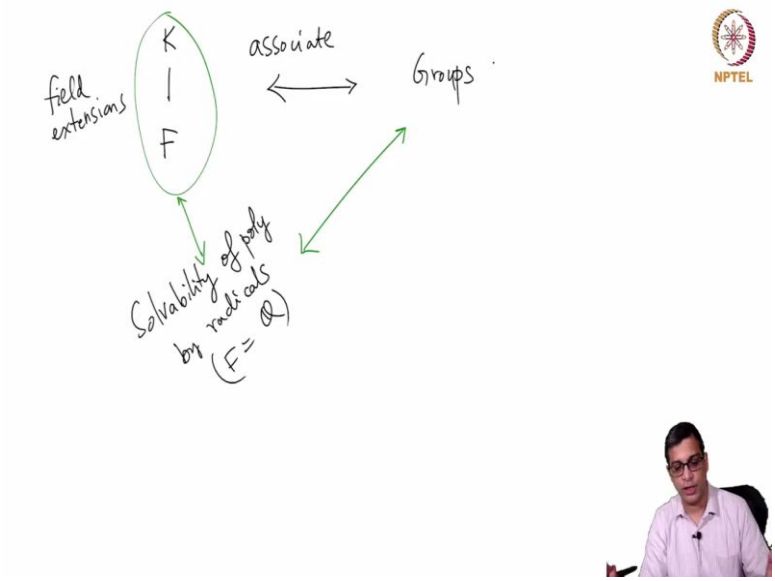
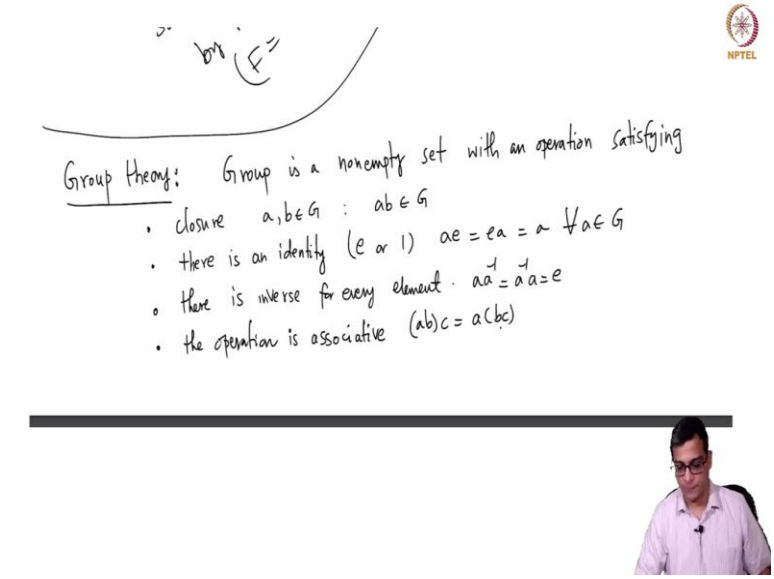
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Review of Group Theory

(Refer Slide Time: 00:14)



Welcome back to the course. In the last video, I introduced the basic ideas of Galois theory, what motivated Galois and what kind of results that he was looking for. So, now we are going to start revision of the basic topics. As I said, we need basics of Group theory, Ring theory and Field theory.

(Refer Slide Time: 00:34)



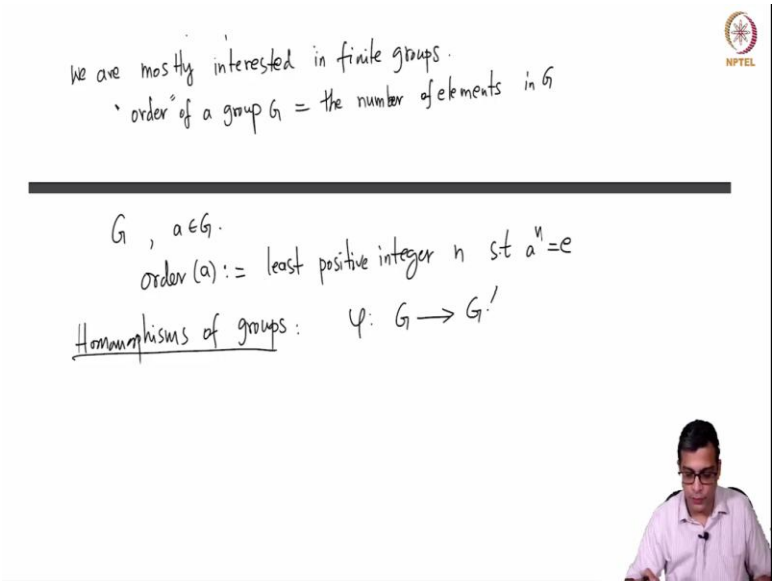
So, the goal here in the next two three videos is to recall the basic notions of these prerequisites, this is not certainly going to be a detailed revision, I only want to introduce the key concepts, key terms and key results that we use. And without going into the proofs or any detailed explanations. And you if you are comfortable with all these, it is perfectly good, you can proceed with the course otherwise, I suggest that you use my previous course or recall these topics from any standard book on algebra, including the main reference for us, which is Michael Artin's algebra.

So, in this video, today, we are going to recall the notions of group theory that we use constantly throughout the course. And in fact, as I mentioned last time, Galois was the person who developed Group theory as we learn today, and this was required when he started solving this problem of solubility of quintics. So we all know what are groups. So group is a set, non empty set with 1 operation, with an operation satisfying some properties.

We will recall Rings later, and rings of two operations. Group has only 1 operation satisfying closure, which is really saying that it is a binary operation on the group. So, we typically denote the very, we typically use multiplicative notation for an arbitrary group unless we know it is an Abelian group, in which case we use an additive notation. So, for two elements of a group their product is, there is an identity which is denoted by e or 1 depending on the context, but it simply means that ae is equal to a for all a in G, there is inverse for every element.

So, we usually denote inverse by a inverse a power minus 1 like this. And the operation is associative. So this is of course familiar to all of you, but I thought I will just quickly recall the definition. So, we really mean that ab times c is same as a times bc

(Refer Slide Time: 03:13)

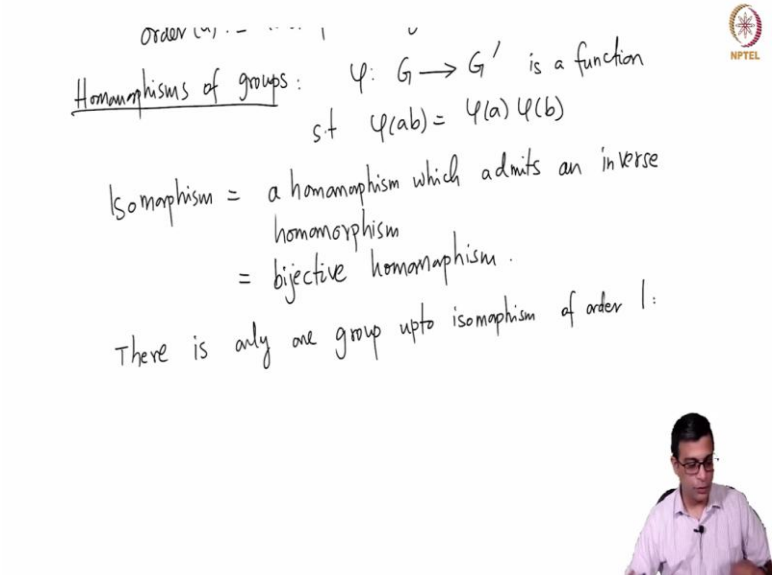


So, we are going to be mostly interested in finite groups. Because these are the groups that arise in Galois theory that we study in this course, so, these are finite groups, that means they have finitely many elements, group is always a nonempty set. So, the cardinality of the group which is order of the group, which is called the order of a group G is equal to simply the number of elements in that group. So, the size of that group.

So, we are going to be interested in finite groups that means, there are finitely many elements. And so, Galois studied, the main group that he was interested in is a symmetry group because he was interested in roots of a given polynomial. So, before we get to that, so, let me just start with some of the key terminology that we use, for example, I just recalled order of a group, if you have G a group and an element a in G.

What is order of a? is by definition, the least positive integer n such that a power n is identity and remember because we are going to stick to finite groups this is actually a positive integer. So, this is the order of an element, order of a group or subgroup is the number of elements in that group or subgroup. So, we have also the notion of Homomorphisms which is very important for us, Homomorphisms of groups.

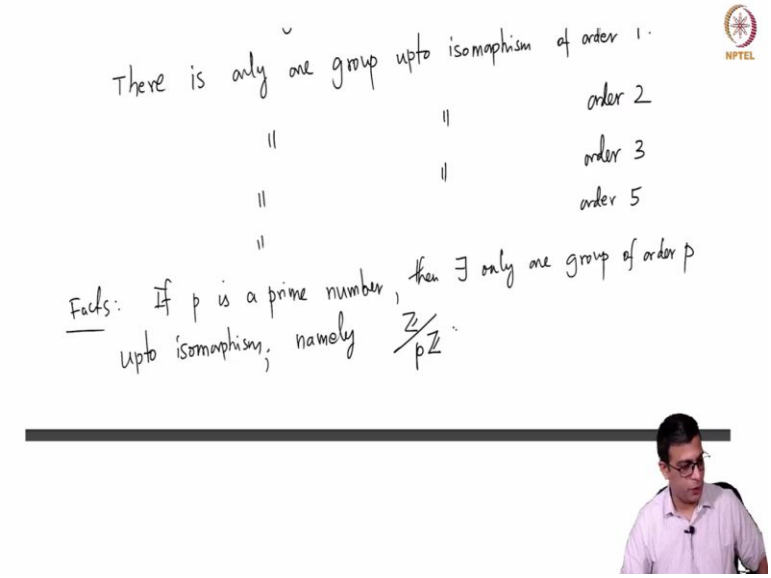
(Refer Slide Time: 05:09)



So, if you have two groups G and G prime, what is a Homomorphism is a function such that phi of ab very simple phi of a equals phi of b. So, the multiplication in G and multiplication in G prime are compatible through this map. So, this is what a homomorphism is. An Isomorphism of groups is simply a by, a homomorphism which admits an inverse homomorphism by which I mean phi from G to G prime is a homo, isomorphism if there is a function from psi from G prime to G which is also a homomorphism such that the compositions, the two compositions are identities on G and G prime respectively and this is actually nothing but by a bijective homomorphism.

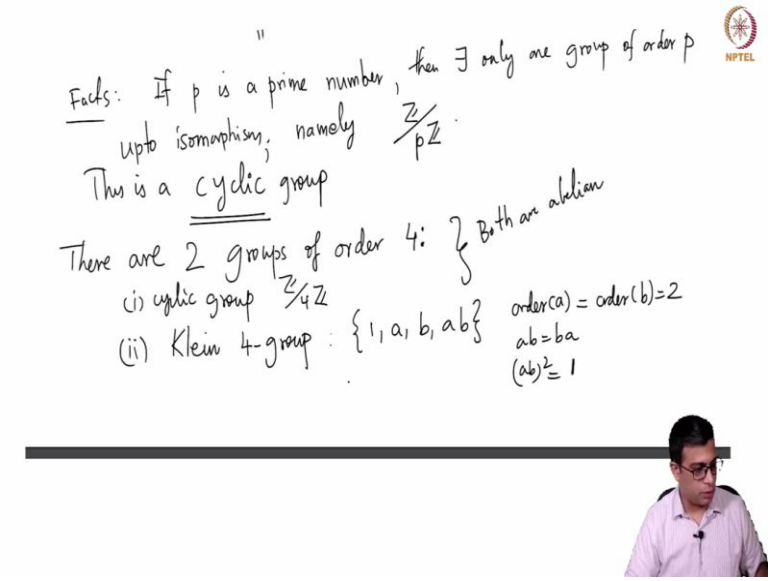
So, in the groups it is nice that an isomorphism is simply by a bijective homomorphism, we are mainly interested in isomorphism classes of groups. For example, we are not going to treat two groups which are isomorphic as different. So, for all practical purposes they are same. So, there is only 1 group up to isomorphism as always, of order one, of course. There is only 1 group of order 1 because it has to be the identity element.

(Refer Slide Time: 06:50)



Similarly, there is only 1 group up to isomorphism of order two also there is only 1 group up to isomorphism of order 3, order 5, and so on. So, not true for 4, but in fact, so now, I am beginning to recall some of the standard facts that we will use repeatedly. So, if p is a prime number, then there exists only 1 group of order p up to isomorphism which is to say that any two groups of order p are isomorphic. So, you can take Z mod p Z. So this you take the additive group of integers and go modulo the subgroup of all multiples of p. So, that is the only group of order p.

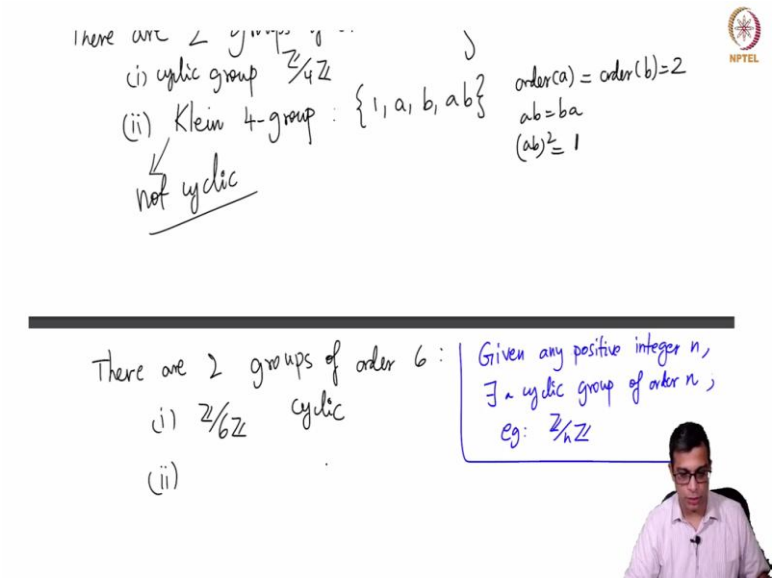
(Refer Slide Time: 07:52)



This is a cyclic group, this is a cyclic group. So, this is another important word for us. What is the cyclic group? That means there is 1 element in this group which generates the entire group that means all its powers or multiples in the additive notation cover the entire group. On other hand, there are two groups again up to isomorphism which I will not write every time because always when I make a statement like this, this is up to isomorphism, there are two groups of order 4.

One is the cyclic group which is Z mod 4 Z and other one is Klein 4 group, that has lot of awatars, it is basically 1 way of defining this is a and b are elements, which are order 2 and ab is equal to ba. So, and of course, ab square is also e or 1 in this case. So, this is an Abelian group. So, every order group for, every group of order 4 is abelian. So both are Abelian. And of course out of five group, there is only one Z mode 5Z which is Abelian.

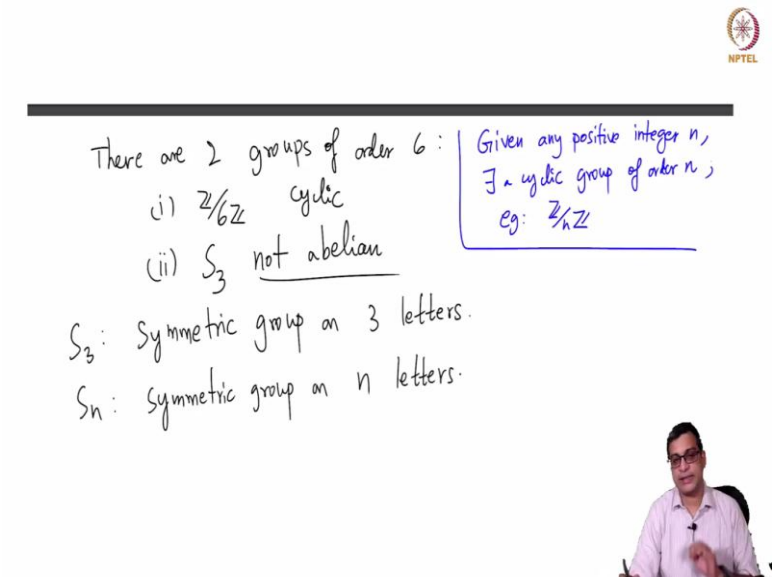
(Refer Slide Time: 09:38)



So, if you take, if you want the first non abelian group or the smallest non abelian group, you will have to go degree order 3, order 6 rather. So, there are three groups, sorry there are two groups of order 6 again, up to isomorphism. And what are they? 1 is Z mode 6Z cyclic always so of course here, it is clear what I am saying. But I will stress explicitly write this. Given any positive integer n there exists a group, cyclic group rather of order n. For example, take that Z mode nZ. So, that is a cyclic group of given, any given order n.

But in some cases there are more groups for example, client 4 group is not cyclic. So, this is not cyclic, any two cyclic groups of same order of course are isomorphic. So, here is client 4 group is not cyclic, but Abelian.

(Refer Slide Time: 10:53)



But if you go to order 6 in fact, S3 is not only not cyclic, it is not even Abelian. And now, that gives me a chance to important, talk about the important notional Symmetry groups. S3 is the symmetry group on 3 letters. So, in other words, this is the group of bijections of an element of a set with three elements. So, more generally, Sn is a symmetric group on n letters, in many ways, this is the most important group for us.

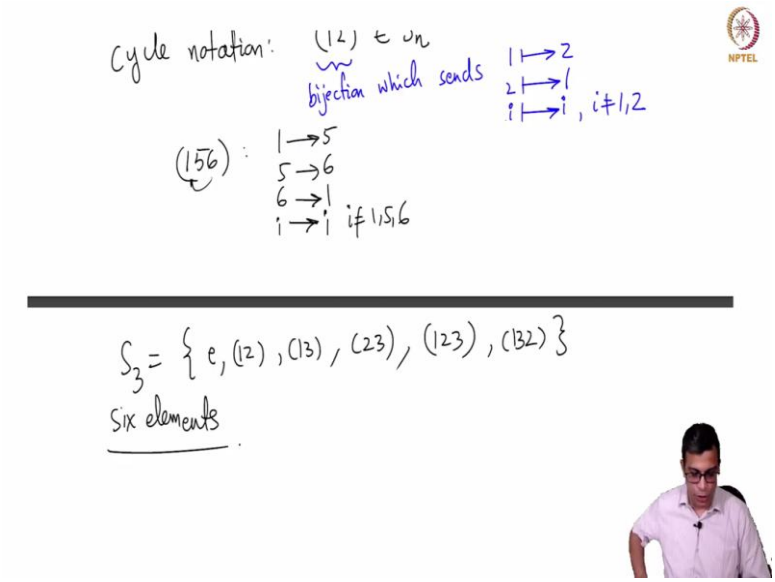
So, let me just spend two minutes on what introducing the basic ideas of Sn, so, this is the set of bijections of it an n element set, so, which we can, the elements can be called 1, 2 upto n. So, this is the set of projections of this set 1 to n and the operation is simply the compositions, composition. So, if you take two bijections of this set 1 through n and compose them, you get another bijection.

So, because composition is typically not Abelian, this is also not Abelian unless n equal to 3 or n equal to 1 or 2. In that case, of course, you get an Abelian group. So, Sn is a group of order. So, these are all standard facts that I will only mention and not prove. Again, this is something that is done in any standard Group theory course at the beginning of any standard big Group theory course.

So, I am not going to spend time proving this but typically, how do we define, how do we describe elements of Sn to use cycle notation. So, for example, if you take 1 2 as an element of Sn 1, 2 is the bijection, which sends 1 to 2, 2 to 1 and everything else to itself. So, i to i for i is not equal to1 and 2. So it does not matter what n is. So this is only interchanging 1 and 2, fixing everything else.

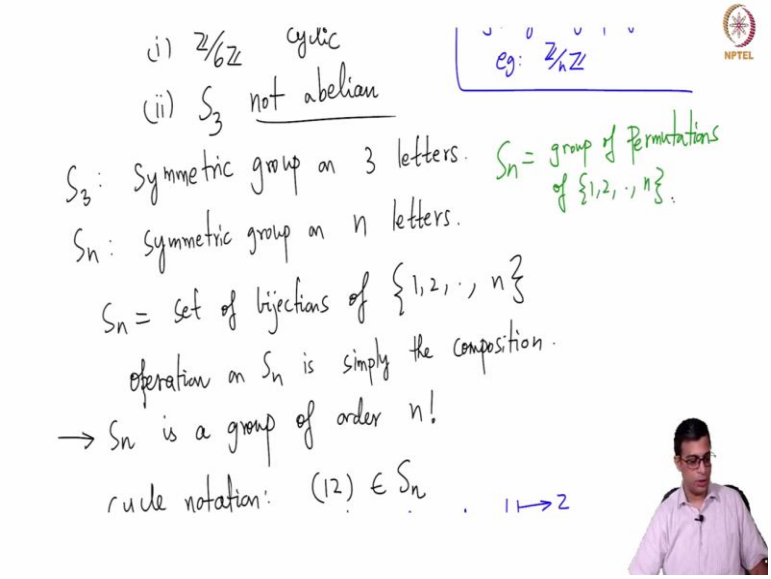
So more generally, if you have more examples rather 1 5 6, what does it do 1 sends, 1 goes to 5, 5 goes to 6, you just look at that. What is next to 1, which is 5, so 5 goes to 6, 6 goes it is a cycle, so you come back to 1, so 6 goes to 1 and everything else to itself i not equal to 1 5 6 , so and then we can multiply them easily and we can find the inverse also easily. And cycle notation is very important. So in this cycle notation, what is S3?

(Refer Slide Time: 14:14)



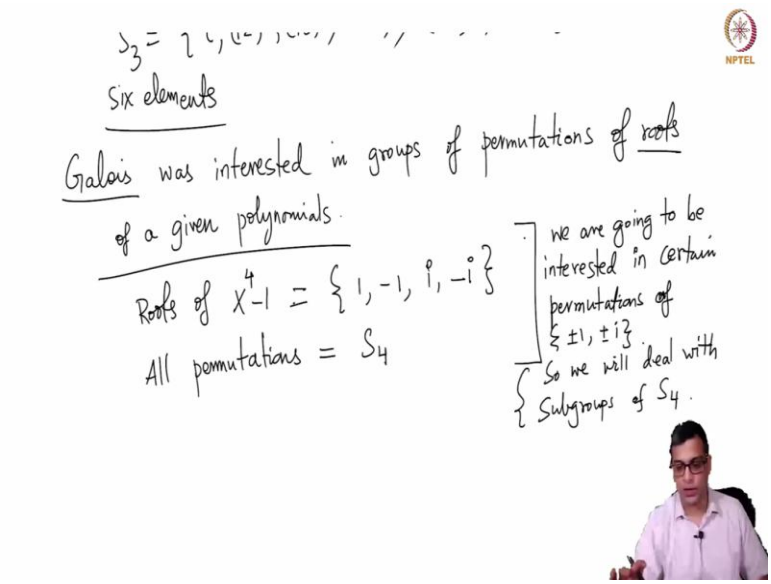
S3 is of course, e 1 2, 1 3, 2 3, 1 2 3, 1 3 2. So 6 elements so S3 is the symmetric group on three letters. And if you think about it, there are only these 6 permutations. So these are called permutations.

(Refer Slide Time: 14:44)



So I should use this notation also. Sn is the group of permutations. That is an important word for us of n elements, 1, 2, upto n. So these are called permutations this 1 5 6 is a permutation 1 2 3, 1 2 is a permutation and so on.

(Refer Slide Time: 15:13)



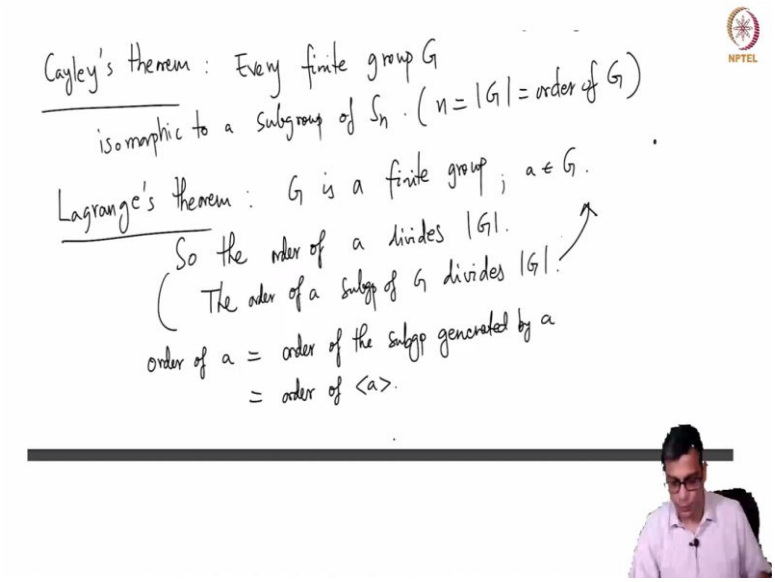
And Galois was mainly interested in, in fact, he only really studied permutation groups or symmetry groups interested in groups of permutations of and what is the set whose permutations he studied that set is the roots of a given polynomial and as we go along and learn more things in this course, you will understand more about this, but he was interested in permuting polynomials

permuting the roots of polynomials for example, roots of x4 minus 1 as we saw in the previous video are these.

So, what are the permutations if you take all permutations you get S4 but in the context of field theory that we will develop later, we are not going to allow some permutations, for example, 1 cannot go to i. So, I do not want to get into that right now, because that is it involves more theory and it will take away take me away from recalling the group theory that we need, but we are let me just end move on after saying that.

We are going to be interested in certain permutations as we will discover later of this set, plus minus 1, plus minus i. So, we will deal with subgroups S4 consists of all permutations of these four elements set, but they are all not going to be of interest to us only certain subs subgroups of S4 is what we are going to be interested in. So, the permutation groups are very important.

(Refer Slide Time: 17:39)



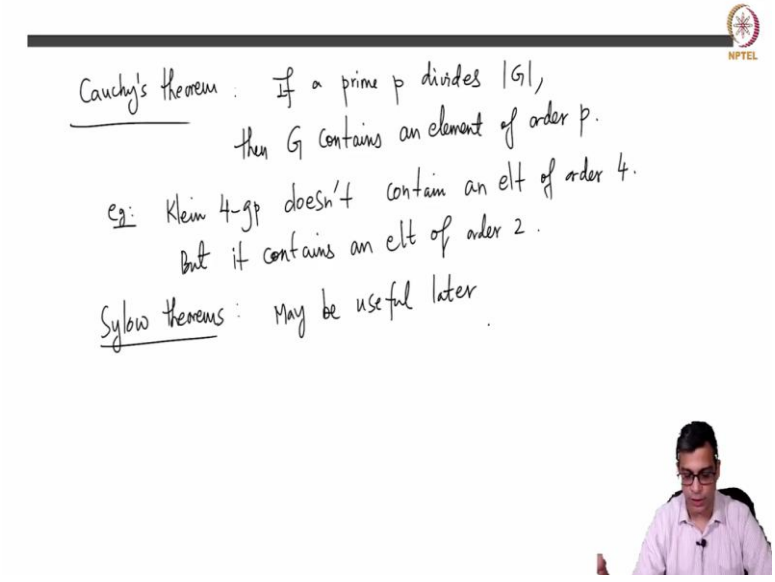
And also this conceptually or structurally they are important in group theory, because you are all familiar with this theorem of Cayley which says that every finite group is isomorphic to a subgroup of Sn in fact, n here is the order of G. So, this is the notation that I use for order of G, so, every finite group can be embedded inside Sn. So, in other words, what I am saying is, if you study symmetric groups and their subgroups, you studied all groups.

All finite groups rather if you studied symmetric group and subgroups of symmetric groups, you covered all finite groups. So symmetry groups are important in this sense. So some other important things that we will constantly use Lagrange's theorem. So it says that, if you have a G is a group, always a finite group. Except I do not think I will ever talk about an infinite group. But if I do in this course, I will explicitly mention it.

So, I will say, without any adjectives, I will just say if I say G is a group, I always use finite groups, I always refer to finite groups. If x is an element or a is an element of G, the order of a divides the order of G. So the order of a divides the order of G. So as a consequence, you know that order of a subgroup, subgroup of G divides this is a consequence because, you take actually, this is the Lagrange's theorem, I should say.

So, so I should really this is Lagrange's theorem, and so I should write so, this really should come first, the order of a subgroup of G divides out of G itself. So, if you take an element its order is equal to the order of the subgroup generated by a. So, which I denote by this symbol, so, that divides this. Lagrange's theorem is very important, very foundational result in group theory. So, you know for example, that if you have a group of out of 10 it can consist of an element of order 3 for example. And there is more results I will recall maybe a few of them

(Refer Slide Time: 20:41)

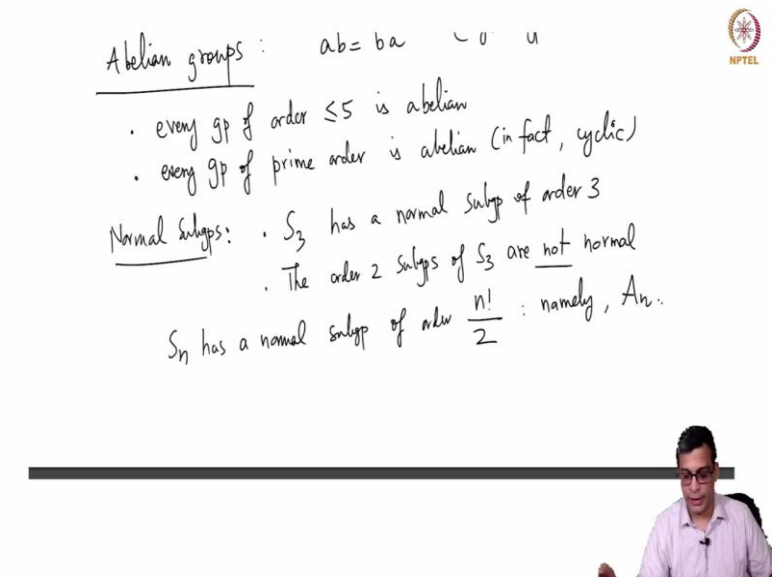


Cauchy's theorem. So, the sort of a converse to Lagrange's theorem say if a prime p divides order of group G then G contains an element of order p. So, remember this is not true in general

if you do not assume that the order is p. So, for example, Klein 4 group does not contain an element of order 4. 4 does divide its order which is 4 itself, but it does not contain an element of order 4 but it contains an element of order 2. So, 2 is a prime number dividing the order of the group which is 4 in this case. So, there is an element of order 2.

This is an important theorem that again will occur a lot and more generally I will not recall these because these may not come up till the very end. Sylow theorems which develop which start from Cauchy's theorem but prove a lot more, a lot more powerful statements may be useful later we will recall them if and when we need this. So, this is sort of structure of some information about finite groups and their structure.

(Refer Slide Time: 22:25)

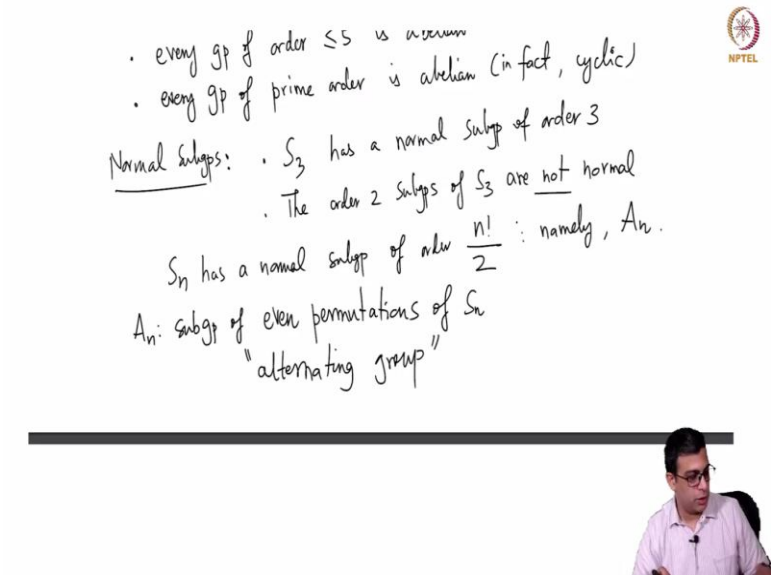


So, we have notions of Abelian groups, so, I am not doing this in any particular order. So I am just recalling some of the key concepts that will use. Abelian groups are where the binary operation is commutative. So, for example, every group of order less than or equal to 5 is a Abelian as I mentioned a couple of minutes ago, so, every group of prime order is Abelian, in fact, cyclic, cyclic groups are Abelian.

So, cyclic groups are Abelian, so, trivial statement. So, you have the notion of normal subgroups. So, I will not get into this in detail, every subgroup of an Abelian group is normal, but for a non Abelian group, some subgroups need not be normal. For example, if you have S3 has a normal subgroup of order 3.

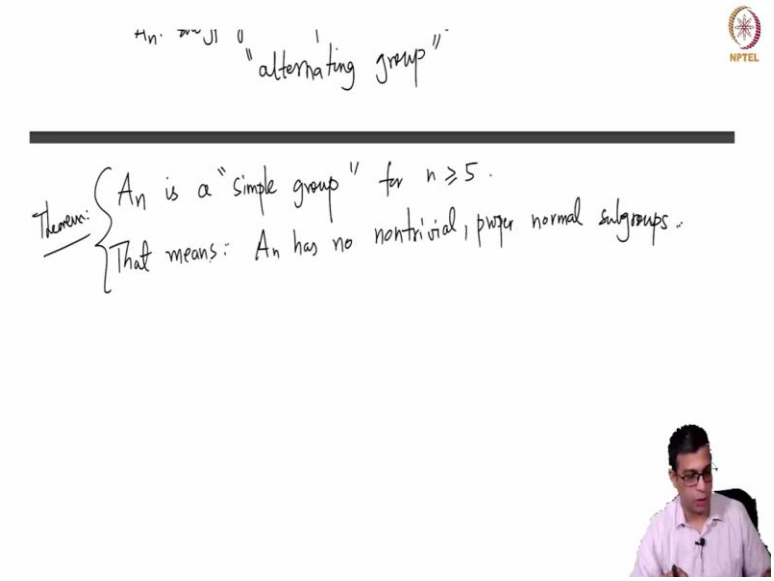
The order two subgroups of S3 are not normal. Again, let me remind you I am not really, I am, just a hodgepodge of various facts that I am recalling right now about Group theory that I believe will come up throughout the course. So, Sn has a normal subgroup always of order n factorial by 2 namely An.

(Refer Slide Time: 24:30)



An is the group of even permutations subgroup. So, there is a notion of parity of permutations. So, every permutation is either even or odd. So, if you take even once, and they are exactly n factorial divided by 2 of them, the other half are odd. So, if you take even permutations they form a subgroup. So, An alternating group it is called Alternating group is always a normal subgroup. In fact, any subgroup of index 2 which is a subgroup whose order is exactly half the order of the group is normal.

(Refer Slide Time: 25:15)



And An is and this we will use later here. An is a simple group for n greater than equal to 5 that means, An has no non trivial proper normal subgroups. I mean, this is a difficult fact, so this is in fact a theorem. And this is covered typically in any group theory course so, you might recall the proof, but this is something that we will use at the very end when we show that quintics in general cannot be solved by radicals. So, these are some of the facts that I want you to recall about groups.

There are many other things that I may be forgetting right now. But what I will do in the course is I will, so these are the things that I have done today. So, I recall what is a group homomorphisms of groups, very important basic notions, Cyclic groups, Abelian groups, Symmetry groups, and talked about homomorphisms, isomorphisms. And some important theorems Cayley's theorem like Lagrange's theorem, Cauchy's theorem, and so on.

What I mean, this is by no means an exhaustive list of topics in Group theory that we will need, but what I will do in the course of the next eight weeks, is that any topic that I will require, I will maybe mention it as a theorem in group theory, without going into the details, which and then you can refer to the group theory sources for more explanations. So this is roughly the review of group theory that I wanted to do. And then in the next few videos, we will recall rings and fields. So let me stop this video here and continue with a review of Ring theory in the next video. Thank you.