



NPTEL

NPTEL ONLINE COURSE

Discrete Mathematics

Functions

Advanced Topics

Formal definition of a Group

Discrete Mathematics

Advanced Topics

Formal definition of a Group

Prof. S. R. S. Iyengar
Department of Computer Science
IIT Ropar



Prof S.R.S. Iyengar

Department of Computer Science

IIT Ropar

You are now motivated to see an abstract set like that of my lab. Let us define this formulae. A set S with an operation star is called a group if it satisfies the following four properties. The first property is for every element X and Y in S $X * Y$ should also belong to S .

Do you think it's the same as what I said in the first property of my lab?

Second property is for every X, Y, Z in S $X * (Y * Z)$ should be equal to $(X * Y) * Z$ as you would have observed the $*$ here means mix the chemicals X and Y or add two numbers or multiply two numbers. It could be anything you see. Anything absolutely.

Third property is there exists an element E in S such that for every element X in S $X * E$ is same as X . We also actually write. $E * X$ is also X . $X * E$ and $E * X$ is also X . this may not be true. When you multiply A with B it may not always be equal to multiplying B with A . You see when you take matrices you know this. When you multiply A and B you might get something. When you multiply B and A you may get something else. In fact, sometimes A into B of two matrices A and B is possible B into A may not even be possible. Think about it. There are many such examples.

A set S with an operation $*$, is called a Group,
if it satisfies the following properties:

- ✓ $\forall x, y \in S, x * y \in S$. - Closure
- ✓ $\forall x, y, z \in S, x * (y * z) = (x * y) * z$ - Associative
- ✓ $\exists e \in S$, such that $x * e = x = e * x$ - Identity
- ✓ $\forall x \in S, \exists x' \in S$ such that $x * x' = e$ - Inverse

GROUP

Okay. Fourth property what was it? Let us try to translate it. For every chemical there is a another chemical X' – so that X one mixed with X' – gives me the universal chemical E . So that translated look something like this. For every X in S there exists an X' – in S such that $X * X'$ – is my E from the previous property. If S is such that with the $*$ operation if S satisfies these four properties, one, two, three and four, what are they? Closure, associative, identity and inverse then S is called a group, a mathematical group. I prefixed the word mathematical just to make you realize that it's not the same group from the English dictionary. This is called a group in mathematics. Okay.

Let us see some nice examples. Some obvious examples. And not so obvious examples.