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 $\alpha$ is a product of an even number of transpositions, then $\alpha$ 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 |
| | 60 |

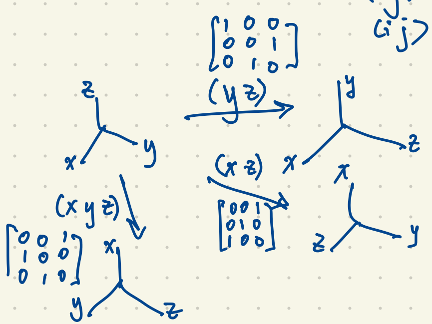
Odd

| | |
|---|---|
| $(i\,j)$ | 10 |
| $(i\,j\,k\,l)$ | 30 |
| $(i\,j\,k)(l\,m)$ | 20 |
| | 60 |

$|S_5| = 120$

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

$|A_5| = 60$




$$\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix} \quad \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix} \quad \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$$

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 $\alpha$ is a product of an even number of transpositions, then $\alpha$ is even.

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

In $S_3$:

$(1\,3)(1\,2)(1\,3)(2\,3)(2\,3)(2\,3)(1\,2)(2\,3) = (1\,2\,3)$ says $(1\,2\,3)$ 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

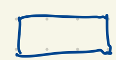
| $\circ$ | $()$ | $(12)$ |
|---|---|---|
| $()$ | $()$ | $(12)$ |
| $(12)$ | $(12)$ | $()$ |

| $+$ | 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)

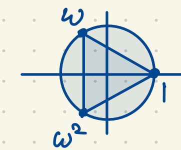
<u>Theorem</u> Any two groups of prime order are isomorphic; they are cyclic of order $p$.

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 |

| $\circ$ | () | (123) | (132) |
|---|---|---|---|
| () | () | (123) | (132) |
| (123) | (123) | (132) | () |
| (132) | (132) | () | (123) |

| $\cdot$ | $1$ | $\omega$ | $\omega^2$ |
|---|---|---|---|
| $1$ | $1$ | $\omega$ | $\omega^2$ |
| $\omega$ | $\omega$ | $\omega^2$ | $1$ |
| $\omega^2$ | $\omega^2$ | $1$ | $\omega$ |




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 $H$

$G$

| | $y$ |
|---|---|
| $x$ | $xy$ |

$\xrightarrow{\phi}$

$H$

| | $\phi(y)$ |
|---|---|
| $\phi(x)$ | $\phi(xy)$ |

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

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

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

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

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

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

| + | 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.

<u>Theorem</u>: 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 ($bc=a$).

<u>Theorem</u> If every non-identity element of a group G has order 2, then G is abelian.

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

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

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

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

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, $\pi$ 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

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

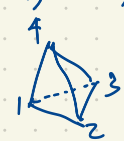
$$(ag_1)(ag_2)(ag_3)\cdots(ag_n) = \pi = a^n g_1 g_2 \cdots g_n = a^n \pi$$

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 $A_4$.