Lecture 1

Instructor: Dinakar Muthiah

ES 3141 dmuthiah@math.toronto.edu

Office hour W 3pm-5pm

Read every word in the textbook.

What is a symmetry?

A symmetry is sth. remains the same after a specific transformation.

There are 2 symmetries of 

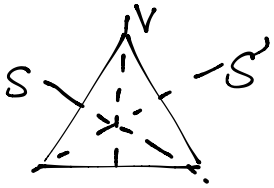
{do nothing, reflect about the y-axis}

Dihedral group of symmetries

D_n = {symmetries of a regular n-sided polygon}

D_3 = {symmetries of regular triangle (aka an equalatral triangle}

D_4 = {symmetries of a square}



n=3

Also, there is rotational symmetry

R_{120} = rotate 120° counter-clockwise

R_0 = do nothing

R_{240} = ...

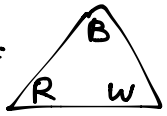
$R_{120} \circ Flip_V$
$=$
$R_{120} Flip_V$

The convention of composition of functions ~~doesn't hold~~ holds here.

$R_{120} Flip_V = Flip_S$

$R_{120} Flip_V$ 

$= R_{120}$ 

$=$ 

$= Flip_S$ 

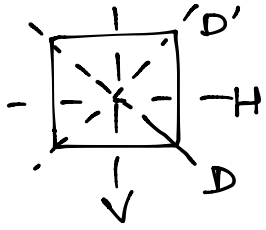
	R_0	R_{120}	R_{240}	V	S	S'
R_0	R_0	R_{120}	R_{240}	V	S	S'
R_{120}	R_{120}	R_{240}	R_0	S	S'	V
R_{240}	R_{240}	R_0	R_{120}	S'	V	S
V	V	S'	S	R_0	R_{240}	R_{120}
S	S	V	S'	R_{120}	R_0	R_{240}
S'	S'	S	V	R_{240}	R_{120}	R_0

Cayley Table
(operation table)
(multiplication table)

Symmetries do not commute in general.
(not commutative)

$VS \neq SV$
$\|$ $\|$
R_{240} R_{120}

For D_4, exercise: understand the discussion of D_4 in the txt



R_0 R_{90} R_{180} R_{270}

Theorem: D_n will have $2n$ elements.

Proof:

Under any given symmetry, v_1 can assume n-different positions.

_____, v_2 can assume 2 different positions once v_1 has been fixed.

Once the locations $v_1 + v_2$ are fixed, the entire polygon is fixed.

So we have $2n$ possible symmetries ∎

Definition of a group

Motivation: Given a set of symmetries (transformations of an object that leave the object unchanged.
What can we say about these symmetries.
- "Do nothing" is always a symmetry.
- Symmetries are invertible transformations
- You multiply symmetries (compose the transformations)
  $f \circ (g \circ h) = (f \circ g) \circ h$ (associativity property)

Def: A group is a set G with a binary multiplication operation. If $a \in G$, $b \in G$, then we write ab for the result of "a times b": applying the binary multiplication to a AND b.

Moreover, the multiplication, should satisfy the following properties:

① Identity: There is an element $e \in G$ s.t. $ae = a$ for all $a \in G$
$ea = a$
("doing nothing element")

② Inverses For all $a \in G$, there exists $b \in G$, s.t. $ab = e = ba$

③ Associativity: For all $a, b, c \in G$, $(ab)c = a(bc)$

Examples

- $\mathbb{Z}$ (integers) is a group under $+$
  - identity for $(\mathbb{Z}, +)$ is 0,
  - the inverse of n is $-n$.
  - associativity is automatic

- $\mathbb{Q}$ — — · +
  - ··· 0
  - ·· · $-r$
  - ··· we know

$\{1, -1, i, -i\} \subseteq \mathbb{C}$ → complex under multiplication.

identity: 1
inverses $(1)^{-1} = 1$
$(-1)^{-1} = -1$
$(i)^{-1} = -i$
$(-i)^{-1} = i$

nxm matrices ...

- $GL(n, \mathbb{R})$ = { invertible nxn matrices } under matrix multiplication
  general linear group = {nxn matrices $A \mid \det(A) \neq 0$}

Ex: $GL(2, \mathbb{R})$ under matrix multiplication
$= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0 \right\}$

identity: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

inverses: In your linear algebra class, you learned how to invert matrices

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

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \stackrel{?}{=} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\frac{1}{ad-bc} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

In $GL(2,\mathbb{R})$ (and $GL(n,\mathbb{R})$ in general)
$AB \neq BA$ (multiplication of matrices is not commutative)

Practice Problems
Ch 1: 3, 4 – 9
Ch 2: 2, 5, 6, 7

Non-examples of groups
$\mathbb{Z}$ under $\times$
(there are no inverses in general)

$\mathbb{Q}, \mathbb{R}$ under $\times$ (0 doesn't have an inverse)

$\mathbb{R} \setminus \{0\}$ under $\times$ is a group identity $= 1$
inverse of $a = \frac{1}{a}$

All $n \times n$
– Matrices under multiplication
– There are not always inverses.

Important examples
$\mathbb{Z}_n$ = integers modulo n
$= \{0, 1, 2, \cdots, n-1\}$

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ $\quad 5 \equiv 0 \bmod 5$

Fact: $\mathbb{Z}_n$ is a group under addition
identity: 0
inverse of k is $n-k$
associativity: is just the associativity of $\mathbb{Z}$

$\mathbb{Z}_n$ is not ..... multiplication
identity: 1
associative: yes.
not every element of $\mathbb{Z}_n$ is invertible

Which elements of $\mathbb{Z}_6$ are invertible.
$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$U(6) = \{$invertible elements of $\mathbb{Z}_6$ under multiplication$\}$
$= \{1, 5\}$

Later we will see that $U(6)$ is "isomorphic" to symmetries of ☺

In general, we will define $U(n) = \{$invertible elements of $\mathbb{Z}_n$ under multiplication$\}$.

If n & m are positive integers, $\gcd(m,n)$ = the largest positive integer k that divides both n & m.

Def: n & m are relatively prime if $\gcd(m,n)=1$.

Prop: (Read in chapter 0)
If n & m are integers and $\gcd(m,n)=1$, then we can find k & l integers so that $kn+lm=1$.
Conversely, if n & m are integers (but we know nothing about their gcd) but we can find k & l integers s.t. $kn+lm=1$, then we can conclude that $\gcd(n,m)=1$

Theorem: $U(n)=\{a\in\mathbb{Z}_n \text{ s.t. } \gcd(a,n)=1\}$
Proof: Sps $a\in U(n)$. Thus $a\in\mathbb{Z}_n$ and a is invertible.
This means $\exists\ b\in\mathbb{Z}_n$ s.t. $ab\equiv 1 \bmod n$
but this means $ab-1$ is divisible by n. This means $\exists\ k\in\mathbb{Z}$ s.t. $ab-1=kn$.
We rearrange this to $ab-kn=1$. By the Prop, $\gcd(a,n)=1$.

Now sps $a\in\mathbb{Z}_n$ and $\gcd(a,n)=1$. By the prop we can find integers b and k s.t. $ba+kn=1$
Then we can write $ba-1=-kn$, which implies $ba-1$ is divisible by n.
Thus $ba\equiv 1 \bmod n$. Hence, a is invertible. ∎

Def: We say a group G is Abelian if $\forall\ a\in G$ & $b\in G$, $ab=ba$
We say G is non-Abelian if $\exists\ a\in G$ & $b\in G$ s.t. $ab\neq ba$.

Elementary properties of Groups

Thm 2.1: In a group there is only one identity element.
Proof: Suppose $e'\in G$ is another identity element.
$e=ee'=e'$ ∎

Thm 2.2 Groups have the cancellation property i.e.
Sps $a,b,c\in G$ and $ac=bc$ Then $a=b$

Similarly if $ca=cb$, then $a=b$.
Pf: Assume $ac=bc$. Let d be an inverse of c. (in particular $cd=e$)
Then $(ac)d=(bc)d$
$\Updownarrow$ $\Updownarrow$
$a(cd)=b(cd) \Rightarrow ae=be \Leftrightarrow a=b$ ∎

For $\mathbb{Z}_6$ we know $2\neq 0$.
$2\cdot 3=0$
$2\cdot 0=0$ here we DO NOT have the cancellation property.

Thm 2.3
Uniqueness of inverse. $\forall\ a\in G, \exists$ a unique inverse $b\in G$ s.t. $ab=ba=e$.

Proof: Sps $a\in G$, and suppose $b+b'\in G$ are inverses to a. Then $ab=e$ and $ab'=e$. In particular, $ab=ab'$. By the cancellation property, $b=b'$. ∎

Thm 2.4
"Socks — Shoes thm"
For $a \& b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

Proof: We just need to check that $b^{-1}a^{-1}$ is an inverse to ab.
So $abb^{-1}a^{-1} = e$. Similarly $b^{-1}a^{-1}ab = e$ ∎