LECTURE 2

GROUPS

$(\mathbb{Z}, +)$

① We can add two integers to get another integer.

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(m, n) \longmapsto m+n$$

$\boxed{\text{Closure}}$

② There exists 0, such that $m+0 = m = 0+m$

$\boxed{\text{identity}}$

③ For $m \in \mathbb{Z}$, there exists $-m$ such that

$$m + (-m) = 0 = (-m) + m$$

$\boxed{\text{Inverse}}$

④ $\boxed{\text{Associativity}}$ $m + (n+p) = (m+n) + p$

<u>Defn:</u> A group G is a set of elements together with an operation $(G, *)$ such that the following properties hold:

i) Closure $*: G \times G \to G$

ii) Identity exists, say e.

iii) Corresponding to every $g \in G$, there is an inverse g^{-1}

iv) $*$ is associative.

<u>Aside:</u> $(\mathbb{N}, +)$ $+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$+$ is associative

no identity

no inverses

$(\mathbb{Z}, -)$ associativity

$$m - (n-p) \neq (m-n) - p$$

$m - e = m = e - m$ no such e

$(\mathbb{Z}, \times)$ closure

associative

identity $\quad m \times 1 = m = 1 \times m$

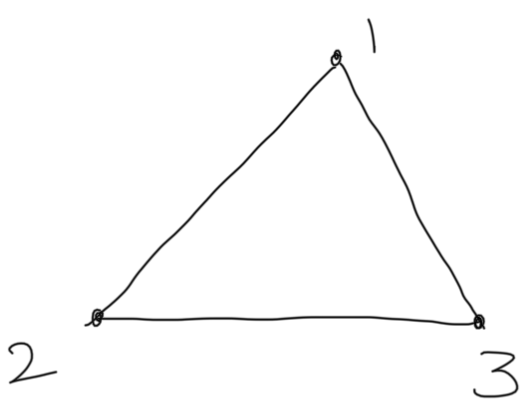
inverses $\quad \times$

$$2 \times \left(\frac{1}{2}\right) = 1$$

$\downarrow$

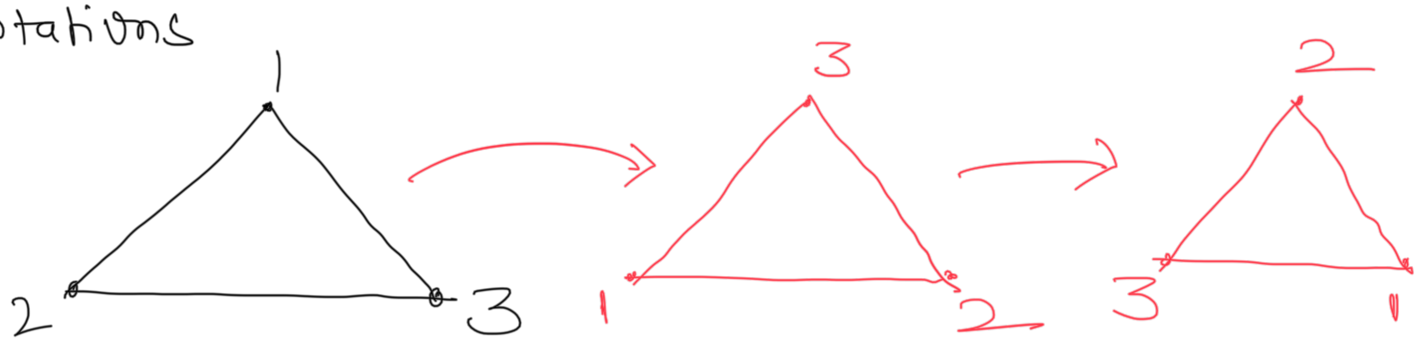
not an integer

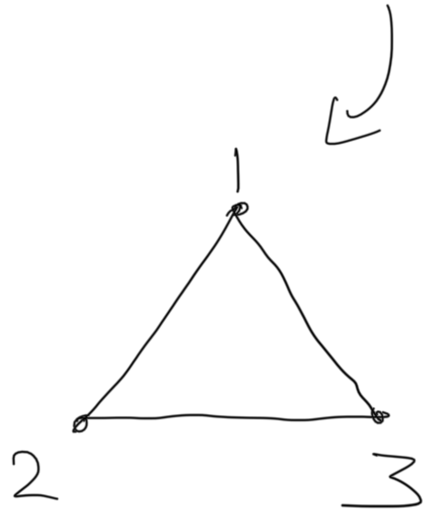
Example of Symmetry



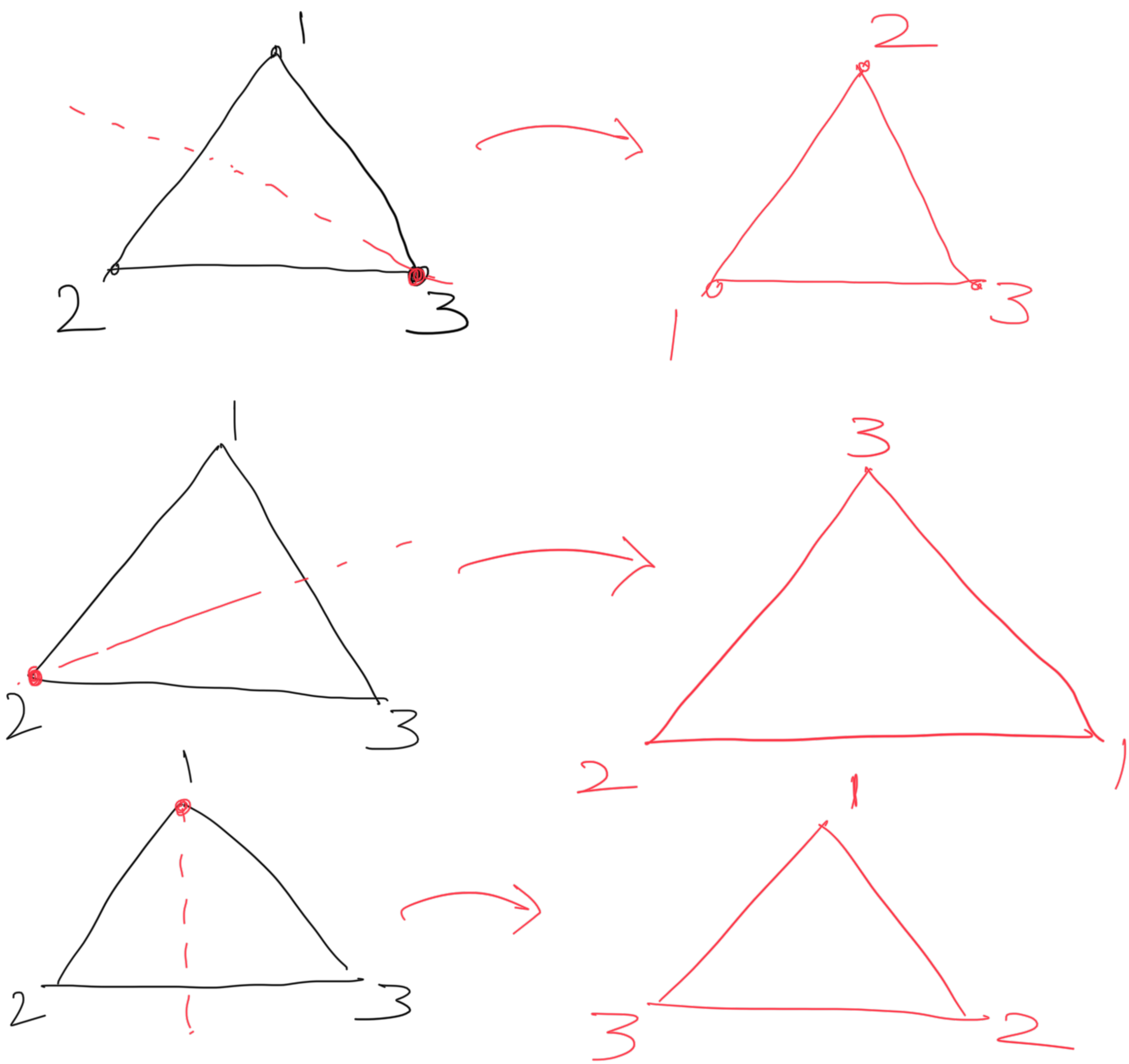
1. Rotations
2. Reflections

Rotations





Reflections



$$\left\{\begin{matrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{matrix}\right\} \quad \left\{\begin{matrix} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2 \end{matrix}\right\}$$

$$\left\{\begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix}\right\} \quad \left\{\begin{matrix} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{matrix}\right\}$$

$$\left\{\begin{matrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{matrix}\right\} \quad \left\{\begin{matrix} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{matrix}\right\}$$

We are constructing maps from $\{1, 2, 3\}$ to itself that are both one-one + onto.

Set of all of these 6 maps, also known as S_3.

$S_n \to$ Set of all one-one + onto maps from $\{1, 2, \dots, n\}$ to itself

$(S_3, \text{Composition of functions})$

$f : \{1,2,3\} \to \{1,2,3\}$

$1 \mapsto 3$
$2 \mapsto 1$
$3 \mapsto 2$

$g : \{1,2,3\} \to \{1,2,3\}$

$1 \mapsto 2$
$2 \mapsto 3$
$3 \mapsto 1$

$f \circ g : \{1, 2, 3\} \to \{1, 2, 3\}$

$1 \mapsto 1$
$2 \mapsto 2$
$3 \mapsto 3$

Exc: Check that $(S_3, \text{Composition})$ is a group.

RINGS

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

$(R, +, \times)$

1. $(R, +)$ is a group, further $m+n = n+m$. (commutativity)

2. $(R, \times)$
   - $\times$ gives closure
   - $\times$ is associative
   - Identity exists

3. Distributivity

$$a \times (b+c) = (a \times b) + (a \times c)$$
$$(b+c) \times a = (b \times a) + (c \times a)$$

Matrices (an example of rings)

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z} \right\}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1-1 & 0+0 \\ 0+0 & 2-1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1\times1 + 1\times3 & \cdot \\ \cdot & \cdot \end{pmatrix}$$

Exc: Check that $M_2(\mathbb{Z})$ is a ring.

More examples: $M_2(\mathbb{Q})$, $M_2(\mathbb{R})$,

$M_2(\mathbb{C})$

$M_n(\ )$

Exc: Check that $M_n(\mathbb{Z})$ is a ring.

Fields

Defn: A field F is a ring such that $(F-\{0\}, \times)$ is a commutative group.

Example: $(\mathbb{Q}, +, \times)$ is a field.

$$\frac{m}{n} \times \frac{n}{m} = 1 = \frac{n}{m} \times \frac{m}{n}$$

Next class: Talk about finite fields, discuss arithmetic on it.

$\mathbb{F}_3$ finite field of 3 elements

$\mathbb{F}_9$ finite field of 9 elements

$$\begin{array}{c} \mathbb{F}_9 \\ 2 \Big| \\ \mathbb{F}_3 \end{array}$$

(field extension of $\mathbb{F}_3$ of degree 2)

$$\begin{array}{c} \mathbb{F}_{p^r} \\ r \Big| \\ \mathbb{F}_p \end{array}$$