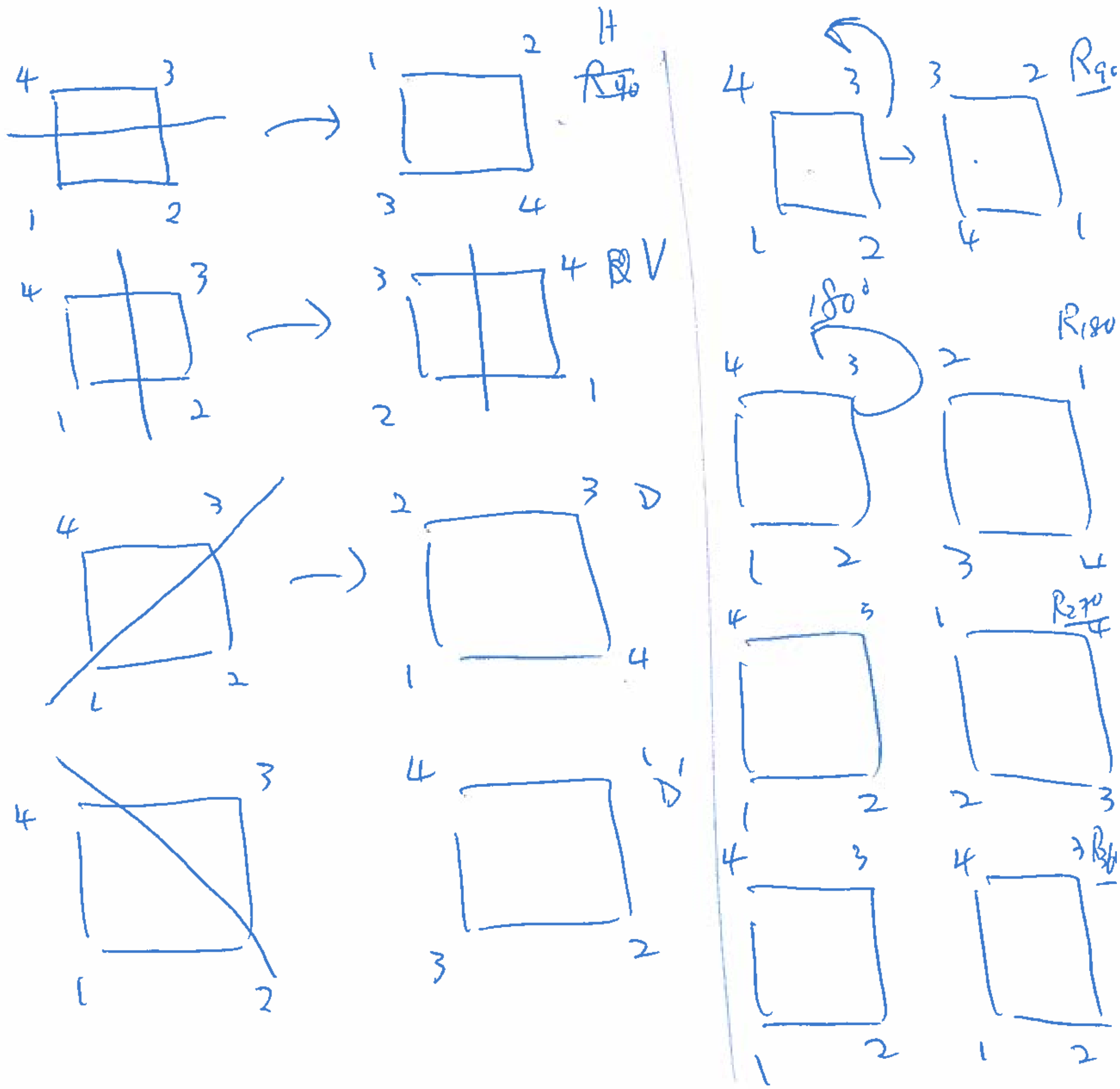
Chapter 1 Symmetry of squares and regular polygons

Examples of symmetry group and subgroup

- For a square, there are rotation symmetries: $R_0, R_{90}, R_{180}, R_{270}$, reflection symmstries: H, V, D, D'.
- These operations will "permute" the four corners of the square labeled by $1, 2, 3, 4$, and generate 8 different permutations $\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$ in S_4 (the group of all permutations of $\{1, 2, 3, 4\}$. See the table in p. 33.

  8 bijection $\begin{pmatrix} 1 & 2 & 3 & 4 \\ \square & \square & \square & \square \end{pmatrix}$

- The eight opertaions will form the dihedral group D_4 under composition.
- In general, for an regular n-side polygon with $n \geq 3$, we can form a **dihedral group** D_n.

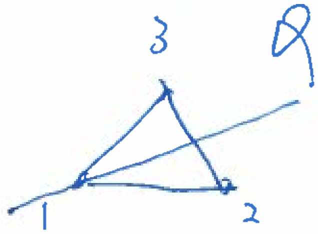


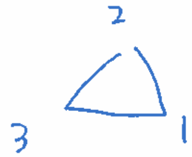
Symmetry group of Triangle $= S_3$

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

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

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



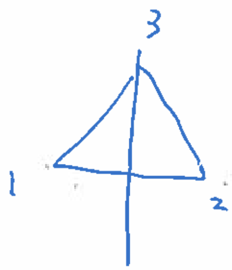


120

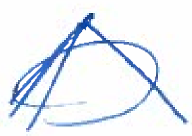
240

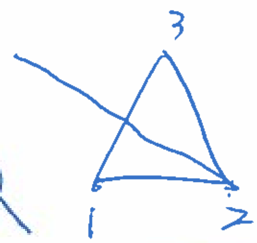
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

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



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

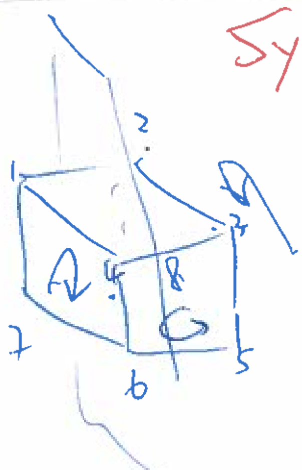




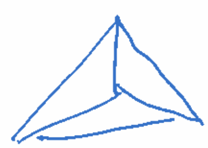
Fact: Symmetry group of an n-side polygon has $2n$ operations (elements)

Symmetry groups of solid

$\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ \end{pmatrix}$



Cube



Tetrahedron

$x * x \; + \; a * x = b$

Chapter 2 Groups

- We will begin with a structure - *Group* - with only $\boxed{\text{one operation } *}$ in which we can solve the equation $\boxed{a * x = b.}$
- You will be amazed by the fact that very rich theory can be developed with a single operation satisfying some simple rules (axioms).

Definition of Binary operations A $\boxed{\textit{binary operation } *}$ on a set G is a rule assigning every pair of elements $\boxed{a, b \in G}$ a *unique* element $\boxed{c = a * b \text{ in } G.}$
So, a binary operation is a function from $G \times G$ to G.

Examples ...

Definition of a group A binary structure $(G, *)$ is a group if

(G1) $*$ is associative,

(G2) there is an identity $e \in G$, and

(G3) for every $a \in G$, there is an "inverse" $a' \in G$ so that $a * a' = a' * a = e$. ← ✓✓✓

Remarks

- (G0): $*$ is binary **must** be checked. →
- By (G2), G is not empty. One needs to check (G2) before (G3).
- A group $(G, *)$ is Abelian if $*$ is commutative.
- Examples: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^*, \cdot), \ldots$

Note: In $x, y \in \mathbb{R}^n$, $\boxed{x + y = z} \in \mathbb{R}^n$ is a binary operation.

But $\lambda \in \mathbb{R}$, $x \in \mathbb{R}^n$, λx is not a binary operation.

$x, y \in \mathbb{R}^n$ $x \cdot y = x_1 y_1 + \cdots + x_n y_n$ is NOT a binary operation.

(G0) $x, y \in \mathbb{R} \Rightarrow x + y \in \mathbb{R}$

(G1) $(x+y)+z = x+(y+z) \quad \forall x, y, z \in \mathbb{R}$

(G2) $0 \in \mathbb{R}$ satisfies $0 + x = x + 0 = x \quad \forall x \in \mathbb{R}$

(G3) let $x \in \mathbb{R}$, let $x' = -x \in \mathbb{R}$, $x + x' = x + (-x) = 0$
$= (-x) + x = x' + x$.

↑

$(\mathbb{R}^n, +)$ is a group!

Examples of groups.

1) ~~(G, *) = (R,~~ $(G,*) = (\mathbb{R}, -)$ is $\boxed{\text{not}}$ a group. because (G1)

(G0) ✓ (G1) ✗ (G2) ✗

Let $(a,b,c) = (3,2,1)$.

Then $(a-b)-c = (3-2)-1 = 0$

$a-(b-c) = 3-(2-1) = 3-1 = 2.$

$\therefore (a*b)*c \neq a*(b*c)$

---

2) $(G,*) = (\mathbb{N}, +)$ is NOT a group

(2-1)

(G0) ✓

(G1) ✓ If $a,b,c \in \mathbb{N}$, then,

$(a+b)+c = a+(b+c)$.

(G2) If $\boxed{\mathbb{N} = \{1, 2, \cdots\}}$ then no $e \in \mathbb{N}$ such that $e+a = a+e = a$.

$\therefore$ (G2) Fails

(2-2) $(G,*) = (\mathbb{N}, +)$

Peano's axiom $\boxed{\mathbb{N} = \{0, 1, 2, 3, \cdots\}}$

(G0) ✓

(G1) ✓

(G2) ✓ $0 \in \mathbb{N}$ & $0+a = a+0 = a \ \forall a \in \mathbb{N}$.

(G3) ✗ For example $1 \in \mathbb{N}$, there is no $x \in \mathbb{N}$ such that $x+1 = 0 = 1+x$.

$\therefore$ (G3) fails

3) $(\mathbb{Q}, \cdot)$ is $\boxed{\text{not}}$ a group.

(G0) $x, y \in \mathbb{Q} \Rightarrow x \cdot y \in \mathbb{Q}$ ✓

(G1) $(x \cdot y) z = x \cdot (y \cdot z) \quad \forall x, y, z \in \mathbb{Q}$ ✓

(G2) Let $e = 1 \in \mathbb{Q}$. Then $e \cdot x = x \cdot e = x \quad \forall x \in \mathbb{Q}$ ✓

(G3) Let $x = 0$. Then there is no $x' \in \mathbb{Q}$ such that $x x' = 1$.

$\therefore$ (G3) Fails

3') $(\mathbb{Q}^*, \cdot)$ $\quad \mathbb{Q}^* = \{x \in \mathbb{Q} : x \neq 0\}$.

is a group

(G0) $x, y \in \mathbb{Q}^* \Rightarrow x y \in \mathbb{Q}^*$

(G1) $(x y) z = x (y z) \quad \forall x, y, z \in \mathbb{Q}^*$

(G2) $e = 1 \in \mathbb{Q}^*$ satisfies $e * x = x * e = x \quad \forall x \in \mathbb{Q}^*$

(G3) $\forall\ x = \frac{m}{n} \in \mathbb{Q}^*$, $m \neq 0$, $\therefore$ $x' = \frac{n}{m} \in \mathbb{Q}^*$ satisfies

$\therefore$ $x \cdot x' = x' \cdot x = 1$.

---

4) $(\mathbb{Z}_6^*, \cdot)$ is not a group

$(\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}, \cdot)$ $\quad \bar{2}, \bar{3} \in \mathbb{Z}_6^*$, $2 \cdot 3 = 6 = 0$ in $\mathbb{Z}_6$

(G0) Fails $\quad \bar{2}, \bar{3} \in \mathbb{Z}_6^*$, $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0} \notin \mathbb{Z}_6^*$

(3'') $(\mathbb{Z}^*, \cdot)$ is <u>not</u> a group.

(G0) $x, y \in \mathbb{Z}^* \Rightarrow x \cdot y \in \mathbb{Z}^*$ ✓

(G1) $(x \cdot y)z = x(y \cdot z) \quad \forall x, y, z \in \mathbb{Z}^*$ ✓

(G2) $1 \in \mathbb{Z}^*$ s.t. $1 \cdot x = x \cdot 1 = x \quad \forall x \in \mathbb{Z}^*$ ✓

(G3) $2 \in \mathbb{Z}^*$, but there is not

$\therefore$ (G3) Fails

$x' \in \mathbb{Z}^*$ s.t. $2 \cdot x' = x' \cdot 2 = 1$. $(*)$

Rmk: A less desirable ~~proof~~

To have $2x' = 1$ we need $x' = \frac{1}{2} \notin \mathbb{Z}^*$

is a viable proof but use information beyond $(\mathbb{Z}, \cdot)$. So it is not ~~proof~~ as good as $(*)$

(3''') $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ are groups

$(\mathbb{Z}_n, +)$ ✓, ~~$(M_n(\mathbb{R}), +)$~~ $(M_{m,n}(\mathbb{R}), +)$ are groups.

Remark: Check (G0) (G1) (G2) (G3)!

Example

Remark: All the previous examples satisfy (G4). Here is an example not satisfying (G4)

$$GL_n(\mathbb{R}) = \{ X \in M_n(\mathbb{R}) : X \text{ is invertible} \}$$

$$= \{ X \in M_n(\mathbb{R}) : \det(X) \neq 0 \}$$

(G0) ✓ $X, Y \in GL_n(\mathbb{R}) \Rightarrow \det(X) \neq 0$, $\det(Y) \neq 0$

$$\Rightarrow \det(XY) = \det(X)\det(Y) \neq 0$$

$$\Rightarrow XY \in GL_n(\mathbb{R})$$

(G1) By matrix theory,

$$(AB)C = A(BC) \quad \forall A, B, C \in GL_n(\mathbb{R})$$

(G2) $I_n \in GL_n(\mathbb{R})$ satisfies $I_n X = X I_n = X$ $\forall X \in GL_n(\mathbb{R})$

(G3) $X \in GL_n(\mathbb{R}) \Rightarrow X^{-1}$ exists & satisfies

$$X^{-1}X = X^{-1}X = I_n .$$

$\therefore$ $GL_n(\mathbb{R})$ is a group.

(G4) Fails if $n > 1$.

$$X = \left[\begin{array}{cc|c} 0 & 1 & 0 \\ 1 & 0 & \\ \hline 0 & & I_{n-2} \end{array}\right] \qquad Y = \left[\begin{array}{c|c} -1 & \\ \hline & I_{n-1} \end{array}\right] \in GL_n(\mathbb{R})$$

~~Then~~ But

$$XY = \left[\begin{array}{cc|c} 0 & -1 & 0 \\ 1 & 0 & \\ \hline 0 & & I_{n-2} \end{array}\right], \quad YX = \left[\begin{array}{cc|c} 0 & 1 & 0 \\ -1 & 0 & \\ \hline 0 & & I_{n-2} \end{array}\right].$$

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: $M_2(\mathbb{Z}_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}_2,\ ad-bc \neq 0 \right\}$

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

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