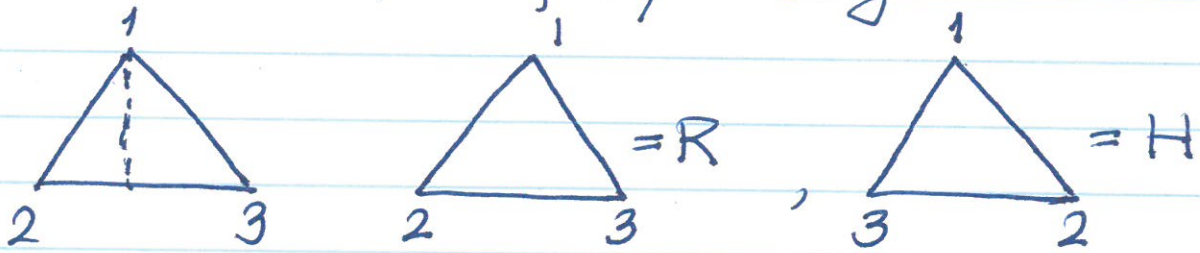
D_3 = symmetries of an equilateral triangle

$$= \{I, R, R^2, H, HR, HR^2\}$$

where R = rotation about $2\pi/3$

H = reflection about the vertical axis of symmetry.



Recall: $R^3 = I$, $H^2 = I$, $RH = HR^2$

$\neq HR$

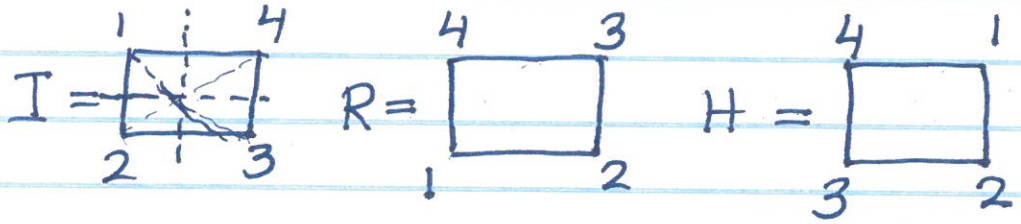
$\Rightarrow D_3$ is not abelian. ($R^2H = HR$)

$\circ$	I	R	R^2	H	HR	HR^2
I	I	R	R^2	H	HR	HR^2
R	R	R^2	I	HR^2	H	HR
R^2	R^2	I	R	HR	HR^2	H
H	H	HR	HR^2	I	R	R^2
HR	HR	HR^2	H	R^2	I	R
HR^2	HR^2	H	HR	R	R^2	I

Latin square

Cayley Table or multiplication table for D_3.

Ex (2) Symmetries of a square $= D_4$



R = rotation by $2\pi/4 = \pi/2$

H = reflection about the vertical axis of symmetry.

$$D_4 = \{I, R, R^2, R^3, H, HR, HR^2, HR^3\}$$

$|D_4| = 8$

Note: $R^4 = I$, $H^2 = I$, $RH = HR^3$, $RH = HR^2$ (verify)

Ex (3) Symmetries of a regular n-gon.

$= D_n$ = Dihedral group of degree n.

$|D_n| = 2n$

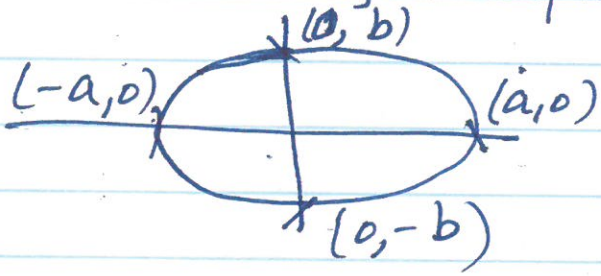
$$D_n = \{I, R, R^2, \cdots, R^{n-1}, H, HR, \cdots, HR^{n-1}\}$$

R = rotation about $2\pi/n$

H = reflection about vertical axis of symmetry.

Ex (4)

$G =$ Symmetries of ellipse



$G = \{I, R, H, HR\}$

R = rotation by 180°

H = reflection about the vertical axis of symmetry

$\Rightarrow HR = RH$ is the reflection about the horizontal axis of symmetry.

$\circ$	I	R	H	HR
I	I	R	H	HR
R	R	I	HR	H
H	H	HR	I	R
HR	HR	H	R	I

Note: G is abelian.

G group.

order of $G = |G| = \#$ of elements in G.

For $a \in G$
order of 'a' $= o(a) = m$ if m is the smallest positive integer such that $a^m = e$.

Ex(1) $\mathbb{Z}_{10} = \{0, 1, 2, \cdots, 9\}$

$e = 0$

$o(1) = 10$
$o(2) = 5$
$o(3) = 10$
$o(4) = 5$
$o(5) = 2$
$o(6) = 5$
$o(7) = 10$
$o(8) = 5$
$o(9) = 10$
$o(0) = 1$

$\underbrace{1+1+\cdots+1}_{10} = 0$

What are the inverse?

$0^{-1} = 0$, $1^{-1} = 9$, $2^{-1} = 8$, $3^{-1} = 7$, $4^{-1} = 6$
$5^{-1} = 5$, $6^{-1} = 4$, $7^{-1} = 3$, $8^{-1} = 2$, $9^{-1} = 1$

Thm: G group, $a \in G$

Then $o(a) = o(a^{-1})$

$a \in G$, G group, $b \in G$

- $(a^{-1})^{-1} = a$
- $(ab)^{-1} = b^{-1}a^{-1}$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$$
$$= (ae)a^{-1}$$
$$= aa^{-1} = e$$

Remark: $a \in G$, assume $o(a) = 2$

$\Rightarrow aa = e \Rightarrow a^{-1} = a$

Recall: G abelian group $\iff ab = ba \ \forall a, b \in G$.

Ex (2) Suppose ~~$\forall e \neq a \in G$~~, G group $o(a) = 2$. Show that G is abelian.

Let $a, b \in G \Rightarrow ab \in G$ and

$o(a) = 2$, $o(b) = 2$, $o(ab) = 2$

$\Rightarrow (ab)^{-1} = ab$, $a^{-1} = a$, $b^{-1} = b$

$b^{-1}a^{-1} = ba$

$\Rightarrow ab = ba \ \forall a, b \in G$

$\Rightarrow G$ abelian.

~~Ex(3) $GL(2,\mathbb{R}) = \{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a$~~

Ex(3) $GL(2,\mathbb{R}) = \left\{ \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{A} \mid \underbrace{ad-bc \neq 0}_{\det(A)}, \; a,b,c,d \in \mathbb{R} \right\}$

$A, B \in GL(2,\mathbb{R})$

AB = multiplication of matrices

$\det(AB) = \det(A)\det(B) \neq 0$

$\Rightarrow AB \in GL(2,\mathbb{R})$

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R})$ identity

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{(ad-bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$GL(2,\mathbb{R})$ is a group, called the general linear group.

Ex(4) $SL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \underset{ad-bc=1}{a,b,c,d \in \mathbb{R}} \right\}$

called the special linear group.

Ex(5) $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ not a group under $\cdot_5$.

1 = multiplicative identity

$(2)(3) = 1 \Rightarrow 2^{-1} = 3,\ 3^{-1} = 2$

$(4)(4) = 1 \Rightarrow 4^{-1} = 4$

$(\mathbb{Z}_5 - \{0\}, \cdot_5)$ is a group.

$e = 1$.

Consider $GL(2, \mathbb{Z}_5)$ group

$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \in GL(2, \mathbb{Z}_5)$

$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^{-1} = \frac{1}{4}\begin{pmatrix} 1 & -2 \\ -1 & 1 \end{pmatrix} = 4^{-1}\begin{pmatrix} 1 & 3 \\ 4 & 1 \end{pmatrix}$

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

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

$\det = 1 - 2 = -1 = 4$

P54 # 1, 3, 4, 5, 6, 7, 11, 15, 16, 18, 19, 20, 23, 25, 27, 32, 33, 34, 47, 52.

$\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$

$(\mathbb{Z}_n, +_n)$ abelian group

$(\mathbb{Z}_n, \cdot_n)$ not a group

$U(n) = \{ k \in \mathbb{Z}_n \mid \gcd(k, n) = 1 \}$ Abelian group with $\cdot_n$

Ex(1) $U(8) = \{1, 3, 5, 7\}$

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Abelian Group

$e = 1$, $3^{-1} = 3$, $5^{-1} = 5$, $7^{-1} = 7$.

$k \in U(n)$, $k^{-1} = ?$

$\gcd(k, n) = 1 \Rightarrow kt + ns = 1$

$\Rightarrow (kt + ns) \bmod n = 1$

$(kt) \bmod n + (ns) \bmod n$

$\Rightarrow (kt) \bmod n = 1$ ($ns \bmod n = 0 \bmod n$)

$(k \bmod n)(t \bmod n) = 1$

$k''(t \bmod n) = 1$, $\Rightarrow k^{-1} = a (= t \bmod n)$.

Ex(2) $U(10) = \{1, 3, 7, 9\}$

$3^{-1} = 7$, $7^{-1} = 3$, $9^{-1} = 9$

$(3)(3) = 9$, $(3)(3)(3) = 7$, $(3)(3)(3)(3) = 1$

$\Rightarrow o(3) = 4 = o(7)$, $o(9) = 2$.

Remark: p prime

$$\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$$

$$U(p) = \{1, 2, \cdots, p-1\} = \mathbb{Z}_p - \{0\}$$

$$|\mathbb{Z}_p| = p, \quad |U(p)| = p-1.$$

Subgroup: A nonempty subset H of a group G is a subgroup if

(1) For $a, b \in H$, $ab \in H$

(2) For each $a \in H$, $a^{-1} \in H$.

($\Rightarrow e \in H$.)

(In particular, if H is a subgroup of G then H is a group under the mult. in G.)

Remark: Conditions (1) & (2) above is equivalent to

(*) For $a, b \in H$, $ab^{-1} \in H$.

Ex(1) $G = (\mathbb{Z}, +)$

$H = 2\mathbb{Z}$ = set of even integers.

$0 \in H$

(*) $\underbrace{2m}_{a}, \underbrace{2n}_{b} \in H$

$ab^{-1} = a + (-b) = a - b = 2m - 2n$

$= 2(m-n) \in H$

$\Rightarrow$ H subgroup.

Remark: Every subgroup of an abelian group is abelian.

Ex(2) $G = GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad - bc \neq 0 \right\}$

$H = SL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad - bc = 1 \right\}$

$\subset GL(2, \mathbb{R})$

Let $A, B \in H$, $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$

$$AB^{-1} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} d_2 & -b_2 \\ -c_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 d_2 - b_1 c_2 & -a_1 b_2 + b_1 a_2 \\ c_1 d_2 - d_1 c_2 & -c_1 b_2 + d_1 a_2 \end{pmatrix}$$

$$(a_1d_2 - b_1c_2)(-c_1b_2 + d_1a_2) - (-a_1b_2 + b_1a_2)(c_1d_2 - d_1c_2)$$

$$\stackrel{?}{=} 1$$

given $a_1d_1 - b_1c_1 = 1$, $a_2d_2 - b_2c_2 = 1$.

$$= -a_1c_1b_2d_2 + a_1a_2d_1d_2 + b_1b_2c_1c_2 - b_1d_1a_2c_2$$
$$+ a_1c_1b_2d_2 - a_1d_1b_2c_2 - a_2b_1c_1d_2 + b_1d_1a_2c_2$$

$$= a_1d_1(a_2d_2 - b_2c_2) - b_1c_1(a_2d_2 - b_2c_2)$$

$$= (a_2d_2 - b_2c_2)(a_1d_1 - b_1c_1) = 1. \quad //$$