

Algebra I

Group Theory

Book 2

Transpositions (ij) are odd permutations.

$$(123456789) = (19)(18)(17)(16)(15)(14)(13)(12)$$

A k -cycle is a product of $k-1$ transpositions.

If k is even, this is odd; and vice versa.

A cycle of odd length is an even permutation;
 even odd

If α is a product of an even number of transpositions, then α is an even permutation.
 odd odd

Permutations in S_5 :

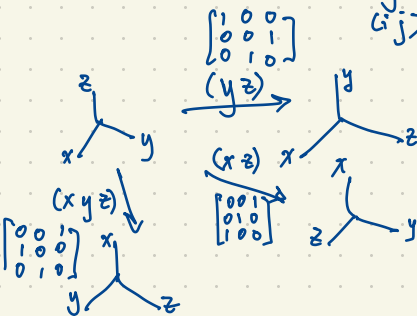
Even	
$()$	1
(ijk)	20
$(ijklm)$	24
$(ij)(kl)$	15
	<hr/>
	60

Odd	
(ij)	10
$(ijkl)$	30
$(ijk)(lm)$	20
	<hr/>
	60

$$|S_5| = 120$$

$$A_5 = \{ \text{even permutations in } S_5 \}$$

$$|A_5| = 60$$



An even permutation of the coordinate axis in \mathbb{R}^n is an orientation-preserving transformation.

An odd permutation of the coordinate axis in \mathbb{R}^n is an orientation-reversing transformation.

If $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ is a linear transformation then

$$\det T \begin{cases} = 0 & \text{if } T \text{ is not invertible} \\ > 0 & \text{preserves orientation} \\ < 0 & \text{reverses} \end{cases}$$

A permutation $\alpha \in S_n$ can be expressed as a product of transpositions.

If α is a product of an even number of transpositions, then α is even.

In S_3 :

$(13)(12)(13)(23)(23)(12)(23) = (123)$ says (123) is an even permutation.

$S_3 \cong \langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \rangle \cong$ dihedral group of order 6
(symmetry group of an equilateral triangle)

Groups of order 2

$S_2 \cong \{0, 1\} \pmod 2$ under addition $\cong \langle -1 \rangle$ under multiplication

n	no. of groups of order n up to isomorphism
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5

o	(1)	(12)	+	0	1	.	1	-1
(1)	(1)	(12)	0	0	1	1	1	-1
(12)	(12)	(1)	1	1	0	-1	-1	1



has a cyclic symmetry group of order 4



has an abelian symmetry group of order 4 which is not cyclic (the Klein four-group)

Cayley tables of groups of order 2 all "look the same"

Theorem Any two groups of prime order are isomorphic; they are cyclic of order p.

Eg. $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ (under addition mod 3) is isomorphic to $A_3 = \langle (123) \rangle = \{(), (123), (132)\}$ and $\{1, \omega, \omega^2\}$ under multiplication, $\omega = \frac{-1+i\sqrt{3}}{2} = e^{2\pi i/3}$

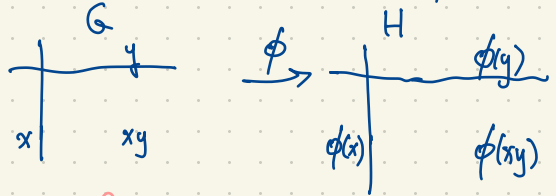
\oplus	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

\circ	$()$	(123)	(132)
$()$	$()$	(123)	(132)
(123)	(123)	(132)	$()$
(132)	(132)	$()$	(123)

\cdot	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω



We say two groups G, H are isomorphic ($G \cong H$) if there exists a bijection $\phi: G \rightarrow H$ such that $\phi(xy) = \phi(x)\phi(y)$



operation in G operation in H

An isomorphism $\phi: \mathbb{Z}/3\mathbb{Z} \rightarrow A_3$ is a bijection satisfying $\phi(x+y) = \phi(x)\phi(y)$

An isomorphism $\phi: \mathbb{R} \xrightarrow{\text{under addition}} (0, \infty) \xrightarrow{\text{under multiplication}}$ is defined by $\phi(x) = e^x$
 $e^{x+y} = e^x \cdot e^y$

(subgroup of $\mathbb{R}^* = (-\infty, 0) \cup (0, \infty)$)
 $\ln = \phi^{-1}: (0, \infty) \rightarrow \mathbb{R}$

$\mathbb{R} \not\cong \mathbb{R}^*$
 since \mathbb{R} (reals under addition) has only one element of finite order whereas \mathbb{R}^* has two elements of finite order: ± 1 .

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

is isomorphic to

*	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

$$\begin{aligned} \phi(0) &= c \\ \phi(1) &= a \\ \phi(2) &= b \end{aligned} \quad \begin{array}{c} * \\ \begin{array}{c|ccc} & c & a & b \\ \hline c & c & a & b \\ a & a & b & c \\ b & b & c & a \end{array} \end{array}$$

or

$$\begin{aligned} \phi(0) &= c \\ \phi(1) &= b \\ \phi(2) &= a \end{aligned} \quad \begin{array}{c} * \\ \begin{array}{c|ccc} & c & b & a \\ \hline c & c & b & a \\ b & b & a & c \\ a & a & c & b \end{array} \end{array}$$

$\mathbb{Z}/3\mathbb{Z}$

Every group of order 1 is isomorphic to $\mathbb{Z}/1\mathbb{Z}$
 2 $\mathbb{Z}/2\mathbb{Z}$

+	0	1
0	0	1
1	1	0

(trivial group $\{1\}$)

	c
a	ac
b	bc

If $ac=bc$ then multiply both sides by c^{-1} on the right
 to get $(ac)c^{-1} = (bc)c^{-1}$
 $a(cc^{-1}) = b(cc^{-1})$
 $a1 = b1$
 $a = b$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Every group of order 3 is cyclic (isomorphic to $\mathbb{Z}/3\mathbb{Z}$ under addition).

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Klein four-group

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Cyclic group of order 4

Two cases: either all ^{non-identity} elements of G have order 2, or G has an element not of order 2.

Theorem: There are exactly two groups of order 4 up to isomorphism: the Klein four-group and the cyclic group of order 4.

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

cyclic group of order 5

$$\langle a \rangle = \{e, a, a^2, a^3, a^4\}$$

$\begin{matrix} & \uparrow & \uparrow & \uparrow \\ & b & c & d \end{matrix}$

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	c	d	a	e
c	c	d	e	b	a
d	d	b	a	e	c

c is a left inverse for b ($cb=e$) but not a right inverse for b ($bc=a$).

is not a group!

It is a quasigroup, in fact since it has an identity e , it is a loop (its Cayley table is a Latin square: each row/column is a permutation of e, a, b, c, d).

This loop is not associative eg. $(ca)d = dd = c$
 $c(ad) = cb = e$

Theorem If every ^{non-identity} element of a group G has order 2, then G is abelian.

Proof (Note: $x^2=e$ = identity for every $x \in G$.)

Let $x, y \in G$. Then $(xy)^2 = xyxy = e$ so

$$yx = \underbrace{x(xyxy)}_{x^2=e} \underbrace{y}_{y^2=e} = xey = xy. \quad \square$$

\curvearrowright In such groups, $x^{-1} = x$ for all $x \in G$.

Shoe-Sock Theorem

In every group G ,
with identity 1 , for $x, y \in G$ we have $(xy)^{-1} = y^{-1}x^{-1}$.

Proof $(y^{-1}x^{-1})(xy) = y^{-1}1y = 1$ and $(xy)(y^{-1}x^{-1}) = 1$. \square

Warning: $(xy)^{-1} \neq x^{-1}y^{-1}$ in general.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Klein
four-group

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Cyclic group
of order 4

Write the rows of the Cayley table as permutations of $\overset{1}{e}, \overset{2}{a}, \overset{3}{b}, \overset{4}{c}$:
 $\{(1), (12)(34), (13)(24), (14)(23)\}$ is a Klein four group
as a subgroup of S_4 .

Gives $\{(1), (1234), (13)(24), (1432)\}$ as a subgroup
of S_4 .

Theorem (Cayley Representation Theorem)
Every finite group G is isomorphic to a subgroup of S_n
where $n = |G|$.

By the way, every finite group G is also isomorphic to
a group of matrices under multiplication.

Theorem If G is a finite group of order n , then every element $g \in G$ has order dividing n .
(If $g \in G$ then $|g| \mid n$.)

Eg. S_4 has elements of order 1, 2, 3, 4. These orders of elements divide $|S_4| = 24$.

S_5 has elements of order 1, 2, 3, 4, 5, 6 (divisors of $|S_5| = 120$).

Proof In the general case this follows from a later theorem, Lagrange's Theorem. Here let's prove the theorem in the special case that G is abelian. (We have already proved the result for cyclic groups.)

Consider the product of all the group elements $\pi = g_1 g_2 \dots g_n$ where $G = \{g_1, g_2, \dots, g_n\}$, $g_1 = 1$.

Note: since G is abelian, π is well-defined; it doesn't depend on what order we list the elements $g_1, \dots, g_n \in G$. Pick $a \in G$. (So $a \in \{g_1, \dots, g_n\}$.) The elements ag_1, ag_2, \dots, ag_n

are again all the elements of G so

$$(ag_1)(ag_2)(ag_3) \dots (ag_n) = \pi = a^n g_1 g_2 \dots g_n = a^n \pi$$

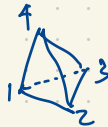
so $a^n = 1$ and $k = |a|$ must divide n . \square

Lagrange's Theorem If G is any finite group of order n , and $H \leq G$ (i.e. H is a subgroup of G) then $|H| \mid n$.

This generalizes the previous statement: if $g \in G$ then by Lagrange's Theorem, $| \langle g \rangle | = |g| \mid |G|$.

Eg. $|A_4| = \frac{1}{2} |S_4| = 12$, $A_4 = \{ (1), (123), (124), (132), (134), (142), (143), (234), (243), (12)(34), (13)(24), (14)(23) \}$.

The symmetry group of a regular tetrahedron



is isomorphic to S_4 .

The rotational symmetry group of the regular tetrahedron (the direct isometry group, consisting of those symmetries that preserve orientation) is isomorphic to A_4 .

$$A_4 = \{(), (123), (124), (132), (134), (142), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

Subgroups of A_4 have order 1, 2, 3, 4.

Elements of A_4 have order 1, 2, 3.

Divisors of $|A_4| = 12$ are 1, 2, 3, 4, 6, 12.

$$\langle (243), (12)(34) \rangle = \{(), (243), (12)(34), (234), (142), (124), \dots\} = A_4.$$

$$(243)(12)(34) = (142)$$

$\{(), (12)(34), (13)(24), (14)(23)\}$ is the Klein four-group, a subgroup of A_4 .

Question: How many subgroups of \mathbb{Z} are there containing 4? (Note: \mathbb{Z} is an additive group.)

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$$

$$2\mathbb{Z} = \{\dots, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}$$

$$4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, 12, \dots\}$$

$$-4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, 12, \dots\}$$

Answer: There are three subgroups of \mathbb{Z} containing 4, namely \mathbb{Z} , $2\mathbb{Z}$, $4\mathbb{Z}$.

\mathbb{Z} has infinitely subgroups: one finite subgroup $\{0\}$ and all the other subgroups are infinite.

There are infinite subgroups of \mathbb{Z} containing 4 but not infinitely many subgroups of \mathbb{Z} containing 4.

Note: For every cyclic group G , all subgroups of G are cyclic; they are generated by powers of the generator of G .

Ex. $G = \langle g \rangle$ where $|g| = \infty$ i.e. $|G| = |\langle g \rangle| = |g| = \infty$.

$= \{ \dots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \dots \}$ with no repeats.

1 is the identity

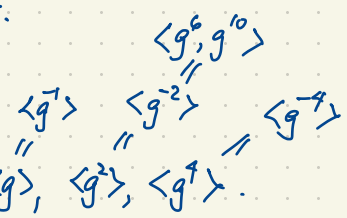
$$g^i g^j = g^{i+j} = g^j g^i$$

How many subgroups of $G = \langle g \rangle$ contain g^4 ? Three: $\langle g \rangle, \langle g^2 \rangle, \langle g^4 \rangle$.

$$G = \{ \dots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, g^4, \dots \}$$

$$\langle g^2 \rangle = \{ \dots, g^6, g^4, g^2, 1, g^2, g^4, g^6, \dots \}$$

$$\langle g^4 \rangle = \{ \dots, g^8, g^4, 1, g^4, g^8, g^{12}, \dots \}$$



$$\langle g^6, g^{10} \rangle \leq \langle g^2 \rangle$$

$$\langle g^2 \rangle \leq \langle g^6, g^{10} \rangle$$

Since $g^2 = (g^6)^2 (g^{10})^{-1}$

So $\langle g^2 \rangle = \langle g^6, g^{10} \rangle$

$G \cong \mathbb{Z}$
 multiplicative cyclic group \cong additive cyclic group

$\phi: \mathbb{Z} \rightarrow G$ is an isomorphism
 $\phi(i) = g^i$

Theorem If G is a group of even order, then G has an element of order 2 (i.e. at least one element of order 2). Note: G is not necessarily abelian.

OCTOBER 2023

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Handwritten annotations on the calendar:

- Red boxes around dates 10-11, 17-18, and 19-20.
- Red 'X' marks on dates 19 and 20.
- Purple boxes around dates 22-23 and 29-30.
- Yellow highlight on date 30 with the word "Test!" written in red.

Free Printable Calendars from [Typecalendar.com](https://typecalendar.com)