Groups :

Def: Let $*$ be a binary operation on a set A. An identity for $*$ is an element e of A satisfying
$$e*a = a*e = a \quad \forall\, a \in A.$$

Ex: If $A = \mathbb{Z}$, $* = +$, $\quad 0*a = a*0 = a \quad \forall\, a \in A.$

Ex: If $A = \mathbb{Z}$, $* = \cdot$, $\quad 1*a = a*1 = a \quad \forall\, a \in A.$

Prop: If $e \in A$ is an identity for A, then e is unique.

Proof: S'pose $\tilde{e} \in A$ is also an identity

$$\left.\begin{aligned} &(1) \quad e*a = a*e = a \quad \forall\, a \in A. \\ &(2) \quad \tilde{e}*a = a*\tilde{e} = a \quad \forall\, a \in A. \end{aligned}\right\}$$

$$= \begin{cases} e*\tilde{e} = \tilde{e} & \text{by } (1) \\ e*\tilde{e} = e & \text{by } (2) \end{cases} \qquad \therefore\ e = \tilde{e}$$

$\square$

Def: Let $*$ be a binary operation on a set A and suppose $*$ has an identity e. If $a \in A$, then an inverse of a is an element $b \in A$ satisfying
$$a*b = b*a = e.$$

Ex: $A = \mathbb{Z}$, $* = +$. $\quad e = 0$

Q: What is the inverse of 4?

Looking for $x \in \mathbb{Z}$ with
$$x*4 = 4*x = e$$
$$x+4 = 4+x = 0$$
$$x = -4$$

Ex: $A = \mathbb{Z}_n$, $* = \cdot$, $e = 1$

Q: What is the inverse of 4?

looking for $x \in \mathbb{Z}_n$ with $x * 4 = 4 * x = e$

$x4 = 4x = 1$

x does not exist!

Def: A <u>group</u> G is a set with a binary operation $*$ having three properties

(1) $*$ is associative

(2) $*$ has an identity e

(3) every element of G has an inverse

<u>Notation</u>: we write x^{-1} to mean the inverse of x.

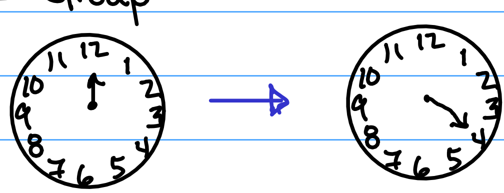
What if $*$ was also commutative?

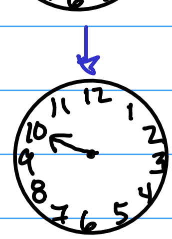
Def: A group G whose binary operation $*$ is commutative is called <u>Abelian</u>.

Why groups?

Groups arise naturally all over in the real world as collections of transformations

Clock Group:





Transformations $= \{1, 2, 3, 4, 5, \dots, 12\}$

In terms of clock geometry $3 + 5 = 8$

$7 + 7 = 2$

$$8+9=5$$

Set is $\{1, 2, \ldots, 12\}$ ← identity

Binary operation is $+_{\text{clock}}$

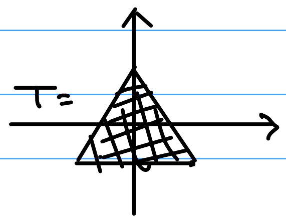
$8+12=8$ for example

$$\boxed{x +_{\text{clock}} y = \begin{cases} x+y, & x+y \leq 12 \\ x+y-12, & x+y>12 \end{cases}}$$

Abelian

inverse of 3 is 9.

Ex: Symmetries of the triangle.



equilateral triangle centered at the origin.

A linear transformation $\mathbb{R}^2 \to \mathbb{R}^2$ is called a <u>symmetry of T</u> if it maps T bijectively onto T.

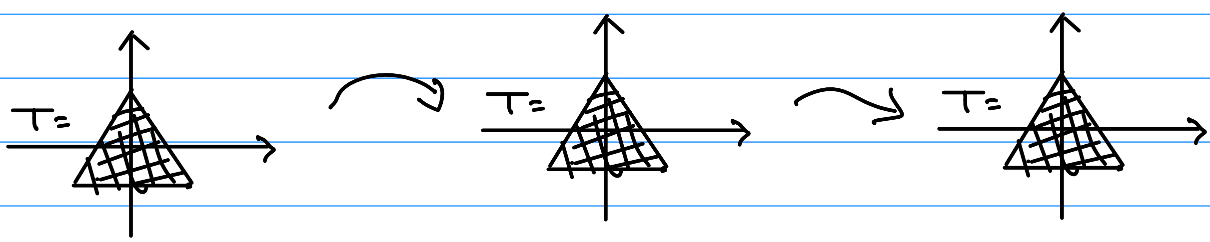
Reflect about y-axis: $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$

Rotate $\frac{2\pi}{3}$ radians: $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ = counter-clockwise rotation by θ radians

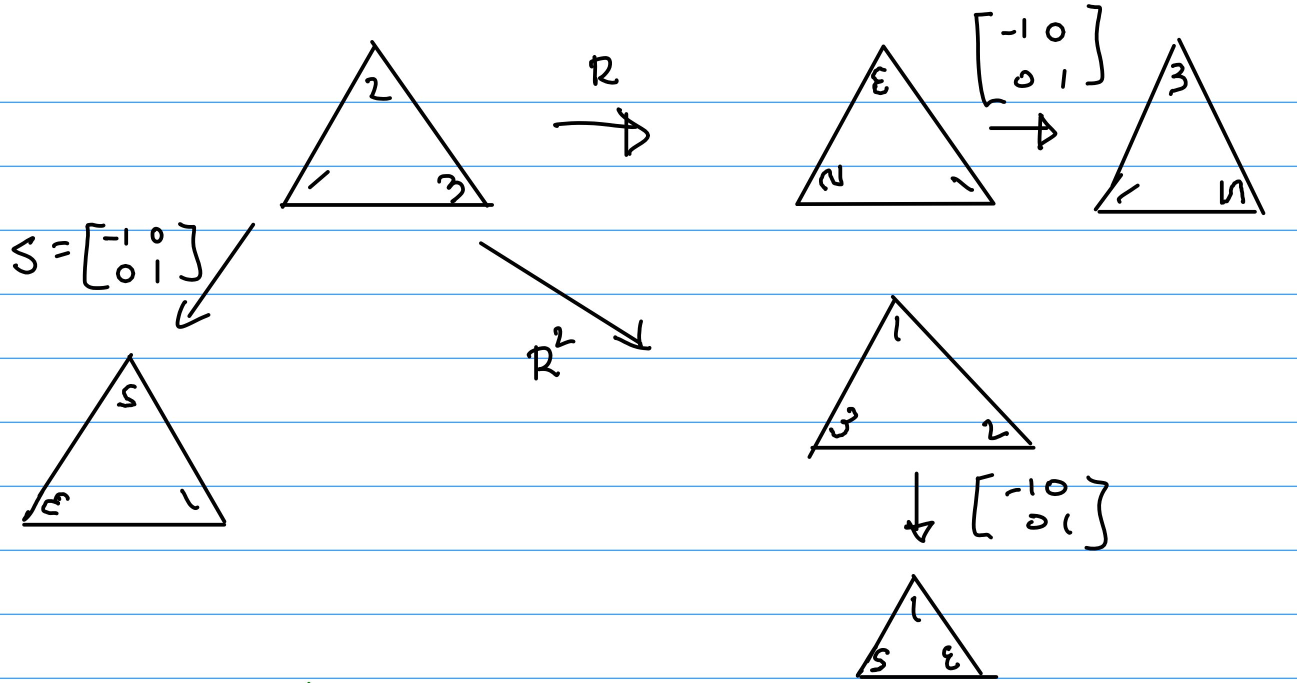
(or a multiple)

$$\begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \quad \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\theta = \frac{2\pi}{3} \qquad \theta = \frac{4\pi}{3} \qquad \theta = \frac{6\pi}{3}$$



Multiples of the matrices above are also symmetries



$S^{-1} = S$ because $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Collection of symmetries : $\{I, S, R, R^2, SR, SR^2\}$

This forms a group with 6 elements (dihedral group D_3)

	I	S	R	R^2	SR	SR^2
I						
S			$\begin{bmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}$			
R						
R^2						
SR						
SR^2						

Try filling this in at home!

$$R = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$$SR \neq RS$$
$$RS = SR^2$$

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

The group $\mathbb{Z}_n$

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

binary operation $+_n$ = modular addition

Ex: $3 +_7 5 = 1$
$2 +_4 9 = 3$

Def: $a +_n b$ = remainder of $\frac{a+b}{n}$.

Theorem $\mathbb{Z}_n$ is a group with the binary operation $+_n$

Proof: NTS
- associative ★
- identity
- inverses

$a \in \mathbb{Z}_n$, $a +_n 0 = a = 0 +_n a$
Thus the identity is 0

$a \in \mathbb{Z}_n$, $a \neq 0$. Then

$a +_n (n-a)$ = remainder of $\frac{n-a+a}{n}$
= remainder of $\frac{n}{n}$ $= 0$. ✓