



**NPTEL**

**NPTEL ONLINE COURSE**

Discrete Mathematics

Functions

Advanced Topics

# Discrete Mathematics

## Advanced Topics

Introduction to Group Theory

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



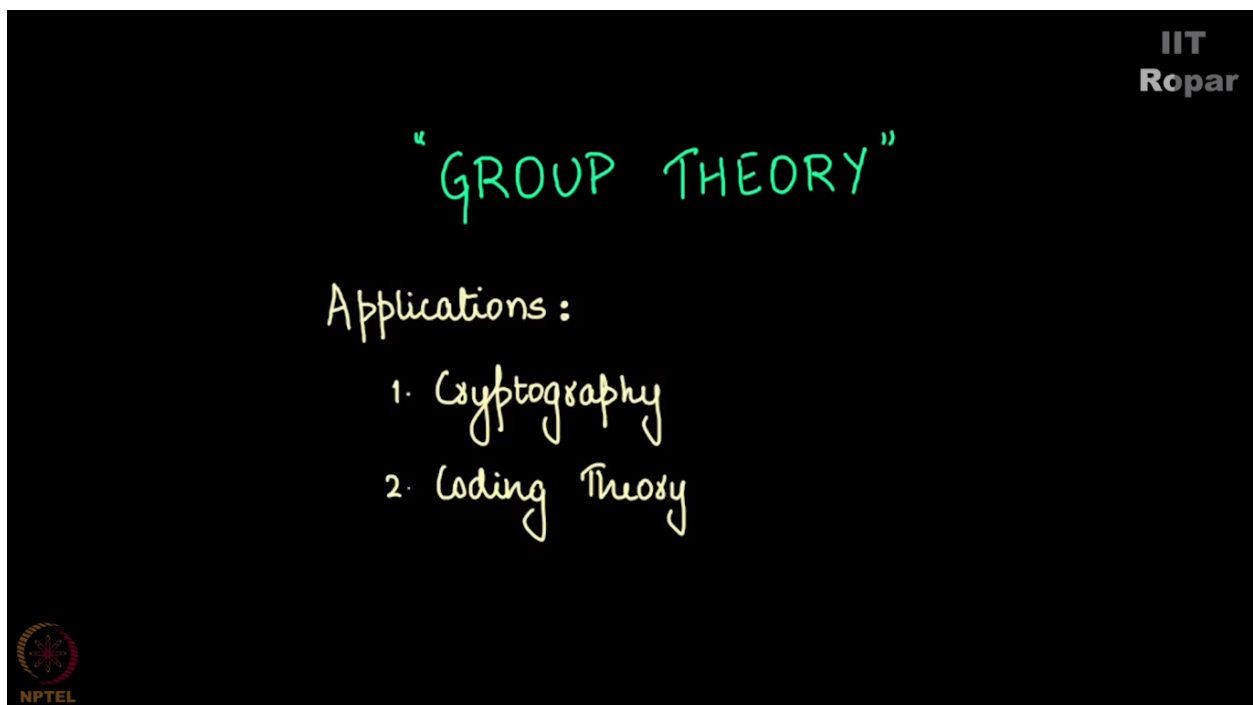
## Introduction to Group Theory

Prof S.R.S. Iyengar

Department of Computer Science

IIT Ropar

We are now going to introduce you all to what is called the group theory. This is one of the most abstract topics we have discussed so far. The reason why this is seen as an abstract topic is mainly because of the way it is taught. It is taught in a way that teacher seldom teach the applications but teach only the abstraction part. And we helplessly are going to do the same for a simple reason that you will be taught this as a motivational concept which will actually be applied in areas such as cryptography coding theory in computer science.



So a computer scientist should know the definition of group theory and you will see its application in places such as as I said cryptography and coding theory. So we will just spend a few minutes for completeness sake.

Imagine I was a chemist and I had this big lab. And I have studied many chemicals let's say some 100 chemicals. I know this chemicals in and out. Now my laboratory satisfies the following four properties. Property number one. You take any two chemicals out of these 100 chemicals that I have studied that are there in my laboratory and mix them. You probably will get a new

chemical. It's always true. You mix some two chemicals mostly you will get something new. And that new chemical is again one of these 100 chemicals in my laboratory. Then I say my laboratory is closed. My laboratory is closed I don't mean the shop is closed closed by closed I mean we don't go outside the lab. The chemical thus formed is not something that I have not studied. This is something that I have already studied. To paraphrase any two chemicals in my laboratory are such that if you mix them the resultant chemical that you are going to get is back again in the lab. Such a property is called the closure property. So while I say my lab satisfied the closure property.


Second property is what is called the associative property which I am going to explain now. Take a chemical. Add that to another chemical. The resultant chemical is chemical AB when added when A is added to B you will get AB let's say. And this resultant chemical AB is further added to chemical C. Whatever you get make a note of it. Now that chemical will be the same as you adding B and C and then adding A to B and C. A to BC rather whatever you get is the same.

Now this is true of addition in general. You see A plus of B plus C is same as A plus B of plus C. this may not really be true with chemicals but my lab is satisfying this. Whenever it satisfies this it is called associative properties being satisfied.

IIT  
Ropar

Imagine I am a chemist, studying 100 chemicals.  
Laboratory satisfies the following properties:

1. Chemical A + Chemical B  $\rightarrow$  Chemical X Already studied  
 - Laboratory is closed.
2.  $(AB) + \text{Chemical C} \simeq A + (BC)$   
same as  
 - Associative property  
 $a + (b + c) = (a + b) + c$



Third property. I have a chemical I call that the universal chemical which one mixed with any other chemical doesn't change the resultant chemical. A chemical E when mixed with the chemical X will always give you X. Such a chemical is called an identity chemical. And if you have such a entity in your lab then you say your lab also satisfies what is called the identity law. You see numbers 0 acts like that. When you add 0 to any number it gives you the same number.

1 also acts like that when the operation is multiplication. 1 when multiplied by any number gives you the same number.

Now coming to the last property. The inverse law. By that it means you saw this identity chemical that I was talking about, the chemical E so inverse law states take any chemical X you can always find another chemical in my lab in my very lab, X – such that when you mix X with X – you will get back E. So let me summarize.

I have some 100 chemicals in my laboratory. And my laboratory satisfies this the following four properties. Property one. Take any two chemicals. Mix them. That is back again in the same laboratory.

Take chemicals A, B, C and mix them in this order. Firstly mix A and B the resultant AB mix it with C. this will be same as you taking A and mixing it with the resultant of B and C because A added to BC. These two will be the same. Then we call it associative law.

Third one is there is always this chemical in my laboratory there is this chemical in my laboratory which when mixed with any chemical of your choice namely X E when mixed with X will give you X always. That's called the identity law.

Now finally there is what is called the inverse law which states give me any chemical X you can always find a chemical X – such that X mixed with X – will always give you this identity E of the previous property. This sounds very complicated. Sounds what are we even doing. So I will give you one marvellous observation one can make if something satisfied these four properties.

IIT  
Ropar

Properties:

1.  $A + B \rightarrow C$
2.  $(A + B) + C$  same as  $A + (B + C)$
3.  $E + X \rightarrow X$
4.  $X + X' \rightarrow E$

NPTEL

So basically I am saying that my lab satisfies these properties. Anything in this universe which satisfies these four properties will satisfy tons of properties. So this structure with four properties

satisfied occurs many at times in scientific studies. So people observe the application of these four laws in physics, in chemistry, of course in mathematics and also in computer science because of which we are studying this and such an identity is called a group the word group as far as English dictionary is concerned is a bunch of people or a bunch of entities but for mathematicians the word group means that set that satisfies these four properties with respect to some operation. What does an operation mean? What is the set here? Set here is 100 chemicals. Operation here means mixing two chemicals. Whenever these four properties are satisfied there are tons of other properties that it satisfies. We will see one startling observation about our lab in the next clip.