

Chapter 1 Introduction to Groups

Contents

1	Basic Axioms and Examples	2
2	Dihedral Groups	3
3	Symmetric Groups	4
4	Matrix Groups	4
5	Quaternion Group	5
6	Homomorphisms and Isomorphisms	5
7	Group Actions	6

1 Basic Axioms and Examples

Definition. (Binary Operation)

1. **(binary operation)** \star on a set G is a function $\star : G \rightarrow G$. write $a \star b$ instead of $\star(a, b)$
 2. **(associative \star)** A binary operation on G is associative if for all $a, b, c \in G$ $a \star (b \star c) = (a \star b) \star c$
 3. **(commutative \star)** A binary operation on G is commutative if for all $a, b \in G$, $a \star b = b \star a$
 4. **(closed under \star)** \star is a binary operation on G and $H \subset G$, if $\star|_H$ is a binary operation on H , i.e. for all $a, b \in H$, $a \star b \in H$, then H is closed under \star . Associativity/Commutativity of \star is inherited on H
- (examples)
 1. $+$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a commutative binary operation
 2. \times on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a commutative binary operation
 3. $-$ is not commutative on \mathbb{Z} ($a - b \neq b - a$ usually)
 4. $-$ is not commutative on \mathbb{Z}^+ ($1, 2 \in \mathbb{Z}^+$, but $1 - 2 = -1 \notin \mathbb{Z}^+$)

Definition. (Group)

1. **(group)** A group is an ordered pair (G, \star) where G is a set and \star is a binary operation on G satisfying
 - (a) (associative) $\forall a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$
 - (b) (identity) $\exists e \in G \forall a \in G$ $a \star e = e \star a = a$ (e is an identity of G , alternatively denoted by 1)
 - (c) (inverse) $\forall a \in G \exists a^{-1} \in G$, $a \star a^{-1} = a^{-1} \star a = e$ (a^{-1} is an inverse of a)
2. **(abelian group)** A group is abelian/commutative if $a \star b = b \star a$ for all $a, b \in G$
3. **(finite group)** G is a finite group if G is a finite set
4. **(direct product)** If (A, \star) and (B, \circ) are groups, a new group $A \times B$ called direct product are defined as

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

with binary operation defined component-wise

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \circ b_2)$$

- (examples)
 - $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under $+$ ($e = 0$, $a^{-1} = -a$, associativity by axioms of $+$)
 - $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+$ are groups under \times ($e = 1$, $a^{-1} = 1/a$, associativity by \times)
 - $(\mathbb{Z} - \{0\}, \times)$ is not a group ($2^{-1} = 1/2 \notin \mathbb{Z} - \{0\}$)
 - $(V, +)$ is an abelian group, where V is a vector space (commutativity by axioms of a vector space)
 - $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group ($e = \bar{1}$, $a^{-1} = \overline{-a}$)
 - $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ is abelian group ($e = \bar{1}$, a^{-1} exists by definition of $(\mathbb{Z}/n\mathbb{Z})^\times$)
- **(theorem)** direct product of two groups is a group
- **(proposition)**
 1. (identity unique) identity of G is unique
 2. (inverse unique) inverse a^{-1} of any a in G is unique
 3. $(a^{-1})^{-1} = a$ for all a in G
 4. $(a \star b)^{-1} = b^{-1} \star a^{-1}$
 5. (generalized associativity law) value of $a_1 \star a_2 \star \dots \star a_n$ independent of how its bracketed
- (notation)

- (\times) denote $x^n = xx \cdots x$ by x^n and $x^{-n} = x^{-1}x^{-1} \cdots x^{-1}$ and $x^0 = 1$ the identity
- $(+)$ denote $na = a + a + \cdots + a$ and $-na = -a - a - \cdots - a$ and $0a = 0$ the identity

• **(proposition)** Let $a, b, u, v \in G$

1. (left cancellation law holds) if $au = av$, then $u = v$
2. (right cancellation law holds) if $ub = vb$, then $u = v$

Definition. (order for an element $x \in G$) is the smallest positive integer $n \in \mathbb{Z}^+$ such that $x^n = 1$, denoted by $|x|$. If no positive power of x is the identity, the order of x is defined to be infinity

- (examples)
 - if $|x| = 1$, then $x = 1$ the identity
 - In $(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, +)$, every nonzero elements has infinite order
 - In $(\mathbb{R} - \{0\}, \mathbb{Q} - \{0\}, \times)$, $|-1| = 2$ and all other nonidentity elements have infinite order
 - In $\mathbb{Z}/9\mathbb{Z}$, $|\bar{5}| = 9$ since 9 is the smallest integer multiple of 5 that is congruent to 0 (mod 9)
 - In $(\mathbb{Z}/7\mathbb{Z})^\times$, $|\bar{3}| = 6$ since 3^6 is smallest positive power of 3 that is congruent to 1 (mod 7)

Definition. (multiplication/group table) Let $G = \{g_1, g_2, \dots, g_n\}$ be a finite group where $g_1 = 1$. The multiplication or group table of G is a $n \times n$ matrix A where $A_{ij} = g_i g_j$.

- (fact) For finite groups, the group table contains all information about the group

2 Dihedral Groups

Definition. (Dihedral Groups)

1. **(symmetry of n -gon)** is any rigid motion of the n -gon. We can describe symmetry by choosing a labelling of vertices $\{1, 2, \dots, n\}$ and let the corresponding permutation σ over the set as symmetry s
2. **(order of D_{2n})** is $2n$. (lower bound: vertex 1 can be sent to any vertex i , and vertex 2 can be sent to either $i - 1$ or $i + 1$. Knowing position of 1, 2 determines position of all other vertices; upper bound: by reasoning that any element of D_{2n} can be written as $r^i s^j$ where $0 \leq i \leq n - 1$ and $0 \leq j \leq 1$)
3. **(dihedral group D_{2n})** Fix a regular n -gon at origin and label vertices through from 1 to n in a clockwise manner. Let r be rotation clockwise about the origin through $2\pi/n$ radian and let s be reflection about line of symmetry through vertex 1 and the origin.

$$D_{2n} = \{r, s \mid r^n = s^2 = 1, sr^k = r^{-k}s\} = \{1, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}$$

(a) $|r| = n$ and $|s| = 2$

(b) $s \neq r^i$ for any i and $sr^i \neq sr^j$ for all $i \neq j$

(c) $r^k s = sr^{-k}$ for all $0 \leq i \leq n$

4. **(interpreting presentation for D_{2n})** $r^n = 1$ means any power of r can be reduced so that the power lie between 0 and $n - 1$. Similarly, any power of s can be reduced so that the power is either 0 or 1. $sr^k = r^{-k}s$ means every element in the group can be written as $r^i s^j$ for some i, j

- (fact) D_{2n} for $n \geq 3$ is non-abelian

Definition. (generators and relations)

1. **(generators of G)** is the set $S \subset G$ where every element of G can be written as a (finite) product of elements of S and their inverses. Denote $G = \langle S \rangle$ and say G is generated by S and S generates G
2. **(relations in G)** any equation in a general group G that the generator satisfies
3. **(presentation of G)** If $G = \langle S \rangle$ and R_1, R_2, \dots, R_m are relations in G such that any relation among S can be deduced from these, the generators and relations are called presentations

$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle$$

- (example) $\mathbb{Z} = \langle 1 \rangle$
- (example) $D_{2n} = \langle r, s \rangle$

3 Symmetric Groups

Definition. (Symmetric Group)

1. (**symmetric group** S_Ω on set Ω) Let Ω be nonempty set, $S_\Omega = \{\sigma : \Omega \rightarrow \Omega \mid \sigma \text{ is a bijection}\}$, the set of all permutations of Ω . (S_Ω, \circ) is the symmetric group on Ω .
2. (**symmetric group of degree n**) If $\Omega = \{1, 2, \dots, n\}$, S_n is the symmetric group of degree n
3. ($|S_n| = n!$) (by counting number of possible permutations using the constraint that σ is injective)
4. (**cycle**) a string of integers representing elements of S_n , which cyclically permutes them. $(a_1 \ a_2 \ \dots \ a_m)$ is the permutation sending a_i to a_{i+1} . $1 \leq i \leq m-1$ and sends a_m to a_1
5. (**length of cycle**) is the number of integers which appear in it
6. (**t -cycle**) is a cycle with length t
7. (**disjoint cycle**) A cycle is disjoint if they have no numbers in common
8. (**k cycles**) Any $\sigma \in S_n$, we can represent σ with k cycles of the form

$$(a_1 \ a_2 \ \dots \ a_{m_1})(a_{m_1+1} \ a_{m_1+2} \ \dots \ a_{m_2}) \cdots (a_{m_{k-1}+1} \ a_{m_{k-1}+2} \ \dots \ a_{m_k})$$

9. (**cycle-decomposition of σ**) is the product of k -cycles that representing σ
 - (convention) 1-cycle not written during cycle-decomposition. This convention ensures that cycle decomposition of $\tau \in S_n$ is exactly the same as cycle decomposition of permutation in S_m where $m > n$, which acts as τ on $\{1, 2, \dots, n\}$ and fixes elements in $\{n+1, n+2, \dots, m\}$
 - (computing inverse) Let $\sigma \in S_n$, cycle decomposition of σ^{-1} can be obtained by writing numbers in each cycle of the cycle decomposition of σ in reverse order
 - (computing product) by following elements in successive permutations
 - (example) S_n is non-abelian for $n \geq 3$ (counterexample: $(12) \circ (13) = (1 \ 3 \ 2)$ but $(13) \circ (12) = (1 \ 2 \ 3)$)
 - (**proposition**) disjoint cycle commutes
 - (**proposition**) cycle-decomposition uniquely expresses a permutation as a product of disjoint cycles
 - (**proposition**) The order of a permutation is the l.c.m. of the lengths of cycles in its cycle decomposition

4 Matrix Groups

Definition. (Field and Matrix Group)

1. (**field**) A field is a set F with two binary operations $+$ and \cdot such that $(F, +)$ is an abelian group and $(F - \{0\}, \cdot)$ is also an abelian group, and follows distributive law

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Denote $F^\times = F - \{0\}$.

2. (**general linear group**) For each $n \in \mathbb{Z}^+$, let $GL_n(F)$ be the set of all $n \times n$ matrices whose entries come from F and whose determinant is nonzero

$$GL_n(F) = \{A \mid A \text{ is } n \times n \text{ matrix with entries from } F \text{ and } \det A \neq 0\}$$

with matrix multiplication as the binary operation. $GL_n(F)$ is a group under matrix multiplication, called **general linear group of degree n** : since its closed under matrix multiplication, and satisfies inverse/identity axioms

- (example) \mathbb{Q}, \mathbb{R} , and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is prime are fields
- (fact) $GL_n(F)$ for $n \geq 2$ is nonabelian (matrix multiplication does not commute)
- (**theorem**) If F is a field and $|F| < \infty$, then $|F| = p^m$ for some prime p and integer m
- (**theorem**) If $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$

5 Quaternion Group

Definition. (quaternion group) The quaternion group Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product \cdot defined as

$$\begin{aligned} 1 \cdot a &= a \cdot 1 = a \quad \forall a \in Q_8 \\ (-1) \cdot (-1) &= 1 \\ (-1) \cdot a &= a \cdot (-1) = -a \quad \forall a \in Q_8 \\ i \cdot i &= j \cdot j = k \cdot k = -1 \\ i \cdot j &= k \quad j \cdot k = i \quad k \cdot i = j \\ j \cdot i &= -k \quad k \cdot j = -i \quad i \cdot k = -j \end{aligned}$$

- (fact) Q_8 is non-abelian
- (fact) order of elements in Q_8

element	order
1	1
-1	2
i, -i, j, -j, k, -k	4

6 Homomorphisms and Isomorphisms

Definition. (homomorphisms) Let (G, \star) and (H, \diamond) be groups. A map $\varphi : G \rightarrow H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y) \quad \forall x, y \in G$$

is called a **homomorphism**. Intuitively, φ respects the group structures of its domain and codomain

- (theorem) If $\phi : G \rightarrow h$ is a homomorphism, then

1. $\varphi(e_G) = e_H$
2. $\varphi(x^{-1}) = \varphi(x)^{-1}$
3. $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$

Definition. (Isomorphisms)

1. (isomorphisms) The map $\varphi : G \rightarrow H$ is called an **isomorphism** and G and H are said to be **isomorphic** or of the same **isomorphic type**, write $G \cong H$, if

- (a) φ is a homomorphism
- (b) φ is a bijection

G and H are the same group, except that elements/operations are written differently.

2. (isomorphism classes) Let \mathcal{G} be nonempty collection of groups. Then \cong is an equivalence relation on \mathcal{G} . the equivalence classes are called isomorphism classes
3. (classification theorems) determine what properties of a structure specify its isomorphic types, i.e.

any non-abelian group of order 6 is isomorphic to S_3

from which we know $D_6 \cong S_3$ and $GL_2(\mathbb{F}_2) \cong S_3$

- (theorem) G and H share properties which rely on group structures (i.e. commutativity)
- (theorem) Isomorphic type of a symmetric group depends on cardinality only $S_\Delta \cong S_\Omega \iff |\Delta| = |\Omega|$

• **(theorem)** If $\varphi : G \rightarrow H$ is an isomorphism, then

1. $|G| = |H|$
2. G is abelian iff H is abelian
3. for all $x \in G$, $|x| = |\varphi(x)|$

• **(examples)**

- $G \cong G$ by the identity map or conjugation $g \mapsto xgx^{-1}$ for some $x \in G$
- $(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$ by the exponential map $\exp : \mathbb{R} \rightarrow \mathbb{R}^+; x \mapsto e^x$
- $S_3 \cong D_6$ by the example classification theorem
- $GL_n(F) \cong F^\times$ by $\det : GL_n(F) \rightarrow F^\times$, i.e. $\det AB = \det A \det B$
- $S_3 \not\cong \mathbb{Z}/6\mathbb{Z}$ (S_3 is non-abelian; $\mathbb{Z}/6\mathbb{Z}$ is abelian)
- $(\mathbb{R}, +) \not\cong (\mathbb{R}^\times, \times)$ ($-1 \in \mathbb{R}$ has order 2; \mathbb{R}^\times has no element of order 2)

Definition. (homomorphism/isomorphism and presentations) Let G be a finit group of order n with a presentation. Let $S = \{s_1, \dots, s_m\}$ be the generators let H be another group and $R = \{r_1, \dots, r_m\}$ be elements of H . If any relation satisfied in G by s_i is also satisfied in H when each s_i is replaced with r_i . Then there exists unique homomorphism $\varphi : G \rightarrow H; s_i \mapsto r_i$

1. if H is generated by $\{r_1, \dots, r_m\}$, then φ is surjective (any $r_{i_1}r_{i_2}\dots \in H$ is $\varphi(s_{i_1}s_{i_2}\dots)$)
2. if in addition, $|H| = |G|$, then surjective φ is necessarily injective, φ is a bijection and $G \cong H$

(examples)

- Let $D_{2n} = \{r, s \mid r^n = s^2 = 1 \text{ } sr = r^{-1}s\}$. Let $D_{2k} = \{r_1, s_1 \mid r_1^n = s_1^2 = 1 \text{ } s_1r_1 = r_1^{-1}s_1\}$ where $k \mid n$, specifically $n = km$. Then

$$\varphi : D_{2n} \rightarrow D_{2k} \quad \text{by} \quad \varphi(r) = r_1 \quad \varphi(s) = s_1$$

is a homomorphism by the previous theorem as r_1, s_1 satisfies the relation of D_{2n} , specifically

$$r_1^n = (r_1^k)^m = 1^m = 1$$

Since r_1, s_1 generates D_{2k} , φ is surjective. However for any $k < n$, $|D_{2n}| \neq |D_{2k}|$ so $D_{2n} \not\cong D_{2k}$

- $D_6 \cong S_3$

Proof. Let $G = D_6$ and $H = S_3$. $a = (1 \ 2 \ 3), b = (1 \ 2) \in H$ satisfies $a^3 = b^2 = 1$ and $ba = ab^{-1}$. Hence exists unique homomorphism φ by $\varphi(r) \mapsto a$ and $\varphi(s) \mapsto b$. Note a, b generates S_3 . Therefore φ surjective. Since $|D_6| = |S_3|$, φ is an isomorphism \square

Definition. (automorphisms) Let G be a group and define

$$\text{Aut}(G) = \{\varphi : G \rightarrow G \mid \varphi \text{ is an isomorphism}\}$$

Then $(\text{Aut}(G), \circ)$ is a group under function composition, called **automorphism group of G** . Any element of $\text{Aut}(G)$ is an **automorphism** of G

7 Group Actions

Definition. (Group Action)

1. **(group action)** A group action of a group G on a set A is a map satisfying

$$\begin{aligned} G \curvearrowright A : G \times A &\rightarrow A \\ (g, a) &\mapsto g \cdot a \end{aligned}$$

- (a) $g_1 \cdot (g_2 \cdot a) = (g_1g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$
- (b) $1 \cdot a = a$ for all $a \in A$

2. (**permutation representation**) For each fixed $g \in G$, define a map σ_g by

$$\begin{aligned}\sigma_g : A &\rightarrow A \\ a &\mapsto g \cdot a\end{aligned}$$

is a permutation, i.e. $\sigma_g \in S_A$. The permutation representation of $G \curvearrowright A$

$$\begin{aligned}\varphi : G &\rightarrow S_A \\ g &\mapsto \sigma_g\end{aligned}$$

is a homomorphism. Intuitively, a group action of G on a set A means every element $g \in G$ acts as a permutation on A in a manner consistent with the group operation in G .

3. (**faithful**) If G acts on B , then the action is faithful if

- distinct elements of G induce distinct permutations of B
- permutation representation is injective

4. (**kernel**) The kernel of action of G on B is defined by to

$$\{g \in G \mid gb = b \text{ for all } b \in B\}$$

i.e. elements of G that fix all elements of B

5. (**trivial action**) $g \cdot a = a$ is the trivial action and the permutation representation φ is the trivial homomorphism. $\ker \varphi = G$ and action not faithful when $|G| > 1$

6. (**left regular action**) $G \curvearrowright G$ by left multiplication (translation) $g \cdot a = ga$ ($g \cdot a = g + a$) for all $g, a \in G$. Then this action is called left regular action and is faithful by cancellation laws.

- (**theorem**) The actions of a group G on a set A and the homomorphisms from G into S_A are in bijective correspondence, i.e. the same thing.

Proof. (\rightarrow) from construction of permutation representation (\leftarrow) Let $\varphi : G \rightarrow S_A$ be any homomorphism, then the map

$$\begin{aligned}g : G \times A &\rightarrow A \\ (g, a) &\mapsto g \cdot a = \varphi(g)(a)\end{aligned}$$

satisfies properties of a group action $G \curvearrowright A$

□

- (**examples**)

– $F^\times \curvearrowright V$ where F^\times is a field and V is a vector space. For example, action for $\mathbb{R} \curvearrowright \mathbb{R}^n$ specified by

$$\alpha \cdot (x_1, x_2, \dots, x_n) = (\alpha x_1, \alpha x_2, \dots, \alpha x_n)$$

– $S_A \curvearrowright A$ by $\sigma \cdot a = \sigma(a)$. The permutation representation $\varphi : S_A \rightarrow S_A$ is the identity map

– $D_{2n} \curvearrowright \{1, 2, \dots, n\}$ where $\{1, 2, \dots, n\}$ is a labelling of vertices of a regular n -gon. The action is faithful or the associated permutation representation $\varphi : D_{2n} \rightarrow S_3$ is injective since distinct symmetries of a regular n -gon induce distinct permutations of the vertices. Since $|D_{2n}| = |S_3|$, φ is surjective and so φ is an isomorphism and $D_6 \cong S_3$. Geometrically, this means any permutation of vertices of a triangle is a symmetry; however this is not true for any n -gon with $n \geq 4$