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° is 90° , and one can compose them, e.g. $270^\circ \circ 180^\circ = 90^\circ$.

These are symmetries of a regular square.

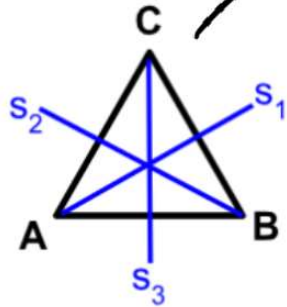
Together, these four operations form a group called C_4 (the cyclic group of order 4).

Symmetries: mathematical object remain unchanged under a set of operations

Natural groups: Symmetries of a regular polygon

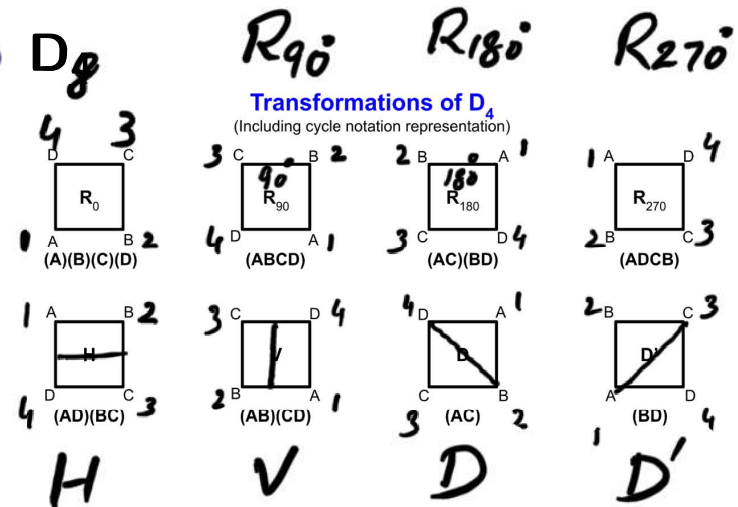
Consider the symmetries of a regular polygon with n sides, where n is a positive integer. The dihedral group of order $2n$, denoted by D_n , is the group of all possible rotations and reflections of the regular polygon.

• D_3



*Symmetries
of Triangle.*

• D_8



The group D_n consists of $2n$ elements.

$$D_8 = \{ R_0, R_{90^\circ}, R_{180^\circ}, R_{270^\circ}, H, V, D, D' \}$$

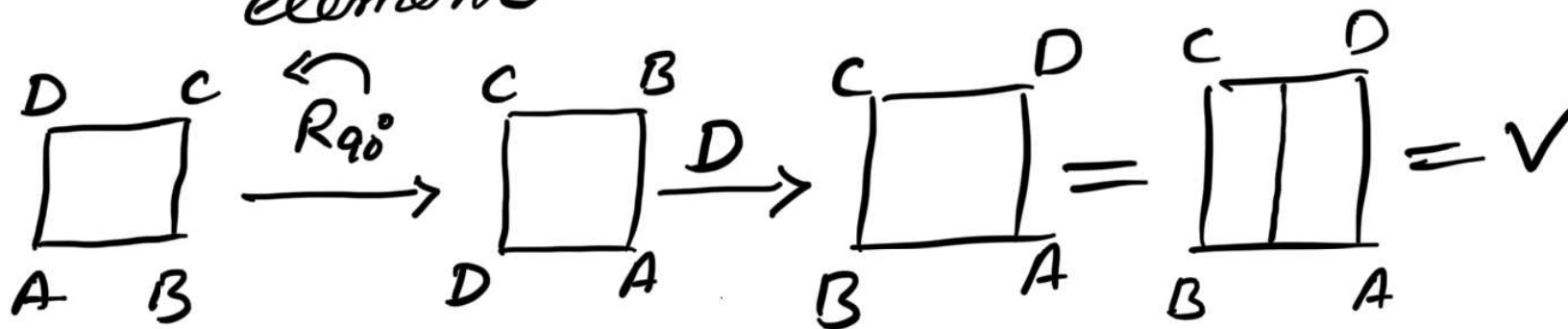
Groups: Definition

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

- G_1 G1 (closure): for every $g, h \in G$ we have $g \circ h \in G$.
- G_2 G2 (associativity): for every $g, h, k \in G$ we have $(\underline{g \circ h}) \circ \underline{k} = g \circ (\underline{h \circ k})$.
- G_3 G3 (identity): there is an element $1 \in G$ such that $1 \circ g = g = g \circ 1$ for every $g \in G$.
- G_4 G4 (inverse): for every $g \in G$, there is an element g^{-1} such that $g^{-1} \circ g = 1 = g \circ g^{-1}$.

1, e means identity element

closure property



Groups: Examples

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

Example

- (i) The set of all functions $\mathbb{R} \rightarrow \mathbb{R}$ 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

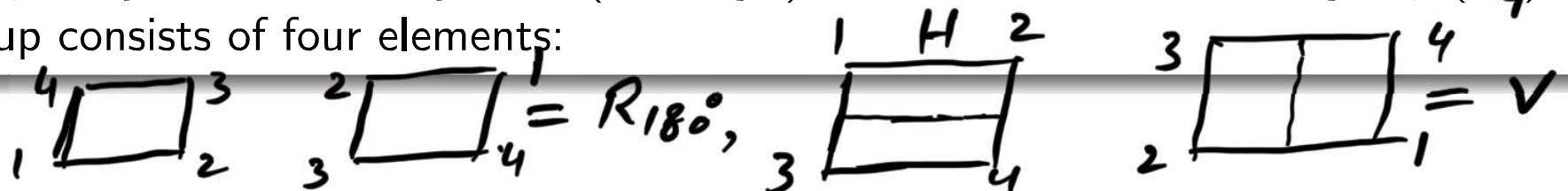
D_3 Dihedral group of order 6 and D_4 Dihedral group of order 8. ✓

D_3 is D_6 and D_4 is D_8 . (Should be consistent with our notations)

Exercise

The group of symmetries of my IPad (rectangle) is known as the dihedral group (D_4).

This group consists of four elements:



Examples

*It has 4 elements — D_4
we will see that $D_4 \cong V_4$*

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, $\{1, x\}$, $1.1 = 1$, $1.x = x.1 = x$, the common name for x is -1 . This makes it the $C_2 = \{1, -1\}$.

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.

D_5 should be D_{10} = Dihedral group of symmetries of a regular pentagon.

Some Useful Notations

Throughout this course, we use the following notation.

- C_n denotes the cyclic group of order n .
- Klein group often symbolized by the letter 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

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

- \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 .

we'll come to this group in next week.

Examples

Klein four-group \mathcal{V}_4

$$a^2 = b^2 = c^2 = 1, \quad ab = ba = c \\ ac = ca = b$$

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

$$\mathcal{V}_4 = \{1, a, b, c\}$$

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

$$bc = cb = a$$

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

$$V = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1 \rangle$$

This is because $c = ab$, we can replace c with ab

Examples

Klein four-group 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 *or* D_4 (using the geometric convention);
- ④ other than the group of order 2, it is the only dihedral group that is abelian.

Exercise

$$V_4 \cong D_4$$

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.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

check out $a^2 = b^2 = c^2 = I$

Definition: Cayley Table

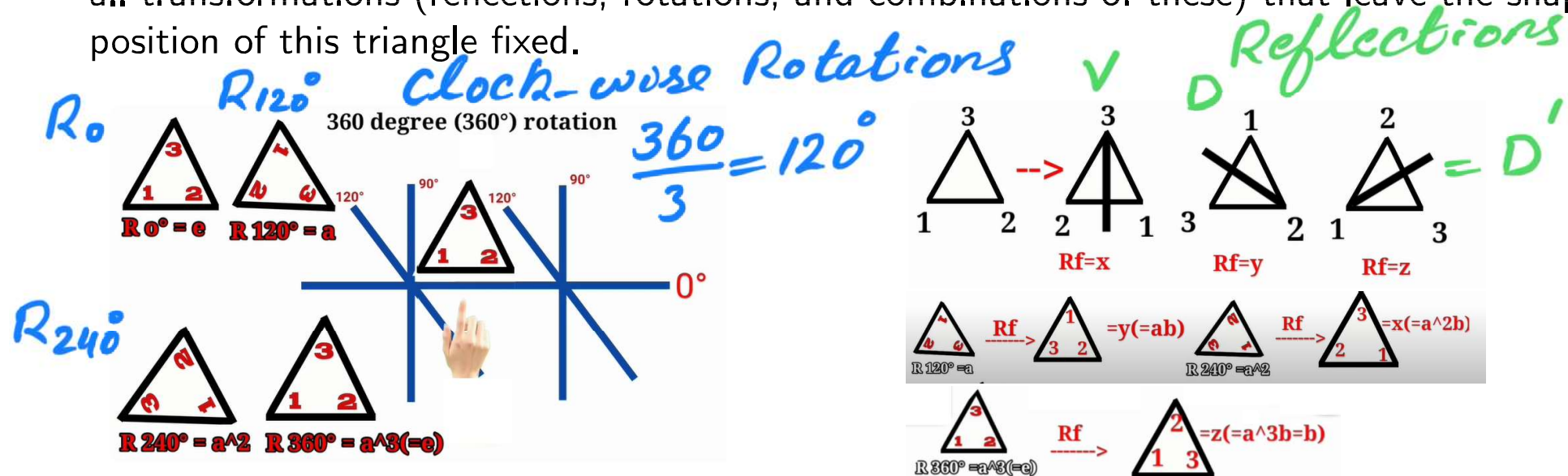
By organising all potential products of all group elements in a table that resembles an addition or multiplication table, a Cayley table describes the structure of a finite group.

Properties of a Cayley Table:

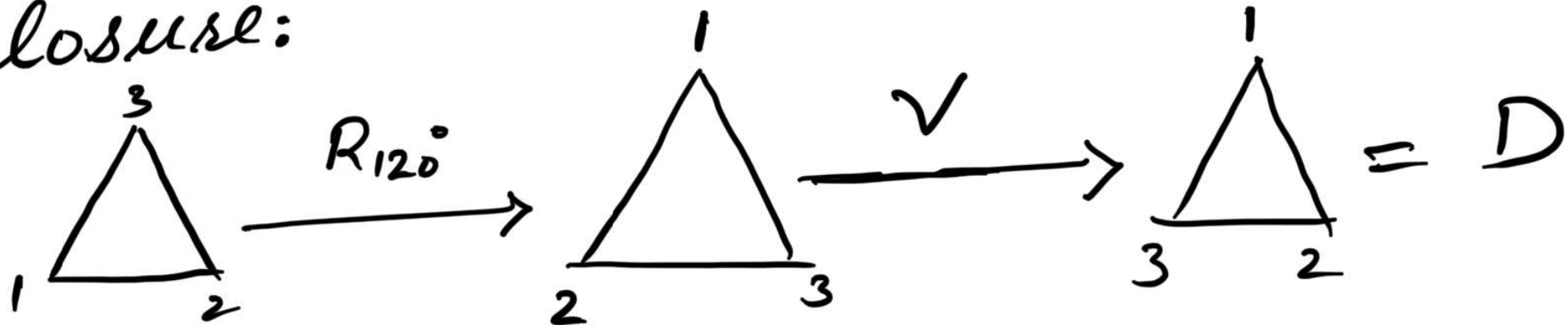
- G_1 : **Closure**: Every entry in the table must be an element of the group.
- G_2 : **Associativity**: The operation must be associative, but this property is not directly visible in the table. It is a requirement for the structure to be a group.
- G_3 : **Identity Element**: Each row and each column must contain the identity element exactly once.
- G_4 : **Inverses**: Each row and each column must contain each element of the group exactly once (this implies that each element has an inverse).

Cayley 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.



closure:



Cayley table of Dihedral Group: D_6

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

V = vertical flip
 D = Diagonal flip
 D' = opp Diagonal flip

$$D_6 = \{ R_0, R_{120}, R_{240}, V, D, D' \}$$

G_1 : Closure

G_2 : Associativity (check manually)

G_3 : Identity

G_4 : Inverses

Cayley table of Dihedral Group: D_8

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

*Cyclic
subgroup of
 D_8 - Rotations*

	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

$$D_8 = \{ R_0, R_{90^\circ}, R_{180^\circ}, R_{270^\circ}, H, V, D, D' \}$$

Definition: Abelian groups

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

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


Example

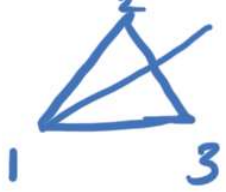
- (i) D_8 , Dihedral group of order 8 is a non-abelian group.
- (ii) Functions (bijections) of \mathbb{R} is a non-abelian group.

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) $g^n \circ g^m = g^{n+m}$, $g^{n^m} = g^{nm}$.

D_6 :

$\triangle \circ R_{120} =$ 

$R_{120} \circ \triangle =$ 

Non-Abelian
Dihedral group of triangle.

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 $g, h \in G$

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

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

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

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1} \quad \leftarrow \text{implies}$$

(i) $\tilde{1}$ is an additional identity, then

$$1 = 1 \cdot \tilde{1} = \tilde{1} \rightarrow \text{if } 1 \text{ is the identity}$$

$$\text{If } \tilde{1} \text{ is the identity} \Rightarrow 1 = \tilde{1}$$

(ii) $g \in G, h_1, h_2 \in G$ s.t. that

$$\left. \begin{array}{l} gh_1 = h_1g = 1 \\ gh_2 = h_2g = 1 \end{array} \right\} \Rightarrow h_1 = h_2$$
$$h_2 = 1 \cdot h_2 = h_1g \cdot h_2 = h_1$$

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 .

Examples:

$$|D_8| = 8$$

$$\text{ord}(\mathbb{R}^\times) = \infty$$

$$|D_6| = 6$$

$$\text{ord}(\mathbb{C}^\times) = \infty$$

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

$$\text{ord}(V_4) = 4$$

Subgroup of a group

Definition: If $H \subseteq G$, where G is a group, then H is a subgroup if and only if

✓ (i) $H \neq \emptyset$ *v. group property.*

(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) $\mathbb{R}^\times \leq \mathbb{C}^\times$.

Similarly $\{1, b\} \leq \mathcal{V}_4$
 $\{1, c\} \leq \mathcal{V}_4$

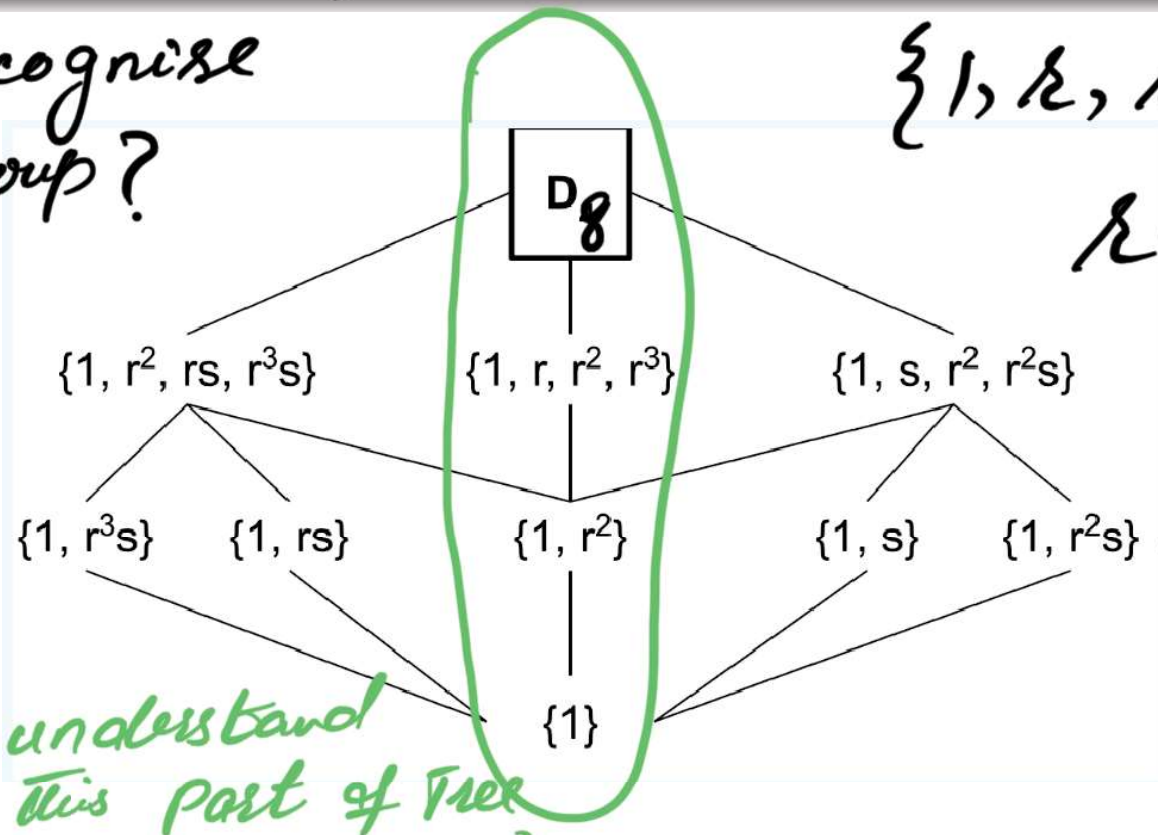
Subgroup of D_4

Example

Find all the subgroups lattice of D_8

Prove that every subgroup of D_8 of odd order is cyclic.

can you recognise
any subgroup?



$$\{1, r, r^2, r^3\}$$

$r = \text{Rotation}$
 $= R_{90^\circ}$

$s = \text{Reflection}$

I hope you understand
this part of tree

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 $g, h \in H$, $\underline{g \circ h^{-1}} \in H$.

Exercise

- (i) $(\mathbb{Z}_+, +)$ is not a subgroup. $5 \in \mathbb{Z}_+, -5 \notin \mathbb{Z}_+$
- (ii) Which subgroups of $(\mathbb{Z}, +)$ do you know? *Even integers under +*
- (iii) Even integers $2\mathbb{Z} \leq \mathbb{Z}$.

$$g, h \in 2\mathbb{Z}$$

$$gh^{-1} = g - h \in 2\mathbb{Z}$$

$$2 - 6 = -4$$

$(2\mathbb{Z}, +)$ is a subgroup of \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 of g , i.e

Subgroup generated by g $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

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

Example

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

$$\langle b \rangle = \{1, b\} \leq \mathcal{V}_4$$

$$\langle i \rangle = \{i, -1, -i, 1\}$$

$$\mathbb{C}^\times = \{a + ib \mid a, b \in \mathbb{R}\}$$

Generators of a group we'll apply subgroup test

Lemma

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

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = \{g, g^2, g^{-2}, g^4, \dots, g^0, \dots\}$$

$g \in \langle g \rangle$, so it's non-empty

$$g^m, g^n \in \langle g \rangle$$

$$(g^m)(g^n)^{-1} = g^{m-n} \in \langle g \rangle$$

Lemma

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

Proof: Case I If $\text{ord}(g) = \infty$, there is no
 $n \neq 1$, $g^n = 1$ & $\{g^n : n \in \mathbb{Z}\}$ are distinct

Generators of a group

If not $g^n = g^m$ $n > m$
 $g^{n-m} = \underline{1}$ contradiction

Case II $\text{ord}(g) = n < \infty$, $g^n = 1$, $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$
all are distinct. For any m , we ll

have $g^m = g^{nk+r}$ $0 \leq r < n$, $m \in \mathbb{Z}$

$$g^m = g^{nk} \cdot g^r = (g^n)^k g^r = g^r$$

$$\Rightarrow g^{r_1 - r_2} = \underline{1}$$

Contradiction

Now

$$g^{r_1} = g^{r_2}$$

$$0 < r_1 < r_2 < n$$

All elements are distinct.

Subgroup generators by a set of elements

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

$$g = \frac{1}{2} + i\frac{\sqrt{3}}{2} = r\cos\theta + i r\sin\theta$$

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

$$g^n = 1, \quad n = ?$$

Polar Coordinates

Subgroup generators by a set of elements

Example

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

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

$$r = \sqrt{a^2 + b^2} \quad a = \frac{1}{2}, \quad b = \frac{\sqrt{3}}{2}$$
$$\theta = \arg(g) = \tan^{-1}\left(\frac{\sqrt{3}}{1}\right) = \frac{\pi}{3}$$

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

$$g^n = e^{in\frac{\pi}{3}} = 1 = \cos(2\pi) + i \sin(2\pi)$$

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

$$n\frac{\pi}{3} = 2\pi \Rightarrow n = 6.$$



$$n = 6$$

$$\cos(2\pi) = 1$$

$$\sin(2\pi) = 0$$

$$\sin \theta = \frac{1}{2}$$

$$\cos \theta = \frac{\sqrt{3}}{2}$$

$$\tan \theta = \sqrt{3}$$

Generators of a subgroup

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

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.

$$(fg)(fg) = f g f g = f \cdot f \cdot g \cdot g = f^2 g^2 = f^2$$

$$(fg)^2 \cdot (fg) = f^2 \cdot f \cdot g = g$$

$$(fg)^3 \cdot (fg) = g f g = f g^2 = f$$

$$(fg)^4 \cdot (fg) = f \cdot f \cdot g = f^2 g$$

$$\begin{aligned} (fg)^5 \cdot (fg) &= f^2 \cdot g f g \\ &= f^2 \cdot f \cdot g \cdot g \\ &= f^3 g^2 \\ &= e \end{aligned}$$

Generators of a subgroup

$$g^6 = e \quad (g^4)^3 = e \quad k=3$$

Exercise

$$\text{ord}(g^4) = 3$$

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

$$(g^4)^k = e \Rightarrow \begin{aligned} 4k &\equiv 0 \pmod{6} \\ 12 &\equiv 0 \pmod{6} \end{aligned}$$

Exercise

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

$$(fg)(fg) = f(f^2g) \cdot g = f^3 \cdot g^2 = e$$
$$\text{ord}(fg) = 2$$

Exercise

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

$$H = \{ 2^a (-3)^b : a, b \in \mathbb{Z} \}$$

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

$GL_2(\mathbb{R})$ = Group of all 2×2

Invertible matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H \text{ as } 1+0=0+1 \quad [3]$$

$$h = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \quad g = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \quad [4]$$

$$hg^{-1} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}^{-1} \quad [4]$$

Prove this is [2] in

H .

Question 1 [21 marks].

(a) Give the definition of a **group**.

(b) Give the definition of a **subgroup**.

(c) Let

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid a+c=b+d \right\}.$$

Prove that H is a subgroup of $GL_2(\mathbb{R})$.

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

(d) Prove that the inverse of g is unique.

(e) Give the definition of the **order** of g .

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

$$ad=1 \Rightarrow da=1$$

[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

$$ac=1$$

$$ca=d$$

Not true - Inverse property.

[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.

- 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

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

- \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

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

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 $\{1, \dots, n\}$, 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

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