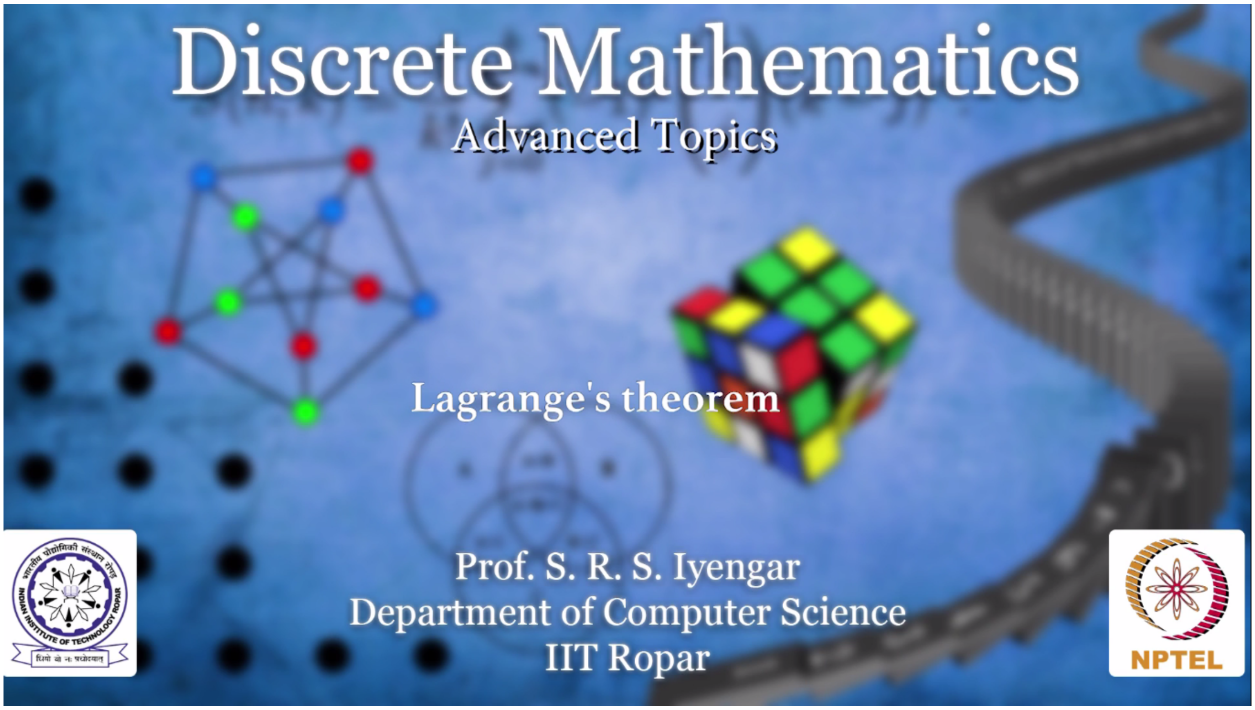
NPTEL

NPTEL ONLINE COURSE

Discrete Mathematics

Functions

Advanced Topics



Discrete Mathematics

Advanced Topics

Lagrange's theorem

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

Lagrange's theorem

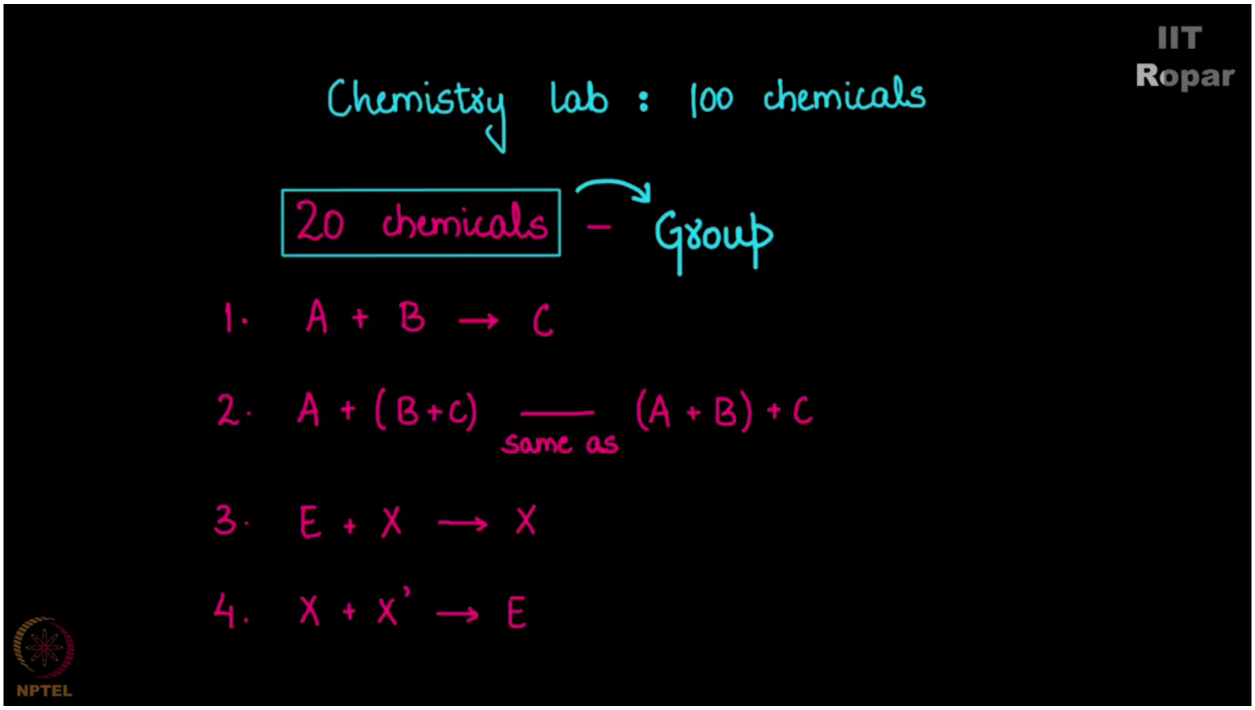
Prof S.R.S. Iyengar

Department of Computer Science

IIT Ropar

Let's get back to the chemistry lab example. You see I had 100 chemicals that satisfies these four properties. You now saw just now before this clip, the definition of subgroup was presented to you. How does that translate to my chemistry lab? Given my 100 chemicals there are these 20 chemicals in my lab I have observed it which satisfies these four properties. What do I mean by that? Property number 1. If you call this a sub-lab 20 chemicals if you take any two chemicals within these 20 chemicals if you mix them you will be back again in the same 20 chemical set. It takes some time. Think about it.

The previous definition of subgroup that our friend presented I am explaining the analogy to you. If you have such a sub-lab satisfying these four properties then it's a lab in itself. It satisfies these four properties and hence it is another group so there are many examples of a group which has a subset which is also a group. What is so interesting about it? Now this is one of the most celebrated results.



Chemistry lab : 100 chemicals

$\boxed{\text{20 chemicals}}$ – Group

1. $A + B \rightarrow C$

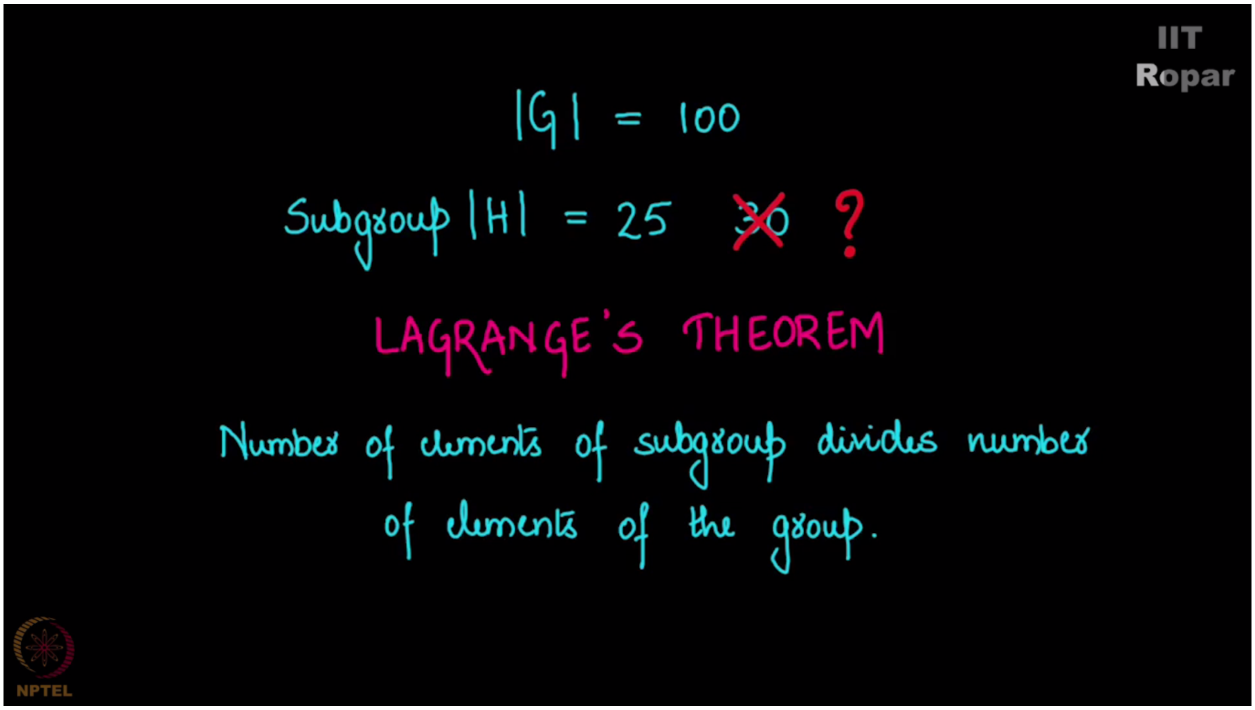
2. $A + (B+C) \underset{\text{same as}}{\underline{\qquad}} (A + B) + C$

3. $E + X \rightarrow X$

4. $X + X' \rightarrow E$

If you have a group with 100 elements and another subgroup of this group then the number of elements of that subgroup should always divide the number of elements of this group. You have a group G with 100 elements. Then the subgroup should have some 50 elements or 20 elements or 25 elements. You cannot have a subgroup with 30 elements. Why not? This is called the Lagrange's theorem which states that the number of elements in the subgroup always divided the number of elements of the group. A celebrated theorem and highly applied in computer science.

So you must at least remember the statement of this theorem the proof of the theorem is not very difficult. In fact it's very interesting but we are skipping this in the interest of time and syllabus. Not even time I think it will be slightly heavy if we start discussing the technical aspects of group theory. So we leave it here. We just state the theorem. And we expect you – expect that you remember this theorem. Theorem is very simple. If you have a subgroup the number of elements in the subgroup will divide the number of elements in the group. I will tell you a very interesting result here.



$|G| = 100$

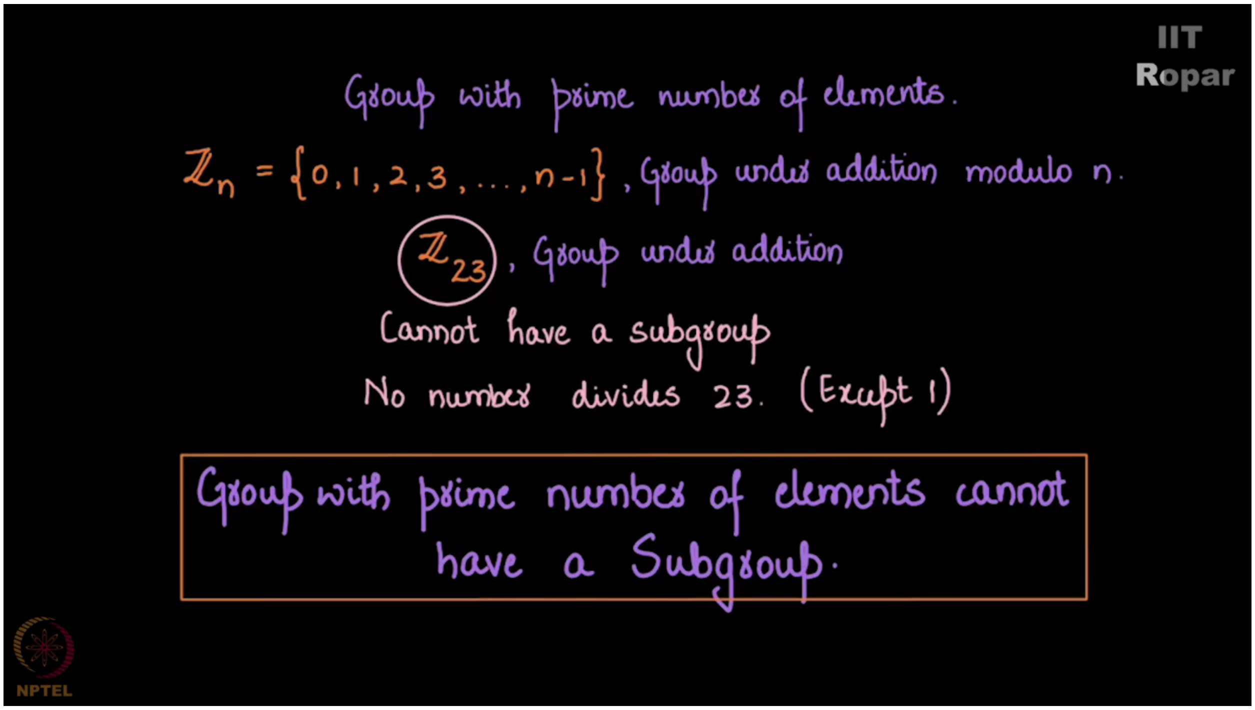
Subgroup $|H| = 25$ ~~30~~ ?

LAGRANGE'S THEOREM

Number of elements of subgroup divides number of elements of the group.

Take a group with prime number of elements. We discussed Zn a while before which is element 0, 1, 2, 3, up to n minus 1 and this forms a group under addition modulo n. If you take Zp instead of Zn it of course forms a group and it has p elements where p is a prime number. So let's say we take Z23 it has 23 elements and forms a group under addition. This cannot have any subgroup. Why is that? If it had some subgroup then that number of elements in the subgroup should divide the number of elements in this group which is 23. There is no such number. Think about it expect for 1 of course.

So a group with prime number of elements cannot have a subgroup. Now how cute is this result. You see you prove you say something as simple as Lagrange's theorem and look at its consequence. The consequence is that if a group has prime elements it cannot have any subgroup. So the whole of group theory is full of such results that are consequences of some theorems and you will be expected to know a few of these if you start studying cryptography which is about the science of secrecy or a subject called coding theory which is the science of communication and information. It's also called the information theory. It's about understanding what one means by information. How can we send and receive information. You might study these subjects as elective in computer science so you must be aware of what is a group before starting to study these two subjects.



Group with prime number of elements.

$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$, Group under addition modulo n.

$\mathbb{Z}_{23}$, Group under addition

Cannot have a subgroup

No number divides 23. (Except 1)

Group with prime number of elements cannot have a Subgroup.

So in our course in discrete mathematics we quickly introduced you to what is group theory but group theory please note is a big ocean. A very big ocean. It is one part of what is called abstract algebra. And you are expected to know only this much whatever we have taught.