Lecture - 2

We already saw some examples of groups. So it's time to see the formal definition. Recall that a **binary operation** on a set takes two elements from the set and gives another element in the set.

Definition A set G with a binary operation '$\cdot$' is called a group if

(1) For any $a, b, c \in G$, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
[i.e, '$\cdot$' is associative]

(2) There exists an element $e \in G$ called the identity, such that $a\cdot e = e\cdot a = a$, for all $a \in G$.

(3) For all $a \in G$ there exists an element $a^{-1} \in G$ such that $a^{-1}\cdot a = a\cdot a^{-1} = e$. a^{-1} is called the inverse of a.

Remark :- 1) We are not writing the closure property in the definition because '$\cdot$' is a binary operation so closure is automatically satisfield. However, when asked whether a set is a group or not, be sure to check closure too.

2) We might use the symbol '$\forall$' for 'for all' and '$\exists$' for there exists.

Definition If $a, b \in G$ are two elements in a group G they are said to **commute** if $a \cdot b = b \cdot a$.

If a and b commute $\forall a, b \in G$, we say G is **abelian**. Otherwise, G is called **non-abelian**.

Ques:- When can you say that a group is non-abelian? Have we seen an example of a non-abelian group?

Before looking at more examples, let's see some basic properties of a group.

Proposition 1 (Uniqueness of identity elements)
In a group G, $\exists$ only one identity element.

Proof. Suppose e and f both are identity elements. Since e and f are arbitrary, in order to prove that the identity is unique, we must show that $e = f$.

Now $ef = f$ (as e is identity)

and $ef = e$ (as f is identity)

$\Rightarrow e = f$

$\blacksquare$

Proposition 2 [Inverse of an element is unique]
Every element $a \in G$ has an unique inverse in G.

Proof :- Left as an exercise. $\square$

Proposition 3 [Cancellation holds in a group]
In a group G, the right and left cancellation law hold, i.e., $ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$.

Proof :- Let's prove the left cancellation, leaving the right cancellation as an exercise. Suppose $ab = ac$. Since a has an inverse in G, let's multiply by a^{-1} on both sides to get

$$a^{-1}(ab) = a^{-1}(ac)$$

$$\Rightarrow (a^{-1}a)b = (a^{-1}a)c \qquad \text{[Associative]}$$

$$\Rightarrow eb = ec$$

$$\Rightarrow b = c \qquad \text{[by the definition of } e\text{]}.$$

$\square$

More examples of Groups

Ex 1. Integers modulo n, $\mathbb{Z}_n$.
Recall from MATH 135 that $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ where $[a]$ is an equivalence class (we'll learn about them in more detail) defined by

$[a] = \{ b \in \mathbb{Z} \mid a-b \text{ is divisible by } n \}$

$\mathbb{Z}_n$ is a group under addition in $\mathbb{Z}_n$ (which is not the same as addition in $\mathbb{Z}$).

Recall that in $\mathbb{Z}_n$, $[a]+[b]=[a+b]$. The identity element is $[0]$ and the inverse of any $[a]$ is $[n-a]$.

e.g. Consider $\mathbb{Z}_4 = \{[0],[1],[2],[3]\}$. To see how the operation in group look like, we'll draw a table called the Cayley table (in honour of the mathematician Arthur Cayley).

identity

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

[3] is inverse of [1]

<u>Ex 2</u> The group of units modulo n, $U(n)$

For any $n \in \mathbb{Z}$, the set $U(n)$ is the set of all the elements in $\mathbb{Z}_n$ which have inverses. Again, recall from MATH 135 that $a \in \mathbb{Z}_n$ has an inverse if and only if $\gcd(a,n)=1$.

Since we are collecting only those, elements in $\mathbb{Z}_n$, which have inverses, so we have that $U(n)$ is a group under multiplication in $\mathbb{Z}_n$. The identity is [1].

e.g. consider U(12). The integers a between 0 and 12 which are coprime to 12 are 1, 5, 7, 11, so $U(12) = \{1, 5, 7, 11\}$. The Cayley table for U(12) is as follows :-

·	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

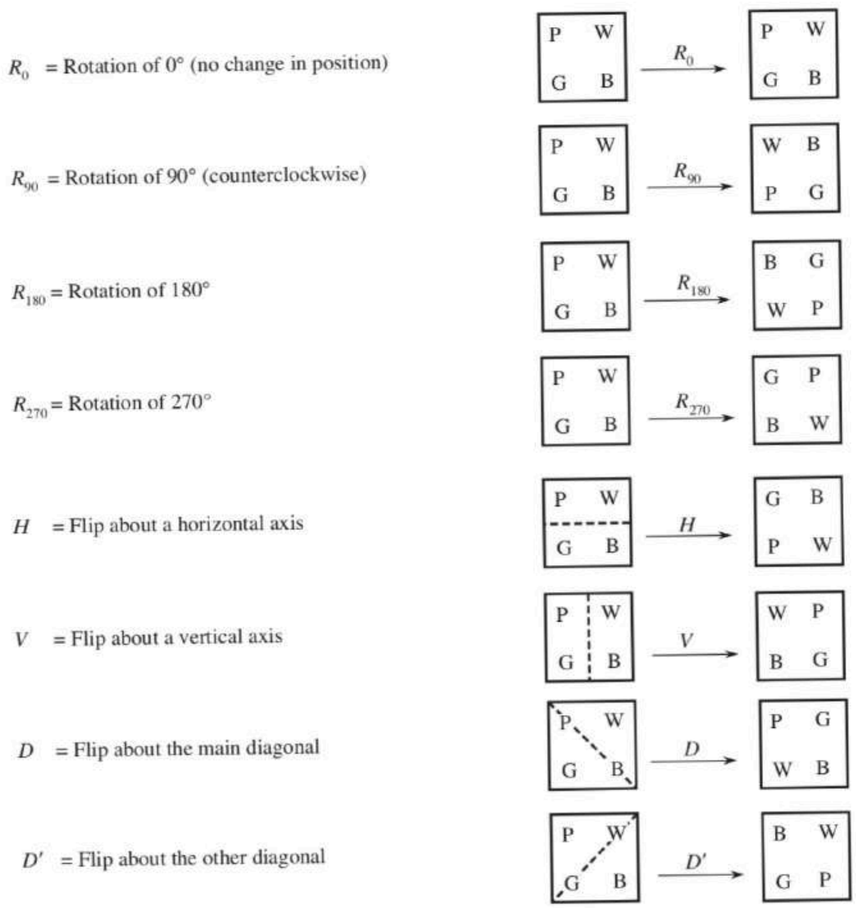
Ques:- 1) What is the inverse of 5 in U(12)?

2) What is the set U(5)? Can you generalize it?

Ex3 Dihedral Groups

Let's introduce a very important set of examples called the dihedral group D_n, $\forall\, n \geq 3$. D_n, by definition is the group of symmetries of a regular n-gon, where symmetry means an operation which might change the individual places in an n-gon but doesn't change the overall shape.

For simplicity, let's under the group D_4, which is the group of the symmetries of a square.



Symmetries of a square
Credit : Contemporary Abstract Algebra, Joe Gallian

As you can see in the figure, 4 of the symmetries are anti-clockwise rotation by 0°, 90°, 180° and 270° which are denoted by R_0, R_{90}, R_{180}, R_{270} respectively. If you rotate the square by say 360° they you'll get back R_0 and rotation by 540° will give back R_{180}.

The letters on the vertices of the square are only there for visual aid to see which operation is taking place.

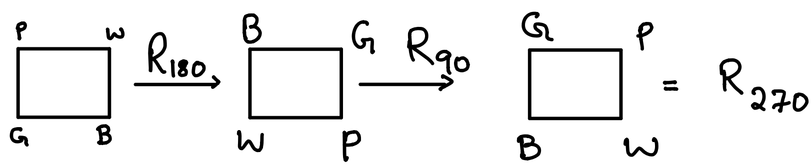
The other symmetries are reflections :- along a vertical axis, horizontal axis, and both the diagonals.

So, we have the set $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

But if D_4 is a group there must be some operation too. This is pretty simple : the operation is composition of symmetries, i.e., if suppose S_1 and S_2 are symmetries then $S_1 S_2$ will be performing S_2 and then performing S_1, i.e., from right to left.

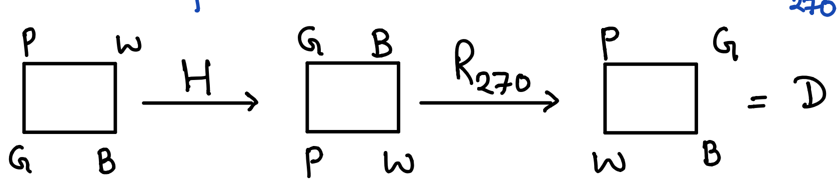
e.g. What is $R_{90} \cdot R_{180}$? We first perform R_{180} and then R_{90}

so



What is $R_{270} \cdot H$?

We first do H and then do R_{270} to it.



So atleast in these cases it seems that the operation is a binary operation, i.e., it is taking two symmetries and producing another symmetry.

But is that always the case? For that we just make the Cayley table for D_4.

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

Cayley table

<u>Exercise</u> :- Understand this Cayley table by doing the operations from figure 1.

Note from the Cayley table that R_0 serves as the identity (the horizontal and vertical rows below R_0 remains unchanged).

For inverses, e.g. inverse of H is H itself (which makes sense geometrically too as two horizontal flips in a row should cancel the effect) and the inverse of R_{90} is R_{270}

(again makes sense geometrically).

Also notice that $R_{270} \cdot H = D$ and $H \cdot R_{270} = D'$

so $R_{270} \cdot H \neq H \cdot R_{270}$ and hence

D_4 is non-abelian.

There is nothing special about the square. We can talk about the dihedral group of any regular polygon. The group of symmetries of a regular n-gon is the group D_n and the operation is again the composition of symmetries.

Exercise Find the Cayley table of D_3. In fact, draw the symmetries of the triangle.