

Chapter 1 Why Abstract Algebra?

Italian Renaissance, 16th century algebra

Problem-solving Competitions

Giralamo Cardano (1501), Book Ars Magna (The Great Art)

Tartaglia (~ 1500) = solving any cubic equation $x^3 + ax^2 + bx = c$

Ludovico Ferrari = solving any quadratic equations $x^4 + ax^3 + bx^2 + cx = d$

1824, Niels Abel (Norwegian) = \nexists formulas for roots for degree ≥ 5

Similar times = Matrix Algebra

Boolean Algebra

Axiomatics / Abstraction = varying the possible choices of axioms

1845, Évariste Galois = explains exactly which equations of degree ≥ 5 (published) (1832 died) have solutions (traditional kind), which do not

~ 1930, Early 20th Centuries = Algebraic Structure (completed)

Chapter 2 Operations

Valid operations on a set A.

- ① $a * b$ is defined for every ordered pair $(a, b) \in A$
- ② $a * b$ uniquely defined
- ③ $a * b \in A$

Exercises

B. Properties of Operations

$$7. x * y = \frac{xy}{x+y+1}$$

(a) Commutative?

$$y * x = \frac{yx}{y+z+1} = x * y \rightarrow \text{is commutative}$$

(b) associative?

$$\begin{aligned} x * (y * z) &= \frac{x \left(\frac{yz}{y+z+1} \right)}{x + \left(\frac{yz}{y+z+1} \right) + 1} = \frac{xyz}{y+z+1} \cdot \frac{y+z+1}{x(y+z+1) + yz + (y+z+1)} \\ &= \frac{xyz}{(x+1)(y+z+1) + yz} = \frac{xyz}{xy + xz + yz + x + y + z} \end{aligned}$$

$$\begin{aligned} (x * y) * z &= \frac{\left(\frac{xy}{x+y+1} \right) * z}{\left(\frac{xy}{x+y+1} \right) + z + 1} = \frac{xyz}{x+y+1} \cdot \frac{x+y+1}{xy + z(x+y+1) + (x+y+1)} \\ &= \frac{xyz}{(z+1)(x+y+1) + xy} = \frac{xyz}{xy + xz + yz + x + y + z} \end{aligned} \quad \text{is associative}$$

(c) has an identity? (on \mathbb{R}^+)

$$x * e = \frac{xe}{x+e+1} = x$$

$$xe = x(x+e+1)$$

$$x = 0 \text{ or } -1 \notin \mathbb{R}^+ \rightarrow \text{no identity on } \mathbb{R}^+$$

(d) has inverse for every x ? (on \mathbb{R}^+)no identity \rightarrow no inverse(otherwise = solve x' for $x * x' = e$)

Chapter 3 The Definitions of Groups

(G1) $*$ is associative

(G2) \exists identity $e \in G$ s.t. $x * e = e * x \forall x \in G$

(G3) \exists inverse $x^{-1} \forall x \in G$ s.t. $x * x^{-1} = x^{-1} * x = e$

Exercises

A. Examples of Abelian Group

$$4. x * y = \frac{x+y}{xy+1} \text{ on } \{x \in \mathbb{R} : -1 < x < 1\}$$

[(a) associative?]

$$x + \left(\frac{y+z}{y+z+1} \right) = \frac{xy + xz + y + z}{xy + xz + y + z + 1}$$

$$\frac{\frac{y+z}{x(y+z+1)} + 1}{\frac{x+y}{xy+1} + 1} = \frac{y+z}{y+z+1} \cdot \frac{y+z+1}{xy+xz+yz+1} = \frac{xyz+(x+y+z)}{xy+xz+yz+1}$$

$$\frac{\frac{xy}{(xy+1)z} + z}{\frac{x+y}{xy+1} z + 1} = \frac{x+y+z+xyz}{xy+1} \cdot \frac{xy+1}{xz+yz+xy+1} = \text{same} \quad \rightarrow \text{is associative}$$

is
a
Group

(b) \exists identity?

$$\frac{x+e}{xe+1} = x \Rightarrow x+e = x(xe+1)$$

$$x+e = ex^2 + x \quad e=0$$

$$e(1-x^2) = 0$$

$$e=0 \text{ or when } x=\pm 1$$

(c) \exists inverse $\forall x$?

$$x * x^{-1} = 0 \Rightarrow \frac{x+e}{xe+1} = 0$$

$$x+e = 0$$

$$e = -x$$

$$\frac{x+(-x)}{x+(-x)+1} = \frac{0}{1} = 0 \Rightarrow \exists \text{ inverse}$$

(d) Abelian Group?

$$\frac{x+y}{xy+1} = \frac{y+x}{yx+1} \rightarrow \text{commutative} \Rightarrow \begin{array}{l} \text{is} \\ \text{Abelian} \\ \text{Group.} \end{array}$$

B Groups on the Set $\mathbb{R} \times \mathbb{R}$

$$2. (a,b) * (c,d) = (ac, bc+d) \text{ on } \{(x,y) \in \mathbb{R} \times \mathbb{R} : x \neq 0\}$$

(a) associative?

y can be 0

$$(a,b) * ((c,d) * (e,f)) = (a,b) * (ce, de+df)$$

$$= (ace, bce+de+df)$$

$$\begin{aligned} ((a,b) * (c,d)) * (e,f) &= (ac, bc+cd) * (e,f) \\ &= (ace, (bc+cd)e+df) \\ &= (ace, bce+de+df) \end{aligned} \quad \begin{array}{l} \text{is} \\ \text{associative} \end{array}$$

is a

Group

(b) \exists identity?

(b) \exists identity e :

$$(a, b) * (e_1, e_2) = (a, b)$$

$$(ae_1, be_1 + e_2) = (a, b)$$

$$\begin{aligned} \Rightarrow ae_1 &= a \Rightarrow e_1 = 1 \\ be_1 + e_2 &= b \Rightarrow e_2 = 0 \end{aligned}$$

(c) \exists inverse $\forall x$?

$$(a, b) * (a^{-1}, b^{-1}) = (1, 0)$$

$$(aa^{-1}, ba^{-1} + b^{-1}) = (1, 0)$$

$$\begin{aligned} \Rightarrow aa^{-1} &= 1 \Rightarrow a^{-1} = \frac{1}{a} \\ ba^{-1} + b^{-1} &= 0 \Rightarrow b^{-1} = -\frac{b}{a} \end{aligned}$$

$$\text{Confirm: } (a, b) * \left(\frac{1}{a}, -\frac{b}{a}\right)$$

$$= \left(1, \frac{b}{a} - \frac{b}{a}\right) = (1, 0) \rightarrow \exists \text{ inverse}$$

(d) Is Abelian Group?

$$(a, b) * (c, d) = (ac, bcd)$$

$$(c, d) * (a, b) = (ca, dadb)$$

not commutative
 \rightarrow not Abelian Group

Chapter 4 Elementary Properties of Groups

Exercises

A. Solving Equations in Groups

Let $G = \{a, b, c, x\}$. Solve x in terms of a, b and c .

$$3. x^2a = bx^{-1} \text{ and } acx = xac.$$

$$x^2ac = bx^{-1}$$

$$x(acx) = bx$$

$$xac = b$$

$$x = bc^{-1}a^{-1}$$

B. Rules of Algebra in Groups

1. If $x^2 = e$ then $x = e$ *Wrong*

2. If $x^2 = a^2$ then $x = a$ *Wrong*

	I	A	B	C	D	K
I	I	A	B	C	D	K
A	A	I	C	D	K	P
B	C	D	I	A	B	
C	D	K	A	I	B	
D	K	P	B	A	I	
K	P		C	D	B	I
P			D	K	C	A

$$3. (ab)^2 = a^2 b^2 \quad \text{Wrang}$$

$$(AB)^2 = C^2 = I$$

$$A^2 B^2 = ID = D$$

	A	I	C	B	K	D	A	I	C
B	B	K	D	A	I	C			
C	C	D	K	I	A	B			
D	D	C	I	K	B	A			
K	K	B	A	D	C	I			

$$4. \text{ If } x^2 = x \text{ then } x = e \quad \text{Correct}$$

$$5. \forall x \in G, \exists y \in G \text{ s.t. } x = y^2 \quad \text{Wrang}$$

e.g. $\nexists y \in G$ s.t. $C = y^2$ (diagonal checking)

$$6. \forall x, y \in G, \exists z \in G \text{ s.t. } y = xz \quad \text{Correct (row checking)}$$

Chapter 5 Subgroups

- (SG 1) : closed w.r.t. multiplication (or the operation in original group)
- (SG 2) : closed w.r.t. inverses

$F(\mathbb{R})$ = set of all functions from \mathbb{R} to \mathbb{R}

$\langle F(\mathbb{R}), + \rangle$ = a group

Subgroups:

$C(\mathbb{R})$ = all continuous functions from \mathbb{R} to \mathbb{R}

$D(\mathbb{R})$ = all differentiable functions from \mathbb{R} to \mathbb{R}

Subgroup of G generated by a, b , and c :

the subset of G contains all the possible products of a, b, c and their inverses, e.g. $abc^{-1}, c^{-1}a^{-1}bbc$

this group is

generated by

$\{A, B\}$ only

	I	A	B	C	D	K
I	I	A	B	C	D	K
A	A	I	C	B	K	D
B	B	K	D	A	I	C
C	C	D	K	I	A	B
D	D	C	I	K	B	A
K	K	B	A	D	C	I

Cyclic subgroup of G , $\langle a \rangle$ with generator a

all possible products of a and a^{-1} , e.g. a, aa, aaa, \dots

Addition group \mathbb{Z}_6 is cyclic
i.e. $\mathbb{Z}_6 = \langle 1 \rangle$

$\mathbb{Z}_n =$

group of integers modulo n

operation addition modulo n

\mathbb{Z}_6	$+$	0	1	2	3	4	5
0	0	1	2	3	4	5	0
1	1	2	3	4	5	0	1
2	2	3	4	5	0	1	2
3	3	4	5	0	1	2	3
4	4	5	0	1	2	3	4
5	5	0	1	2	3	4	5

Defining equations completely define the multiplication table

Exercises

B

Subgroup of Functions

5. $G = \langle \mathcal{D}(\mathbb{R}), + \rangle$, $H = \{f \in \mathcal{D}(\mathbb{R}) : \frac{df}{dx} \text{ is a constant}\}$

- is a Subgroup
- (a) closed w.r.t. + ?
 - $\forall f \in H, \frac{df}{dx}$ is constant $\rightarrow f(x) = ax + b$ for some $a, b \in \mathbb{R}$
 - $\forall f, g \in H, f + g = (a_1 + a_2)x + (b_1 + b_2)$ so $\frac{d(f+g)}{dx}$ is constant \rightarrow closed w.r.t. +
 - (b) closed w.r.t. inverses ?
 - 0 is the identity function in $(\mathcal{D}(\mathbb{R}), +)$
 - $-f(x) = -ax - b \rightarrow \frac{df}{dx}$ is a constant \rightarrow closed w.r.t. inverses

C

Subgroups of Abelian Groups

Let G = abelian group

5. Let H = subgroup of G .

$K = \{x \in G : x^n \in H \text{ for some } n > 0\}$

Prove K is a subgroup of G .

is a Subgroup when G is abelian

(a) closed w.r.t. multiplication ?

Let $x^n \in H, y^m \in H \rightarrow x^n y^m \in H$ since H is a subgroup

$\rightarrow (x^n y^m)^k = x^{nk} y^{mk} \in H$ since $(x^n)^k \in H, (y^m)^k \in H$ and H abelian

$\rightarrow K$ is closed w.r.t. multiplication

(b) closed w.r.t. inverses ?

$\exists k \in \mathbb{N} \text{ s.t. } x^{-k} \in H$

$\rightarrow y \in H$ s.t. $x^{-1}(y^k) = e$ since H is a subgroup

$\rightarrow K$ is closed w.r.t. inverses

E Generators of Groups

7. $\mathbb{Z}_2 \times \mathbb{Z}_4$ is NOT cyclic (not generated by $\langle 1, 1 \rangle$)

Direct Product of

Groups = $G_1 \times H$

$$= (x, y) \cdot (x', y')$$

$$= (xx', yy')$$

$$\forall x, x' \in G, y, y' \in H$$

(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(0,1)	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)
(0,2)	(0,1)	(0,0)	(0,1)	(0,2)	(1,1)	(1,2)	(1,3)
(0,3)	(0,2)	(0,1)	(0,0)	(0,1)	(1,2)	(1,3)	(1,0)
(1,0)	(1,1)	(1,2)	(1,3)	(1,0)	(0,1)	(0,2)	(0,3)
(1,1)	(1,0)	(1,1)	(1,2)	(1,3)	(0,0)	(0,1)	(0,2)
(1,2)	(1,1)	(1,0)	(1,1)	(1,2)	(0,1)	(0,0)	(0,1)
(1,3)	(1,2)	(1,3)	(1,0)	(1,1)	(0,0)	(0,2)	(0,3)

F Groups Determined by Generators and Defining Equations

1. Let $G = \{e, a, b, b^2, ab, ab^2\}$

whose generators satisfying $\begin{cases} a^2 = e \\ b^3 = e \\ ba = ab^2 \end{cases}$ Write the table for G .

	e	a	b	b^2	ab	ab^2
e	e	c	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	ab^2	a	ab	b^2	e

$$\begin{aligned}
 a^2b &= eb = b & aba &= aab^2 = a^2b^2 = b^2 \\
 a^2b^2 &= eb^2 = b^2 & abb &= ab^2 \\
 bab &= ab^2b = ab^3 = a & abb^2 &= ab^3 = a \\
 ba.b^2 &= ab^2b^2 = ab^3b = ab & abab &= a(ab^2)b \\
 b^2a &= bba = ab^2 = ab^4b^2 = ab & = a^2b^3 = e \\
 b^4b^2 &= eb = b & abab^2 &= a(ab^2)b^2 \\
 b^3ab &= b(ab^2)b = bab^3 = ba = ab^2 & = b \\
 b^2ab^2 &= b(ab^2)b^2 = ab^2b = ab^3 = a & ab^2a &= ab(ab^2)a = ab^2 \\
 ab^2a &> ab(ab^2)a = ab^2 & ab^2b &= ab^3 = a \\
 ab^2ab &= aab^2 = b^2 & ab^2b^2 &= ab^3 = a \\
 ab^2ab &= abab^2 = b^2 & ab^2ab^2 &= ab(ab^2)b^2 \\
 ab^2ab &= abab^2 = b^2 & = abab^4 = abab = e
 \end{aligned}$$

G Cayley Diagrams

1. Define the group

e	a	ac	c
e	a	ac	c
a	e	c	ac
ac	a	c	e

Chapter 6

Functions

Let $f: D \rightarrow T$

injective \Rightarrow prove if $f(a) = f(b)$, then $a = b \quad \forall a, b \in D$

surjective \Rightarrow prove $\forall x \in T, \exists y \in D$ s.t. $f(y) = x$

bijection \Rightarrow prove injective + surjective

Chapter 7 Groups of Permutations

Permutation of set A = a bijective function from A to A .

Symmetric Group S_A on set A

S_n : The set of all the permutations of $A = \{1, 2, \dots, n\}$.
with the operation \circ of composition,

$$S_3 : \varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

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

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

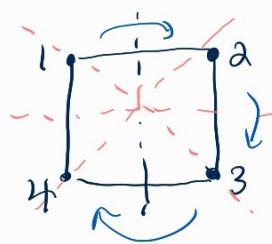
$3! = 6$ elements

\circ	ε	α	β	γ	δ	κ
ε	ε	α	β	γ	δ	κ
α	α	ε	γ	β	κ	γ
β	β	κ	γ	α	ε	γ
γ	γ	γ	κ	ε	α	β
δ	δ	δ	ε	κ	β	α
κ	κ	β	α	γ	γ	ε

Dihedral Group D_n :

The group of symmetries of regular polygons
with $n \geq 3$ sides

D_4 : group of symmetries of the square



$$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$R_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

$$R_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$R_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Chapter 8

Permutations of a Finite Set

$\xrightarrow{\text{(breakdown)}}$ Cycles $\xrightarrow{\text{(breakdown)}}$ Transpositions (cycle of length 2)

product of cycles $(245)(124)$ in S_5

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$$

Even permutations = permutation with even num of transpositions
Odd permutations = _____ odd _____

A_n = the Alternating group on the set $\{1, 2, \dots, n\}$

= The set of all even permutations in S_n

(is a subgroup of S_n)

ϵ the identity permutation is even)

Chapter 9 Isomorphism

Isomorphism between groups G_1 and G_2 :

A bijective function $f: G_1 \rightarrow G_2$ satisfying

$$\forall a, b \in G_1, f(ab) = f(a)f(b)$$

e.g. $\langle \mathbb{R}, + \rangle \cong^{\text{isomorphic}} \langle \mathbb{R}^{\text{pos}}, \cdot \rangle$ with function $f(x) = e^x$

$\begin{cases} \text{(i) } f \text{ is injective} = \text{ if } e^a = e^b \text{ then } a = b \\ \text{(ii) } f \text{ is surjective} = \forall x \in \mathbb{R}^{\text{pos}}, \exists y = \ln(x) \in \mathbb{R} \text{ st. } f(\ln x) = x \\ \text{(iii) } f(a+b) = e^{a+b} = e^a \cdot e^b = f(a) \cdot f(b) \end{cases}$

Cayley's Theorem = (Arthur Cayley)

every group is isomorphic to a group of permutations

Proof: Let G be a graph.

*Left
Representation
of group G*

*If G commutative
left representation
= right representation*

Let $G^* = \{\pi_a : a \in G\}$ where $\pi_a : G \rightarrow G$ is defined as

$$\pi_a(x) = ax. \quad \forall x \in G$$

* π_a is a permutation $\forall a \in G$.

$\begin{cases} \text{(i) } \pi_a \text{ is injective: if } ax_1 = ax_2, \text{ then } x_1 = x_2 \\ \text{(ii) } \pi_a \text{ is surjective: } \forall x \in G, \exists y = a^{-1}x \in G \text{ st. } \pi_a(y) = \pi_a(a^{-1}x) = a(a^{-1}x) = x \end{cases}$
 $\Rightarrow \pi_a$ is bijective
 $\text{mapping } G \rightarrow G \Rightarrow \text{a permutation}$

* G^* is a subgroup of S_G (the group of all permutations)

$\begin{cases} \text{(i) closed wrt. compositions:} \\ \pi_a \circ \pi_b = abx = \pi_{ab} \in G^* \end{cases}$

$\begin{cases} \text{(ii) closed wrt. inverses:} \\ \pi_e \text{ is the identity permutation: } \pi_e(x) = ex = x \end{cases}$

$\begin{cases} a^{-1} \text{ exists so } \pi_{a^{-1}} \text{ is the inverse of } \pi_a = \pi_{a^{-1}}(x) \pi_a(x) = x \\ \Rightarrow G^* \text{ is a subgroup of } S_G \end{cases}$

* Now G is isomorphic to G^* (the selected subgroup of permutations of G)

let $f : G \rightarrow G^*$ be defined as

$$f(a) = \pi_a$$

$\begin{cases} \text{(i) } f \text{ is injective: } \pi_a = \pi_b \Rightarrow a = b \end{cases}$

$\begin{cases} \text{(ii) } f \text{ is surjective: } \forall \pi_a \exists a \in G \end{cases}$

$\begin{cases} \text{(iii) } f(ab) = \pi_{ab} = abx = a(bx) = \pi_a \circ \pi_b = f(a) \cdot f(b) \end{cases}$

$\Rightarrow f$ is an isomorphism, so $G \cong G^*$

Exercises

C Isomorphism of Some Finite Groups

\circ	ϵ	α	β	γ	δ	κ
ϵ	ϵ	α	β	γ	δ	κ
α	α	ϵ	β	γ	δ	κ
β	β	κ	γ	α	ϵ	δ
γ	γ	δ	κ	ϵ	α	β
δ	δ	γ	ϵ	β	α	κ
κ	κ	β	α	γ	δ	ϵ

I	A	B	C	D	K
I	I	A	B	C	D
A	A	I	C	B	K
B	B	K	D	A	I
C	C	D	K	I	A
D	D	C	I	K	B
K	K	B	A	D	C

Isomorphic by $f = \begin{pmatrix} \epsilon & \alpha & \beta & \gamma & \delta & \kappa \\ I & A & B & C & D & K \end{pmatrix}$

I

Group Automorphisms

Automorphism = an isomorphism from G to G .

1. In \mathbb{Z}_6 ,

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$$

$$\left\{ \begin{array}{l} \text{(i) } f \text{ is injective} \\ \text{(ii) } f \text{ is surjective } x=2, y=5 \\ \text{(iii) } f(xy) = f((x+y) \bmod 6) \\ \qquad \qquad \qquad = \text{remainder of } (x+y) \bmod 6 \quad 5 \\ f(x)f(y) = (\text{remainder of } x \bmod 6 + \text{remainder of } y \bmod 6) \bmod 6 \\ \qquad \qquad \qquad = f(xy) \\ \Rightarrow \text{Isomorphism} \rightarrow \text{automorphism} \end{array} \right.$$

Chapter 10 Order of Group Elements

Order of the element a : the least positive integer n s.t.
 $a^n = e$ or if no such integers, the order is infinity

Exercises E Let $a, b \in G$, $\text{ord}(a)=m$, $\text{ord}(b)=n$.

If m, n relatively prime, then $a^i b^j$ ($0 \leq i < m$, $0 \leq j < n$) are all distinct.

Chapter 11 Cyclic Groups

Suppose $\langle a \rangle$ is a cyclic group whose generator has order n .

$$\langle a \rangle = \{a^0, a^1, a^2, \dots, a^{n-1}\} \quad \begin{matrix} \text{ord}(a)=n \Rightarrow |\langle a \rangle|=n \\ \text{order of generator} \quad \text{order of group} \end{matrix}$$

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\} \quad (\text{group of integers modulo } n)$$

$f(i) = a^i$ is an isomorphism from $\mathbb{Z}_n \rightarrow \langle a \rangle$

$$\text{so } \mathbb{Z}_n \cong \langle a \rangle$$

Every cyclic group of order n is isomorphic to \mathbb{Z}_n

Every cyclic group of order infinity is isomorphic to \mathbb{Z}

Every subgroup of a cyclic group is cyclic

Chapter 12 Partitions and Equivalence Relations

\sim : the equivalence relation determined by the partition $\{A_i : i \in I\}$

- (i) Reflexive: $x \sim x \quad \forall x \in A$
- (ii) Symmetric: if $x \sim y$, then $y \sim x$
- (iii) Transitive: if $x \sim y$ and $y \sim z$, then $x \sim z$

Equivalent class $[x] = \{y \in A : y \sim x\}$

If $x \sim y$, then $[x] = [y]$

The family of all equivalent classes $\{[x] : x \in A\}$ is a partition of A
 each partition of A determines / is determined by
 one equivalence relation on A .

Partition: a family $\{A_i : i \in I\}$ of nonempty subsets of A s.t.

(P1) if $x \in A_i$ and $x \in A_j$, then $A_i = A_j$

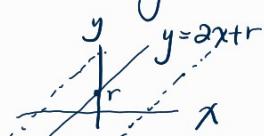
(P2) $\forall x \in A$, $x \in A_i$ for some $i \in I$

Exercises

C. Equivalence Relations and Partitions of $\mathbb{R} \times \mathbb{R}$

1. $\forall r \in \mathbb{R}$, $A_r = \{(x, y) : y = 2x + r\}$.

Geometrically each partition is a line with slope 2 and intercept r



$(x, y) \sim (u, v)$ if they lie on the same slope

(i) Suppose $(u, v) \in A_r$ and $(u, v) \in A_s$

$$\text{then } v = 2u + r = 2u + s \Rightarrow r = s$$

Hence $A_r = A_s$

(ii) $\forall x, y \in \mathbb{R}$, $y = 2x + r \Rightarrow r = y - 2x \in \mathbb{R}$

Hence (x, y) always lie in the class A_{y-2x}

D. Equivalence Relations on Groups

5. $a \sim b$ iff ab^{-1} commutes with every $x \in G$

$\left[\begin{array}{l} \text{(i) reflexive} \\ ab^{-1} \cdot x = x \cdot ab^{-1} \quad \forall x \Rightarrow a \sim a \end{array} \right]$
 $\left[\begin{array}{l} \text{(ii) symmetric} \\ \text{Since } a \sim b, ab^{-1}x = xab^{-1} \\ ab^{-1}xb = xab^{-1} \\ ab^{-1}xba^{-1} = x \\ b^{-1}xba^{-1} = a^{-1}x \end{array} \right]$

$$xba^{-1} = ba^{-1}x \rightarrow bva$$

(iii) transitive

$$\begin{aligned} a \sim b \text{ and } b \sim c, & ab^{-1}x = xab^{-1} \text{ and} \\ ab^{-1}(xbc^{-1})x = x(ab^{-1})bc^{-1} & bc^{-1}x = xbc^{-1} \\ xab^{-1}bc^{-1}x = x xab^{-1}bc^{-1} & \downarrow ? \\ xac^{-1}x = x xac^{-1} & ac^{-1}x = xac^{-1} \\ ac^{-1}x = xac^{-1} & \rightarrow a \sim c \end{aligned}$$

→ is an equivalent relation

$$\text{Equivalent class } [x] = \{y \in G : yx^{-1}z = zyx^{-1} \forall z \in G\}$$

Chapter 13 Counting Cosets

Let G be a group, H be a subgroup.

left coset aH *right coset* Ha

denotes the set of all products ha , as a fixed, h ranges over H

If $a \in Hb$, then $Ha = Hb$

$$\begin{cases} \text{since } a = h_1 b \text{ for some } h_1 \in H, \\ \forall x \in Ha, x = h_2 a = (h_2 h_1)b \in Hb \end{cases}$$

① Thm $\{Ha : a \in G\}$ is a partition of G

$$\begin{cases} \text{(i) suppose } x \in Ha \text{ and } x \in Hb \\ \text{then } x = h_1 a = h_2 b \text{ for some } h_1, h_2 \in H \\ \Rightarrow a = (h_1)^{-1}h_2 b \text{ and } (h_1)^{-1}h_2 \in H \\ \Rightarrow a \in Hb \Rightarrow Ha = Hb \end{cases}$$

(ii) Any $x \in G = x \in H_x$ because $x = ex$

→ is a partition

② Thm H and H_a has a one-one correspondence, for any coset Ha

Define $f: H \rightarrow Ha = f(h) = ha$

$$\begin{cases} \text{(i) injective: } f(h_1) = f(h_2) \Rightarrow h_1 = h_2 \\ \text{(ii) surjective: } \forall x \in Ha, f(h_x) = x \\ \Rightarrow \text{one-one correspondence} \end{cases}$$

③ Lagrange's Theorem

Let G be finite group, H any subgroup.

Then $|G|$ is a multiple of $|H|$ (the order of G
= multiple of order of H)

| Proof: since any coset H_a has the same order (# elements) as H , and the family of cosets $\{H_a\}$ is a partition of G .

④ Thm If a group G has prime number of elements, then G is a cyclic group; any element $\neq e$ is a generator

| Proof: the subgroup is unique (up to isomorphism)
since it must has a prime order equal to the order of G
by Lagrange Theorem. E.g. $\mathbb{Z}_7, \mathbb{Z}_{11}$

Index of H in G $G:H$ - the number of cosets of H in G

Exercises

B. Examples of Cosets in Infinite Groups

1. The subgroup $\langle 3 \rangle$ in \mathbb{Z} (with + as operator)

$$\langle 3 \rangle = \{-3^3, -3^2, -3^1, 1, 3, 3^2, 3^3, \dots\}$$

$$\text{Cosets} = \{\langle 3 \rangle + 1, \langle 3 \rangle + 2, \langle 3 \rangle + 0\}$$

E Elementary Properties of Cosets

Cauchy's Theorem

If G is a finite group, and p is a prime divisor of $|G|$, then G has an element of order p .

Survey of all possible groups whose order is ≤ 10

Prime-related:

Group with 2, 3, 5, 7 elements: $G \approx \mathbb{Z}_p$ (the unique cyclic group)

Group with 4, 9 elements: $G \approx \mathbb{Z}_{p^2}$ or $G \approx \mathbb{Z}_p \times \mathbb{Z}_p$

Groups with 6 elements

the group must have elements with order 2 and order 3. (Cauchy)

$\Rightarrow \{e, a, b, b^2, ab, ab^2\}$ must be distinct by Chapter 10 Exercise E.

\Rightarrow if $ba = ab$, then $G \cong \mathbb{Z}_6$,

if $ba = ab^2$, then $G \cong S_3$

\mathbb{Z}_6 and S_3 are the only possible groups (up to isomorphism)

Groups with 10 elements

the group must have elements with order 2 and 5 (Cauchy)

$\Rightarrow \{e, a, b, b^2, b^3, b^4, ab, ab^2, ab^3, ab^4\}$ must be distinct

\Rightarrow if $ba = ab$, then $G \cong \mathbb{Z}_{10}$,

$ba \neq ab^2, ba \neq ab^3$

if $ba = ab^4$, then $G \cong D_5$

\mathbb{Z}_{10} and D_5 are the only possible groups (up to isomorphism)

Groups with 8 elements

If G has an element of order 8 $\Rightarrow G \cong \mathbb{Z}_8$

Assume no:

if every $x \neq e$ in G has order 2

$\Rightarrow \{e, a, b, c, ab, ac, bc, abc\}$ are distinct $\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

if G has an element of order 4

\Rightarrow let $H = \{e, a, a^2, a^3\}$, let $b \in G$ but $b \notin H$ and $H_b = \{b, ab, a^2b, a^3b\}$.

By Lagrange's Theorem, $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$

\Rightarrow Assume there is an element in H_b that has order 2

\Rightarrow if $ba = ab \Rightarrow G \cong \mathbb{Z}_4 \times \mathbb{Z}_4$ $ba \neq a^2b$

if $ba = a^3b \Rightarrow G \cong D_4$

\Rightarrow Assume not, $\{b, ab, a^2b, a^3b\}$ all have order 4

$\Rightarrow a^4 = b^4 = e, a^2 = b^2, ba = a^3b$ completely determines G

Quaternion group $\mathbb{Q} \Rightarrow \mathbb{Z} \cong \mathbb{Q}$

\therefore The only groups (up to isomorphism) are $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2, D_4$, and \mathbb{Q} .

I Conjugate Elements

Conjugate of $a = \{x \in G : xax^{-1}\}$

1. "a is equal to a conjugate of b" is an equivalence relation

- (a) Reflexive
if $a = eae^{-1} \Rightarrow a$ is equal to a conjugate of a
 - (b) Symmetric
if $a = xbx^{-1} \Rightarrow b = x^{-1}ax = (x^{-1})a(x^{-1})^{-1}$
 $\Rightarrow b$ is equal to a conjugate of a
 - (c) Transitive
 $a = xbx^{-1}, b = xc x^{-1}$
 $a = x(xcx^{-1})x^{-1} = (x)^2 c (x^{-1})^2 \Rightarrow a$ is equal to a conjugate of c
- is a equivalence relation

Centralizer of a: $C_a = \{x \in G : xa = ax\}$ elements commutes with a
 $= \{x \in G : xax^{-1} = a\}$

5. There is a one-one correspondence between

the sets of all Conjugates of a

and the sets of all cosets of Centralizers of a

6. The size of every conjugate class is a factor of $|G|$

I. Group Acting on a Set

Let A be a set.

G be any subgroups of S_A

⇒ a subgroup of permutations of A ⇒ a group Acting on a set A

Orbit of $u \in A = O(u) = \{g(u) : g \in G\}$

define $u \sim v$ iff $g(u) = v$; \sim is equivalent relation

and orbits are equivalent classes

Stabilizer of $u \in A = G_u = \{g \in G : g(u) = u\}$

the set of all permutations in G which leave u fixed.

3. Let $\alpha = (12)(34)(56)$ in S_6 .
 $\beta = (23)$

Let $G = \{\epsilon, \alpha, \beta, \alpha\beta, \beta\alpha, \alpha\beta\alpha, \beta\alpha\beta, (\alpha\beta)^2\}$ be a subgroup of S_6

$$O(1) = \{g(1) : g \in G\} = \{\boxed{1}, 2, \boxed{1}, 2, 3, 4, 3, 4\} = \{1, 2, 3, 4\}$$

$$O(2) = \{g(2) : g \in G\} = \{\boxed{2}, 1, 3, 4, 1, \boxed{2}, 4, 3\} = \{1, 2, 3, 4\}$$

$$G(1) = \{g \in G : g(1) = 1\} = \{\epsilon, \beta\}$$

$$G(2) = \{g \in G : g(2) = 2\} = \{\epsilon, \alpha\beta\alpha\}$$

$$\alpha(2) = 1$$

$$\beta(1) = 1$$

$$\alpha(1) = 2$$

Chapter 14 Homomorphisms

Let G, H be groups.

Homomorphism from G to H :

A function $f: G \rightarrow H$ s.t. $\forall a, b \in G$,

$$f(a_1 b) = f(a_1) f(b)$$

$\Rightarrow H$ is a homomorphic image of G .

Example:

$$\begin{array}{c} \mathbb{Z}_6 + \\ \hline \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 3 & 4 & 5 & 0 \\ 2 & 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 4 & 5 & 0 & 1 & 2 & 3 \\ 5 & 5 & 0 & 1 & 2 & 3 & 4 \end{matrix} \end{array} \xrightarrow{\text{homomorphic image}} \begin{array}{c} f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix} \\ \downarrow \\ \mathbb{Z}_3 + \\ \hline \begin{matrix} 0 & 1 & 2 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{matrix} \end{array}$$

$$\mathbb{Z} \rightarrow P = \begin{array}{c} + \\ \hline \begin{matrix} e & 0 \\ e & e & 0 \\ 0 & 0 & e \end{matrix} \end{array} \quad \text{where } f \text{ carries all even integers to } e \\ \text{odd integers to } 0 \\ f(r+s) = f(r) + f(s)$$

① Thm G, H groups, $f: G \rightarrow H$ a homomorphism. Then

$$(i) f(e) = e$$

$$(ii) f(a^{-1}) = [f(a)]^{-1} \quad \forall a \in G.$$

Normal subgroup H of G :

If H is a subgroup of G and closed w.r.t. multiplication, inverses
 H is closed w.r.t. conjugates, i.e.

$$xax^{-1} \in H \quad \forall a \in H, \forall x \in G$$

Kernel of the homomorphism $f: G \rightarrow H$:

$$\ker(f) = K = \{ x \in G : f(x) = e_H \}$$

all elements of G carried by f onto the identity element of H .

② Thm Let $f: G \rightarrow H$ be a homomorphism.

(i) $\ker(f)$ is a Normal subgroup of G

(a) closed w.r.t. multiplications ?

$$\begin{aligned} a, b \in \ker(f) &\Rightarrow f(a) = e, f(b) = e \\ f(ab) &= f(a)f(b) \quad (\text{homomorphism}) \\ &= e \\ \therefore ab &\in \ker(f) \end{aligned}$$

(b) closed w.r.t. inverses ?

$$\begin{aligned} f(a^{-1}) &= [f(a)]^{-1} \quad (\text{homomorphism}) \\ &= e^{-1} \\ &= e \\ \therefore a^{-1} &\in \ker(f) \end{aligned}$$

(c) closed w.r.t. conjugates ?

$$\begin{aligned} f(xax^{-1}) &= f(x)f(a)f(x^{-1}) \quad (\text{homomorphism}) \\ &= f(x)e f(x^{-1}) \\ &= f(x)[f(x)]^{-1} \quad (\text{homomorphism}) \\ &= e \\ \therefore xax^{-1} &\in \ker(f) \text{ for any } x \in G \end{aligned}$$

is a
subgroupis a
Normal subgroup(ii) range of f is a subgroup of G ExercisesG1. Properties preserved under HomomorphismLet $f: G \rightarrow H$ be a homomorphism. Then

- If G is abelian, then H is abelian
- If G is a cyclic group, then H — “ —
- If every element of G has finite order, then H — “ —
- If every element of G has its own inverse, then H — “ —
- If every element of G has a square root, then H — “ —
- If G is finitely generated (finite number of generators), then H — “ —

Chapter 15 Quotient Groups

Thm If H is a normal subgroup of G ,
then $aH = Ha$ for every $a \in G$.

Proof: Let $x \in aH$.

$$x = ah_1 \text{ for some } h_1 \in H.$$

and $ah_1a^{-1} \in H$ since H is closed wrt. conjugate.

$$\text{Then } x = ah_1(a^{-1}a)$$

$$= (ah_1a^{-1})a \in Ha \quad \therefore aH = Ha \quad \forall a \in G$$

Thm Let H be a normal subgroup of G .

If $H_a = H_c$ and $H_b = H_d$,
 then $H(ab) = H(cd)$ where $H(ab) = H_a \cdot H_b$
 $H(cd) = H_c \cdot H_d$

| Proof: Since $a \in H_c$, $b \in H_d$,
 $ab = h_1 c \cdot h_2 d$
 $= h_1 (ch_2)d$
 $= h_1 (h_3 c)d \leftarrow$ since $ch_2 \in ch_3 H = H_c$
 $= (h_1 h_3)cd \in H(cd)$ when H is normal

Quotient Group of G by H

Let G a group, H a normal subgroup

$$G/H = \{H_a, H_b, H_c, \dots\} = \text{all cosets of } H$$

with Coset multiplication $H_a \circ H_b = H(a,b)$ is a Group

| Proof of G/H is a group:

(i) associative

$$\begin{aligned} H_a(bc) &= H_a \cdot (H_b \circ H_c) \\ &= h_1 a \cdot h_2 b \cdot h_3 c \\ &= (H_a \cdot H_b) \circ H_c = H_{(ab)c} \end{aligned}$$

(ii) \exists identity

$$H_e \text{ is the identity since } H_ae = H_a \circ H_e = H_e \circ H_a = H_a$$

(iii) \exists inverse

$$\forall H_a, H_{a^{-1}} \circ H_a = H_e$$

Thm G/H is a homomorphic image of G .

Consider $f: G \rightarrow G/H$ where $f(x) = H_x$ Natural homomorphism

$$f(xy) = H_{xy} = H_x \circ H_y = f(x)f(y) \text{ so } f \text{ is a homomorphism}$$

Quotient group construction = Manufacturing all homomorphic images