Algebra I

Group Theory

Book 2

Transpositions $(i\,j)$ are odd permutations.

$$(1\,2\,3\,4\,5\,6\,7\,8\,9) = (1\,9)(1\,8)(1\,7)(1\,6)(1\,5)(1\,4)(1\,3)(1\,2)$$

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:

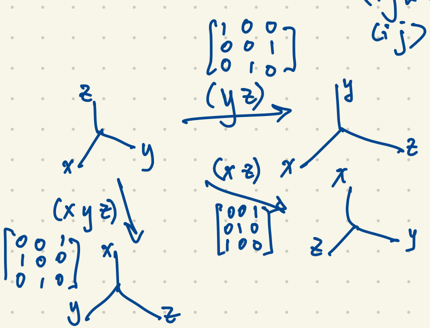
Even
- $()$ 1
- $(i\,j\,k)$ 20
- $(i\,j\,k\,l\,m)$ 24
- $(i\,j)(k\,l)$ 15
- total: 60

Odd
- $(i\,j)$ 10
- $(i\,j\,k\,l)$ 30
- $(i\,j\,k)(l\,m)$ 20
- total: 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 $T: \mathbb{R}^n \to \mathbb{R}^n$ 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.

" " " " " " odd " " " " " " " " " odd.

In S_3:

$(13)(12)(13)(23)(23)(23)(12)(23) = (1\,2\,3)$ says (123) is an even permutation.

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

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

Groups of order 2

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

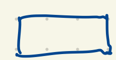
$\circ$	$()$	(12)
$()$	$()$	(12)
(12)	(12)	$()$

$+$	0	1
0	0	1
1	1	0

$\cdot$	1	-1
1	1	-1
-1	-1	1

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

has a cyclic symmetry group of order 4



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

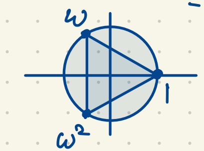
<u>Theorem</u> Any two groups of prime order are isomorphic; they are cyclic of order p.

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, $\omega = \frac{-1+i\sqrt{3}}{2} = e^{2\pi i/3}$

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

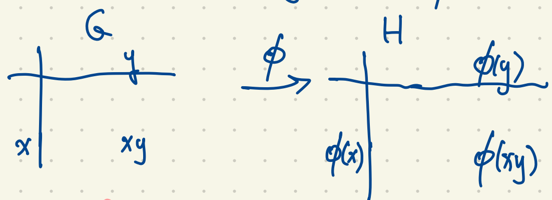
∘	()	(123)	(132)
()	()	(123)	(132)
(123)	(123)	(132)	()
(132)	(132)	()	(123)

·	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 $\phi : G \to H$ such that $\phi(xy) = \phi(x)\phi(y)$

operation in G operation in H



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

An isomorphism $\phi : \mathbb{R} \longrightarrow (0,\infty)$, $\phi(x+y) = \phi(x)\phi(y)$ is defined by $\phi(x) = e^x$

$\mathbb{R}$ under addition; $(0,\infty)$ under multiplication (subgroup of $\mathbb{R}^\times = (-\infty,0) \cup (0,\infty)$)

$e^{x+y} = e^x \cdot e^y$.

$\ln = \phi^{-1} : (0,\infty) \longrightarrow \mathbb{R}$

$\mathbb{R} \not\cong \mathbb{R}^\times$

since $\mathbb{R}$ (reals under addition) has only one element of finite order whereas $\mathbb{R}^\times$ has two elements of finite order: ± 1.

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

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

is isomorphic to

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

$\phi(0) = c$
$\phi(1) = a$
$\phi(2) = b$

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

or $\phi(0) = c$
$\phi(1) = b$
$\phi(2) = a$

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

+	0
0	0

Every group of order 1 is isomorphic to

·	1
1	1

(trivial group $\{1\}$)

" " " " " 2 " " " $\mathbb{Z}/2\mathbb{Z}$

+	0	1
0	0	1
1	1	0

	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

$$\langle a \rangle = \{e, a, \underset{b}{a^2}, \underset{c}{a^3}, \underset{d}{a^4}\}$$

	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

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. $(ca)d = dd = c$
$c(ad) = cb = e$

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

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

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

$\square$

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 $(y^{-1}x^{-1})(xy) = y^{-1} 1 y = 1$ 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

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

	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

Gives $\{(\,), (1234), (13)(24), (1432)\}$ 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 $\pi = g_1 g_2 g_3 \cdots g_n$ where $G = \{g_1, g_2, \ldots, g_n\}$, $g_1 = 1$.
Note: since G is abelian, π is well-defined; it doesn't depend on what order we list the elements $g_1, \ldots, g_n \in G$. Pick $a \in G$. (So $a \in \{g_1, \ldots, g_n\}$.) The elements $ag_1, ag_2, \ldots, ag_n$ are again all the elements of G so

	g_1	g_2	$\cdots$	g_n
a	ag_1	ag_2	$ag_3 \cdots$	ag_n

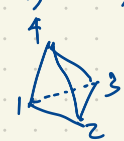
$$(ag_1)(ag_2)(ag_3)\cdots(ag_n) = \pi = a^n g_1 g_2 \cdots g_n = a^n \pi$$

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, $|g| = |\langle g \rangle| \mid |G|$.

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

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.

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

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

$\{(), (12)(34), (13)(24), (14)(23)\}$ 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 <u>additive</u> group.)

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

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

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

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

Answer: There are <u>three</u> 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.

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

$= \{\ldots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots\}$ 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: $\langle g \rangle, \langle g^2 \rangle, \langle g^4 \rangle$.

$\langle g^{-1} \rangle = \langle g \rangle$, $\quad \langle g^6, g^{10} \rangle = \langle g^{-2} \rangle = \langle g^2 \rangle$, $\quad \langle g^{-4} \rangle = \langle g^4 \rangle$

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

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

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

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

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

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

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

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

$\phi : \mathbb{Z} \to G$ is an isomorphism

$\phi(i) = g^i$

<u>Theorem</u> 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.

<u>Proof</u> Pair up each group element with its inverse giving pairs $\{g, g^{-1}\}$ for $g \in G$.
Note that $g = g^{-1}$ iff g has order 1 or 2. ($g = g^{-1} \iff g^2 = 1 \iff |g|$ divides 2). So G is partitioned into subsets $\{g, g^{-1}\}$ having size 1 or 2. If G has no elements of order 2 then we have <u>partitioned</u> a set G of even cardinality into one subset $\{1\}$ of size 1, and a collection of pairs $\{g, g^{-1}\}$ of size 2, a contradiction. $\square$

What we actually showed is that in a group of even order, the number of elements of order 2 is odd. (In a group of odd order, there are no elements of order 2 although we haven't proved this yet except in the abelian case.)

Eg. Direct Products: Given groups G, H (say, multiplicative) we form the <u>direct product</u> of G and H as $G\times H = \{(g,h) : g\in G,\ h\in H\}$ (the cartesian product of the sets G and H) which becomes a group under <u>coordinatewise</u> <u>multiplication</u> i.e.

$$(g,h)(g',h') = (gg', hh')$$

and coordinatewise inverses i.e. $(g,h)^{-1} = (g^{-1}, h^{-1})$

and the coordinatewise identity $1\in G\times H$ is $1 = 1_{G\times H} = (1_G, 1_H)$. or $e_{G\times H} = (e_G, e_H)$.

Eg. $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$ under addition mod 2

+	0	1
0	0	1
1	1	0

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} = \{(x,y) : x,y\in\mathbb{Z}/2\mathbb{Z}\} = \{(0,0),(0,1),(1,0),(1,1)\}$$

$(x,y)+(x',y') = (x+x', y+y')$. The identity $0 = (0,0)$.

This is the Klein four-group since it has 3 elements of order 2.

Note: Many books write $\mathbb{Z}_2$ or Z_2 in place of $\mathbb{Z}/2\mathbb{Z}$

If $|G| = m$ and $|H| = n$ then $|G\times H| = mn$.

If G and H are abelian then so is $G\times H$.

In fact, the converse holds: G and H are both abelian, iff $G\times H$ is abelian.

$G\times H \cong H\times G$

$\phi : G\times H \to H\times G$

$\phi(g,h) = (h,g)$ is an isomorphism.

$G \times H$ has a subgroup $G \times \{1_H\} = \{(g, 1_H) : g \in G\} \cong G$

An isomorphism $G \times \{1_H\} \longrightarrow G$ is given by $(g, 1_H) \longmapsto g$.

Likewise, $G \times H$ has a subgroup $\{1_G\} \times H \cong H$

$$\underbrace{(g, 1_H)}_{\substack{\uparrow \\ G \times \{1_H\} \\ \cong \\ G}} \underbrace{(1_G, h)}_{\substack{\uparrow \\ \{1_G\} \times H \\ \cong \\ H}} = (g, h) = (1_G, h)(g, 1_H)$$

Eg. $\underbrace{\mathbb{R}^\times = (-\infty, 0) \cup (0, \infty)}_{\text{multiplicative group}} \cong \underbrace{\mathbb{R}}_{\text{additive group}} \times \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{additive}}$

An isomorphism $\phi : \mathbb{R}^\times \longrightarrow \mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$ is $\phi(a) = \begin{cases} (\ln|a|, 0) & \text{if } a > 0 \\ (\ln|a|, 1) & \text{if } a < 0 \end{cases}$