Remark: For every $n \in \mathbb{N}$, there is a group with n elements, namely $(\mathbb{Z}_n, +)$.

which is Abelian / Commutative

~~Other examples not satisfying (G4)~~

Example: $GL_2(\mathbb{Z}_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}_2, \ \cancel{ad-bc \neq 0} \ ad-bc=1 \right\}$

Example: $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$

$(G, *) = (S_3, \circ)$ is a group, not Abelian

Will further discuss on Thursday.

Check (G0), (G1), (G2), (G3).

Check $X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $Y = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ $\quad XY = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = YX$.

Check (G0), (G1), (G2), (G3)

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

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

Properties Let $(G, *)$ be a group. i.e., (G0), (G1), (G2), (G3) hold
closed asso. iden inverse.

(a) The left and right cancellation law holds.

(b) The equation $a * x = b$ has a unique solution x for any $a, b \in G$, and so is the equation $y * a = b$.

(c) The identity in a group is unique.

(d) For each element in G, there is a unique inverse.

(e) (Socks-Shoes Property) $(a * b)' = b' * a'$ for any $a, b \in G$.

(a) To prove

For any $a,b,c \in G$ $\begin{cases} a * b = a * c \Rightarrow b = c & \text{left cancellation} \\ b * a = c * a \Rightarrow b = c & \text{right cancellation} \end{cases}$

Proof. Suppose $a * b = a * c$.

Let e be the identity ensured by (G2), and let $\hat{a}$ be the inverse of a.

i.e., $e * x = x * e = x \quad \forall x \in G$, $\quad a * \hat{a} = \hat{a} * a = e$.

Then $\hat{a} * (a * b) = \hat{a} * (a * c)$, By (G1), $(\hat{a} * a) * b = (\hat{a} * a) * C$

Then $b = c$ $\quad$ i.e., $e * b = e * c$

Similarly, we can prove the right cancellation.

Alternatively, assume $a * b = a * c$.

Then $b = e * b = (\hat{a} * a) * b = \hat{a} * (a * b) = \hat{a} * (a * c)$

$= (\hat{a} * a) * C = e * C = C$.

(b) Suppose $a, b \in G$. To solve $a * x = b$. ~~$a * x = b$~~.

Let $\hat{a}$ be the inverse of a. Then

(*) $\hat{a} * b = \hat{a} * (a * x) = (\hat{a} * a) * x = e * x = x$

$\therefore$ $x = \hat{a} * b$ satisfies the ~~condit~~ equation.

existence

In fact, for $x = \hat{a} * b$

Then $a * x = a * (\hat{a} * b) = (a * \hat{a}) * b$
$= e * b = b$.

uniqueness

Suppose $a * x_1 = b$ and $a * x_2 = b$
for $x_1 = \hat{a} * b$.

Then $a * x_1 = a * x_2$ $\therefore$ $x_1 = x_2$.

Similarly, one can show $y * a = b$
has a unique solution.

(c) $e \in G$ is unique. Let e satisfy $e * x = x * e = x$ $\forall x \in G$
Suppose $\hat{e} \in G$ also satisfy $\hat{e} * x = x * \hat{e} = x$ $\forall x \in G$.

$e * e = e$ & $\hat{e} * e = e$

$\therefore$ $e * e = \hat{e} * e$ $\Rightarrow$ $e = \hat{e}$ by right cancellation

Alternatively: $e = e * \hat{e} = \hat{e}$

(d) Let e be the unique identity in G.
Let $a \in G$. Suppose ~~$\hat{a} * a =$~~ $\hat{a} \in G$ ~~s.t.~~ satisfies
$\hat{a} * a = a * \hat{a} = e$.

Let $a' \in G$ also satisfy $a' * a = a * a' = e$.

Then $\hat{a} * a = e = a' * a \Rightarrow \hat{a} = a'$ by right "

(e) Let $a, b \in G$. a', b' be their inverses.

Now, $a*b \in G$ ~~have~~ has an inverse $(a*b)'$

To show :

$$(a*b)' = b'*a'.$$

Note that

$$(a*b)*(a*b)' = e$$

$$(a*b)*(b'*a')$$

$= ((a*b)*b')*a'$ by (G1)

$= (a*(b*b'))*a' = (a*e)*a' = (a)*a'$

$= e$

$\therefore \quad (a*b)*(a*b)' = (a*b)*(b'*a')$

By left cancellation, $(a*b)' = b'*a'$.

Isomorphisms and Group Tables

Group Isomorphism Two groups $(G_1, *_1)$ and $(G_2, *_2)$ are isomorphic if there is a bijection $\phi : G_1 \to G_2$ such that $\phi(a *_1 b) = \phi(a) *_2 \phi(b)$.

Example $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$; $(\mathbb{Z}_n, +)$ and $(\{z \in \mathbb{C} : z^n = 1\}, \cdot)$.

Remrak For groups of small sizes, we can use the group table to check isomorphism.

All two element groups are isomorphic to $(\mathbb{Z}_2, +)$:

$(\mathbb{Z}_2, +)$

$+$	0	1
0	0	1
1	1	0

$(\{1, -1\}, \cdot)$

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

$(G, *)$

$\cdot$	e	a
e	e	a
a	a	e

All three element groups are isomorphic to $(\mathbb{Z}_3, +)$.

$\mathbb{Z}_3$

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

$(G, *)$

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

There are two non-isomorphic four element groups.

($\mathbb{Z}_4, +$), and

the Klein 4-group ($K, *$): the set of 2×2 diagonal orthogonal matrices under multiplication.

Case 1. $a * a = e$.

Then

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

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

$*$	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 4 group.

$\bar{0}$ $\bar{2}$ $\bar{1}$ $\bar{3}$ in $\mathbb{Z}_4$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\mathbb{Z}_4$

Case 2. $a * a = b$

Then

$*$	e	a	b	c
e	e	a	b	c
a	a	b		
b	b			
c	c			

$\rightarrow$

$\bar{0}$ $\bar{1}$ $\bar{2}$ $\bar{3}$ in $\mathbb{Z}_4$

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\mathbb{Z}_4$

There are only one five element group $(\mathbb{Z}_5, +)$ up to isomorphism.

Facts: ① If $|G| = p$, p is a prime

then $(G, *) \underset{\varphi}{\cong} (\mathbb{Z}_p, +)$,

isomorphic

which is Abelian.

② If $|G| = 6$, then

$(G, *) \cong (\mathbb{Z}_6, +)$

or $(G, *) \cong (S_3, \circ)$

which is not Abelian

Check

D_6 : dihedral group with 6 elements (symmetry group of $\triangle$)

S_3 : group of bijections on $\{1, 2, 3\}$

$GL_2(\mathbb{Z}_2)$: 2×2 invertible matrices with entries in $\mathbb{Z}_2$.

are all isomorphic by comparing their group tables