Lecture 3 : Groups

Let A be a set with some "structure."

G = set of permutations of A "preserving the structure".

Then G has the following properties :

1) id_A is in G.

2) f, g in $G \implies g \circ f$ is in G.

3) f in $G \implies f^{-1}$ in G

4) If f, g, h are in G, then

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

Many times, we can understand more about A and its structure if we understand G and its composition rule.

So, we want to understand algebraic objects that "behave like G."

So, how should we define such an object?

Which are the properties of G that matter?

- G is a set
- There is a rule for "combining" two elements of G to get a third element.
- Identity element
- Inverses
- The rule is "associative".

Binary operations

Let S be a set. A binary operation on S is a function

$$* : S \times S \longrightarrow S.$$

Here, $S \times S$ = set of ordered pairs (x, y) where x, y are in S.

The image of (x,y) under $*$ will be written as $x*y$ instead of $*(x,y)$.

<u>Remark</u>: Think of $*$ as a "multiplication rule" on S.

Examples

1) $\mathbb{N}$ - set of natural numbers (i.e. positive integers).

Consider the function

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$(x, y) \longmapsto x + y.$$

This is a binary operation.

2) Similary, addition defines binary operations on

$\mathbb{Z}$ – set of integers

$\mathbb{Q}$ – set of rational numbers

$\mathbb{R}$ – set of real numbers

3) Let S be a set.

Let F = set of functions $S \to S$.

Then composition gives us a binary operation on S.

$(f, g) \longmapsto f \circ g$.

Associativity

Let S be a set with a binary operation $*$. We say that $*$ is associative if $a*(b*c) = (a*b)*c$ for any a, b, c in S.

We have already seen examples of associative binary operations.

<u>A non-example</u>

Consider the binary operation on $\mathbb{Z}$ defined by

$$(a,b) \longmapsto a-b$$

Then, if a, b, c are in $\mathbb{Z}$

$(a-b)-c = a-b-c$,

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

So, this operation is <u>not</u> associative.

Groups

A group consists of a set G with a given binary operation $*: G \times G \to G$ such that:

(1) There exists an element 1_G in G such that $1_G * f = f * 1_G = f$ for all f in G.

2) For any f in G, there exists an element f^{-1} such that $f * f^{-1} = f^{-1} * f = 1_G$

3) $*$ is associative.

We write the group as $(G, *)$.

But we may just write G if $*$ is understood from context.

Remarks

1) We had earlier listed <u>four</u> properties of symmetries. The property which stated that "if f, g are in G, so is $g \circ f$" does not need to be written explicitly as it is built into the notion of <u>binary operation.</u>

2) The notation for the binary, for the identity element and for inverses may vary.

e.g. In $\mathbb{Z}$, the binary operation is "$+$" and the identity element is 0.

3) Sometimes we may not use an explicit symbol for the binary operation.

For example, for multiplication in $\mathbb{Z}$ or $\mathbb{Q}$, we just write ab instead of $a \times b$.

Examples

1) Let S be any set. Then, $\mathrm{Perm}(S)$ is a group, the binary operation being composition

2) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are groups for the binary operation $+$.

We write these as $(\mathbb{Z}, +)$,

$(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ to make it clear that we are talking about the binary operation $+$, and not $\times$.

3) $\mathbb{N}$ is <u>not</u> a group for $+$ as inverses do not exist.

4) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ have another binary operation $\times$. However, these are not groups for this operation as inverses do not exist.

5) Let $\mathbb{R}^\times$ = set of non-zero real numbers.

Then $(\mathbb{R}^\times, \times)$ is a group.

Similarly, if $\mathbb{Q}^\times$ is the set of non-zero rational numbers, $(\mathbb{Q}^\times, \times)$ is a group.

6) Let A be any set with a "distance function".
Then, the set of isometries of A is a group.

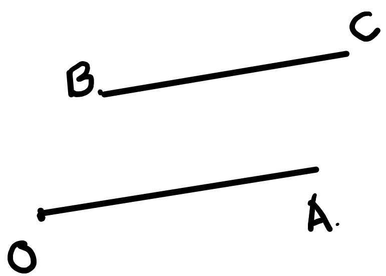
7) The set of isometries of the regular n-gon is called the dihedral group of order $2n$. (Written as D_n..)

8) In the plane $\mathcal{P}$, fix a point O. Given points A, B in $\mathcal{P}$, we construct a third point C as follows:

- If $A = O$, set $C = B$.
- If $A \neq O$, define C to be the unique point such that

the ray $\overrightarrow{BC}$ points in the same direction as $\overrightarrow{OA}$ and

$\text{dist}(O, A) = \text{dist}(B, C)$.



So, C is chosen such that OACB is a parallelogram.

We define $A+B$ to be C.
Then, $(\mathcal{P}, +)$ is a group.
The identity element is O.
If A is any element of $\mathcal{P}$,
its inverse is the unique point
A' such that O is the
midpoint of AA'.