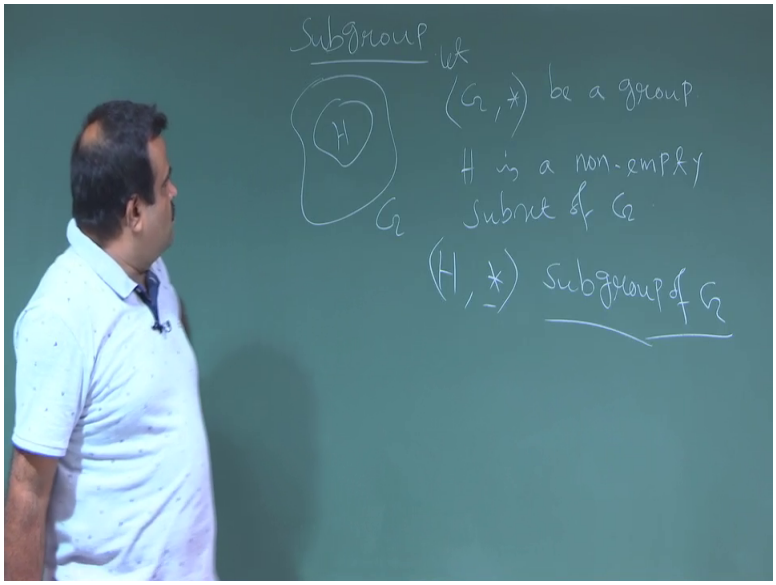
Introduction to Abstract and Linear Algebra
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture – 14
Cyclic Group

Ok. So, we are talking about subgroups.

(Refer Slide Time: 00:18)

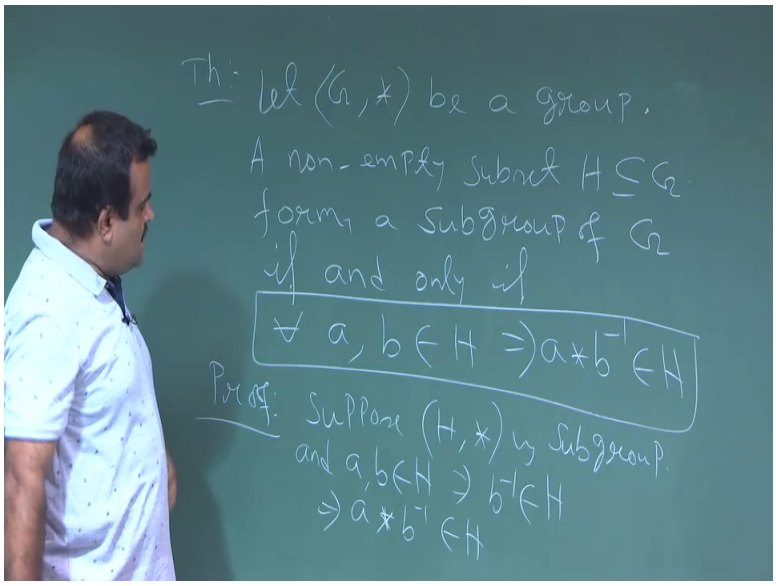


So, in the last class we have seen one necessary and sufficient condition for a non empty subset to be a subgroup. So, today we will talk about another conditions for a non empty subset to be a subgroup. So, this is our group G which is under this binary operator it is a group let G be a group and H is a subset of G this is H non empty subset of G ok.

Now, if H is also form a group under this operator induce operator because these we are considering only those elements only the elements of H. If we consider H has a H to be a group, if this is a group then it is called then it is called a subgroup of group of G because this is a subset and if this subset is also from a group under that induce operator then it is called a subgroup, ok.

So, now we talk about one necessary and sufficient condition to be a H to be a subgroup this is a theorem.

(Refer Slide Time: 01:57)



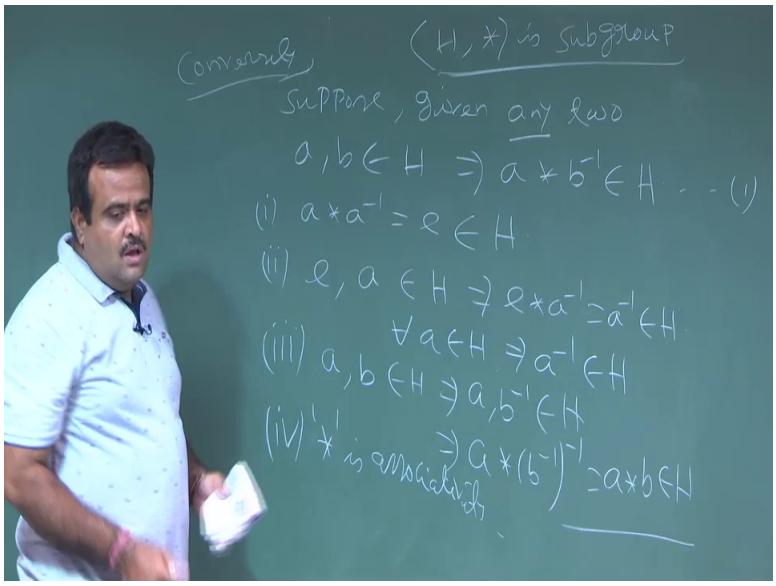
Now. So, this is telling let is the statement of this theorem be a group and then a nonempty subset nonempty subset H this is the subset of G forms a subgroup of G if and only if this is the necessary and sufficient condition if and only if the condition is given two element for any two element a, b belongs to G by belongs to H if it is imply a star b inverse belong to H and if it is true for all such all a, b.

We take any two element from H if a star b star b, b inverse this is the inverse. So, we assume this is multiplicative sense anyway b, b inverse. So, b compose with this will give us the identity element. So, this is necessary and sufficient condition. So, this we have to prove ok. So, how to prove that there are two parts. So, first of all necessary part say suppose this is a group suppose, H is a subgroup then we have to show given any two element is and a, b are same we take a, b from this.

Now, if H is a group then b belongs to H implies b inverse will also belongs to H and a also belongs to h. So, this is the existence of inverse every every elements should have inverse in a group. Now, a belongs to H and b inverse belongs to H. So, this implies a star b inverse belongs to H as this is by the closure property. So, this is by the closure property. So, this part is.

Now, the sufficient part now we assume for any two a, b this condition is happening then I show that this H will be a subgroup. So, we assume this is the sufficient part the conversely just.

(Refer Slide Time: 05:06)



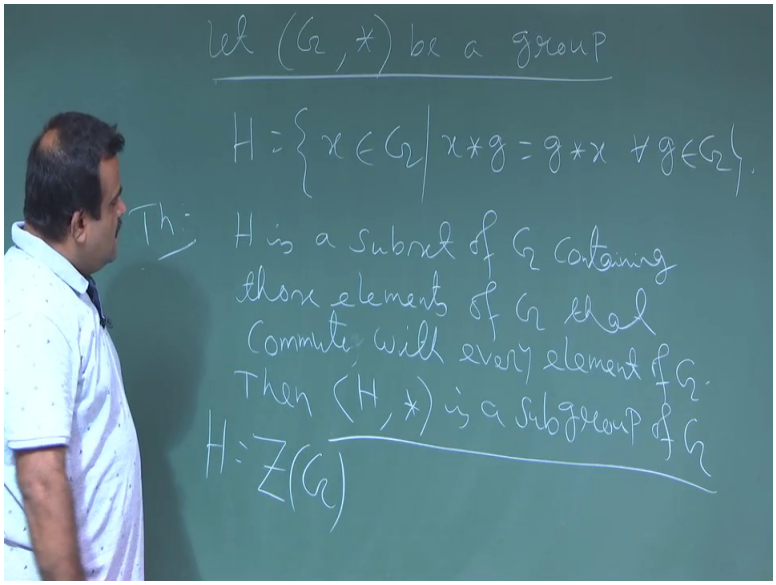
So, conversely suppose given any two element any two a, b any two element a, b belongs to H implies this is the condition we are having. Now, we need to show this H is a H is a group H is a group under this star and it is called a subgroup ok.

So, first of all we so, for that we just take a if we take b to be a then this condition will give us from all this is a. So, b to be a then a star a inverse which is nothing, but e e will be belongs to H. So, that H this is identity element so, existence of identity element. So, identity element of G is in H, and then identity element if there then we take e and e and a belongs to H. Now, this implies e a inverse which is nothing, but a inverse belongs to H. So, this is the existence of inverse every element this is true for all a. So, for all a belongs to H implies a inverse belongs to H. So, every element has the inverse in H.

So, this is the existence of inverse and then the closure property. How to take closer property? We know if a is in we take a b to be in H this implies a b inverse will be in H now this implies if we use this property a star b inverse which is nothing, but a star b which will be in H. So, this is the closure property and associativity property is already there because star is associate that is why G is a group. So, star is associativity associativity property is satisfying. So, that means, this is a H is a group it is a subgroup ok. So, this is a mess another necessary and sufficient condition to become a non empty subset to be a subgroup ok.

So, now, we talked about some important groups those are called central of the group. So, we will talk about some important subgroups.

(Refer Slide Time: 08:21)

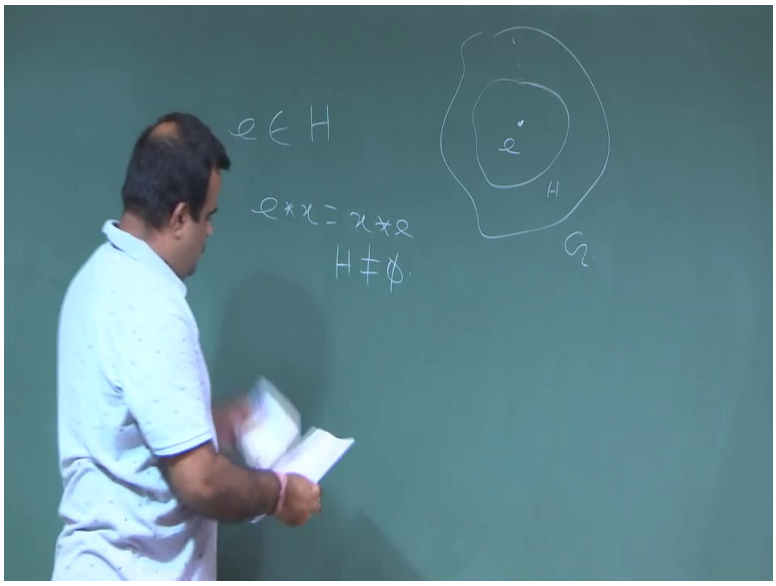


Let G be a group, ok. Now, we consider a set H such that all the elements belongs to G such that x star g is equal to g star x and this is true for all such g belongs to this. So, that means, H is a subset of G where each element are community commutes with each other. So, H is a subset of G containing those elements of G that commutes that commutes with each other with every element of G. So, that commutes with every element of G.

Then we can show, then H is a subgroup of G sub group of G this we need to show this is the theorem this we need to show and this is called this we this we need to show this is subgroup of G and this is called central group of G and this is denoted by Z G this H is denoted by Z G this central a group of G a central group of G.

Now, how to show this is a subgroup first of all we need to show H is non empty. So, can you just tell which element must be there in H? Identity element, yes. So, identity element must be there is in H because for. So, this is our G.

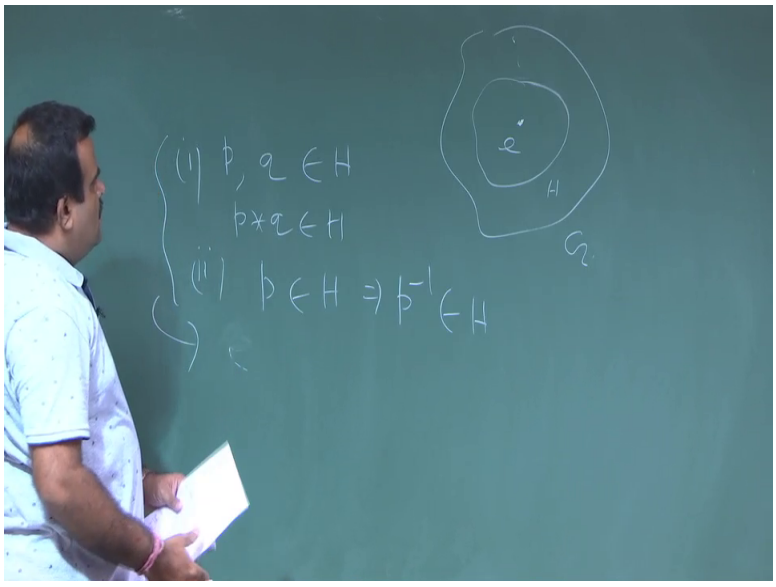
(Refer Slide Time: 10:54)



So, now, id is here identity element. So, we are consist so, i e must be in H because for this e e star x is equal to x star e. So, e commutes with every elements. So, identity elements must be there in G H. So, H is non empty.

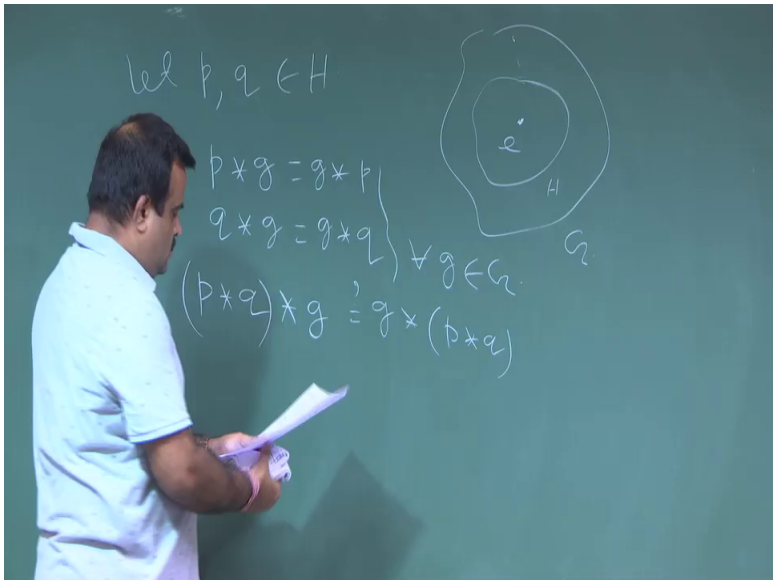
So, now we slowly build this H. So, now, you have to show that H is a subgroup. So, for that we need to use that result which is the theorem that if you take a two element p, q then p star q must belongs to H for all p, q.

(Refer Slide Time: 11:40)



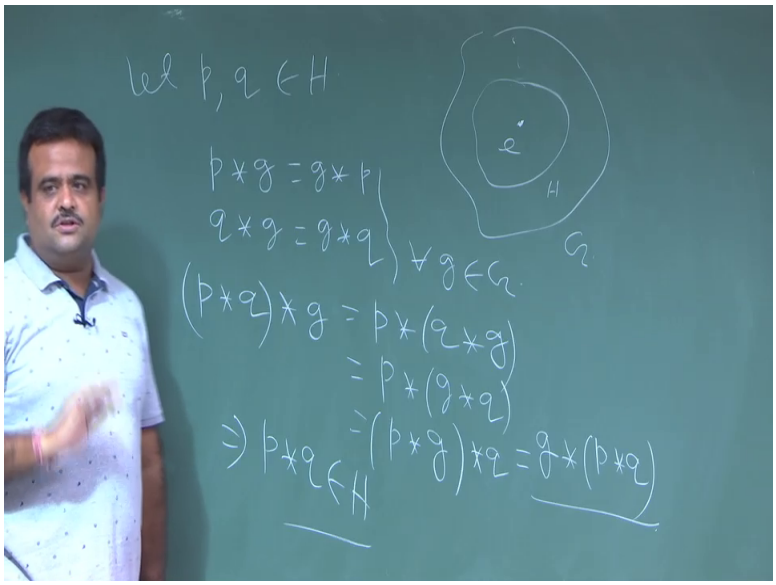
And, then if you take a element from H this must imply inverse is also belongs to H then these two will give us H is a subgroup this theorem. We have seen in the last class is in this is one of the necessary and sufficient condition. So, you have to use this theorem ok.

(Refer Slide Time: 12:12)



So, how to use this theorem? So, first of all let us take p, q belongs to H then we need to. So, p star q also belongs to H. So, p, q belongs to H means. So, p star g is equal to g star p and also q star g is equal to g star q and this is true for all g belongs to G ok. So, now, ok. So, now, p star q star g if you just operate p star q star g we want to see whether this belongs to H or not. So, for that this we have to show to be g star p star q this we need to show. So, for that we need to work out.

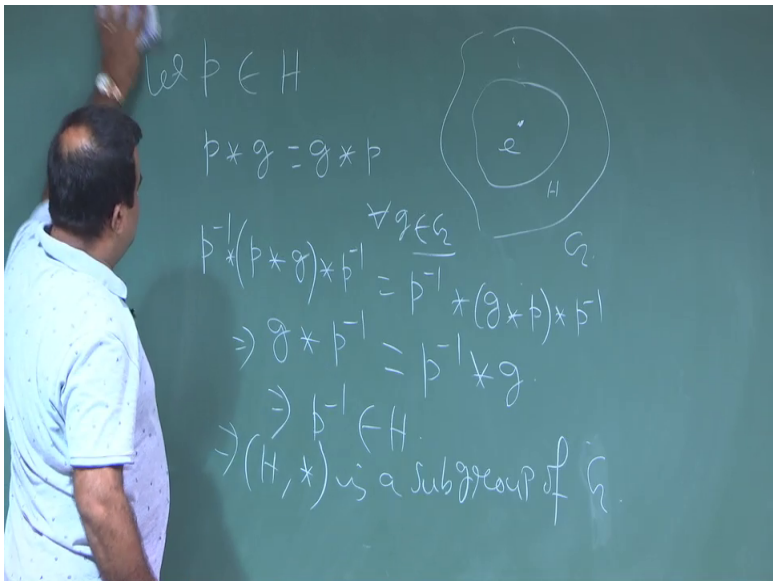
(Refer Slide Time: 13:07)



So, this is nothing, but p star q star g because of associativity property of star. Now, this is nothing, but what this is nothing, but we can use this p star g is equal to g star q. So, this is basically g star q. Now, again associativity property p star g p star g star q now this is again equal to this is again equal to we can write other way around g star p star q. So, we can just take this to be here and again we can apply associativity property.

So, this implies p star q belongs to H. So, if p, q belongs to H then p star q belongs to H this is one part of the theorem and another part you have to take a p and we need to. So, that p inverse is also in H.

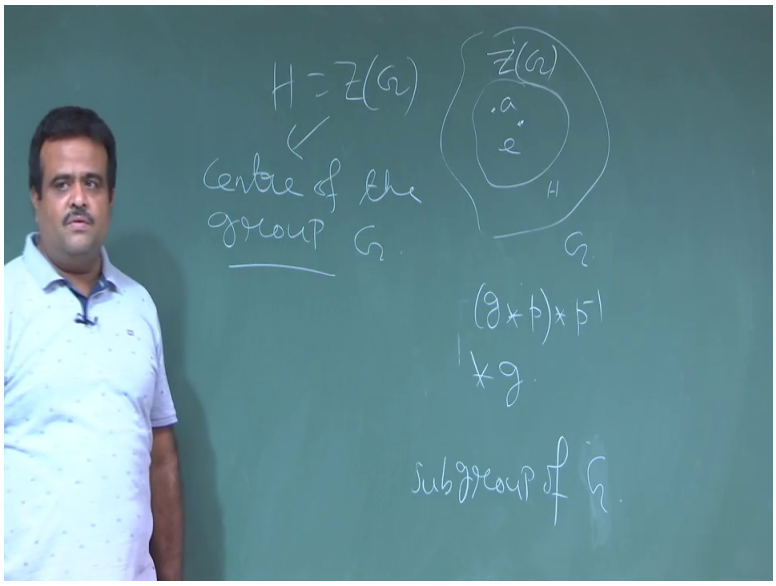
(Refer Slide Time: 14:24)



So, let us take an element p. Let p belongs to H then you have to show p inverse is also belongs to H. So, how to show this. So, p belongs to H means p star g is equal to g star p and this is true for all G.

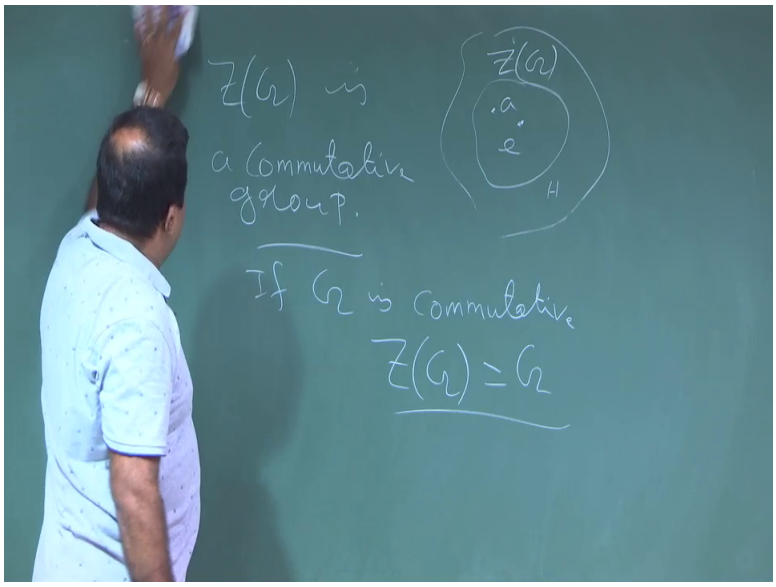
So, now if we apply p inverse on both side p star g p inverse is equal to p g star p star p inverse. So, this will give us what? This will give us we can just take g p inverse because this is cancelling out g star p inverse is equal to p inverse star g. So, this implies p inverse belongs to H. So, by that theorem we can say this implies this is a subgroup of subgroup of G sorry subgroup of G.

(Refer Slide Time: 15:48)



And, this subgroup is denoted by Z G. So, this H is denoted by Z G and this is called central element this is called center of the group center of the group G the subgroup, and any element from this center is called central element of G any element from this. So, any e is a central element if you take any other element from this H this is called central element of G.

(Refer Slide Time: 16:42)

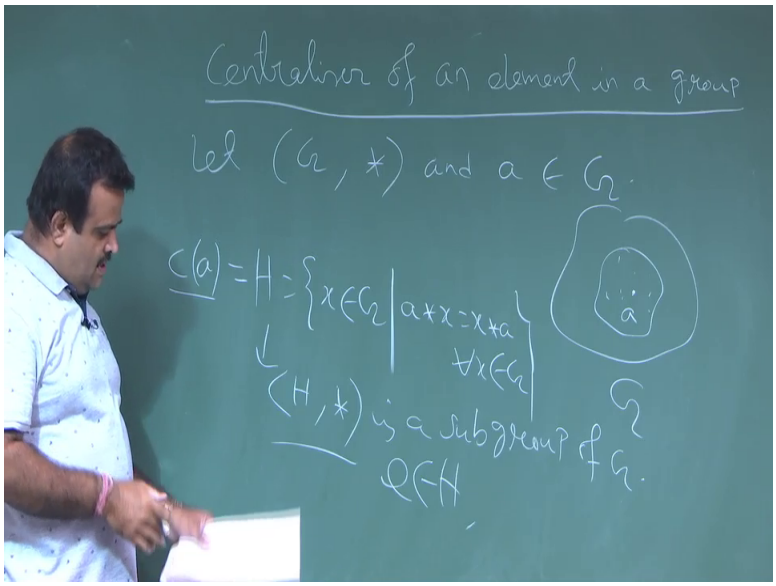


Now, now this central element this has a property this is Z G is commutative because that is the way we choose Z H. Z G just this is a commutative group in general G may not be

commutative, but this central I mean we form the we take all the elements where everybody is committed with each other. So, this is this set will form a group and this is obviously, a commutative group because in this said this operation is commutative.

Now, if G itself is commutative I mean if star is commutative in G if G is a commutative group if G is a commutative group then; obviously, Z G is the G whole group, ok. So, this is the called central group.

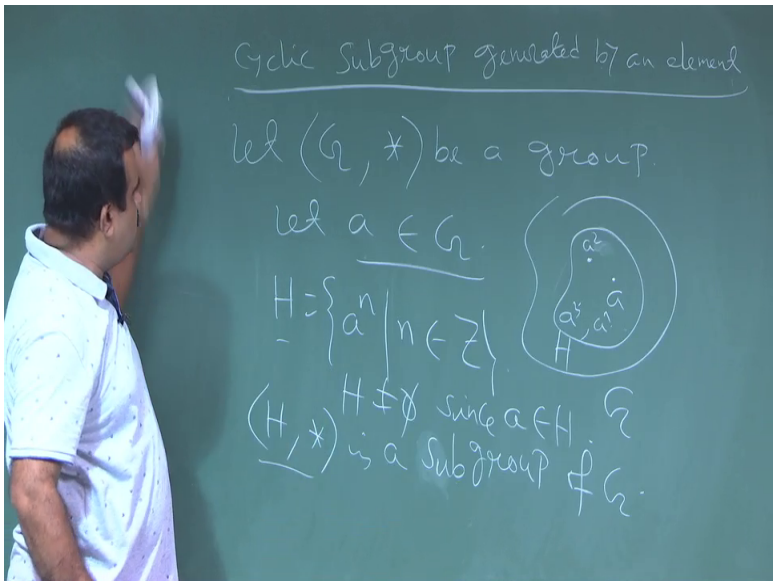
(Refer Slide Time: 17:50)



Now, we define another terminology centralizer group of an element. Centralizer of an element in a group in a group. So, so, how we define this let G be a group and a, b an element in G. So, this is a group and we take an element from G now we defined this set. Now, on this around this a so that means, we do we take all the x from this G which commutes with a. So, we define the set all G such that a star x equal to and this is for all G, then we can.

So, this is all the all the elements where it is community with this is the this set is called centralizer around this element a and we can variance we can show that this is also a subgroup, subgroup of G because this is non empty because e must belongs to H, and again we can use that theorem is an sufficient condition we can. So, this is a subgroup of G and this is denoted by C of a centralized group around the point a, ok.

(Refer Slide Time: 20:04)

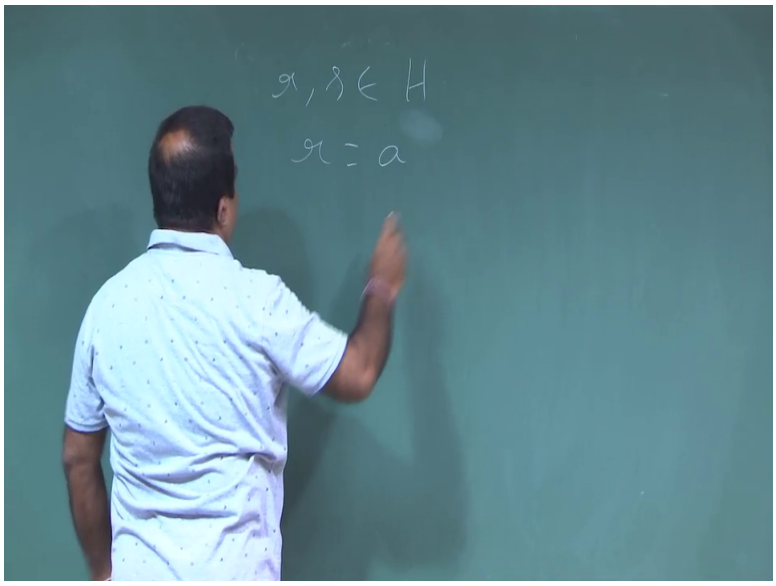


And, so, now, we defined another group which is called cyclic group cyclic subgroup generated by a point a cyclic subgroup. Cyclic subgroup generated by an element, ok. Again that G be a group G be a group and we take an element from a and from G let a, b an arbitrary element from G, ok.

Then we define a set which is a subset of G. So, this is our G and we have an element over here now we take the set where we get the points by generating a. So, a star a which is basically you know a square, a cube, a to the power n like this. So, if we operate a with itself. So, it is a subset which is coming from generating by general from the element a. So, this is this we denote by H which is basically a to the power n; n is a integer right, yeah.

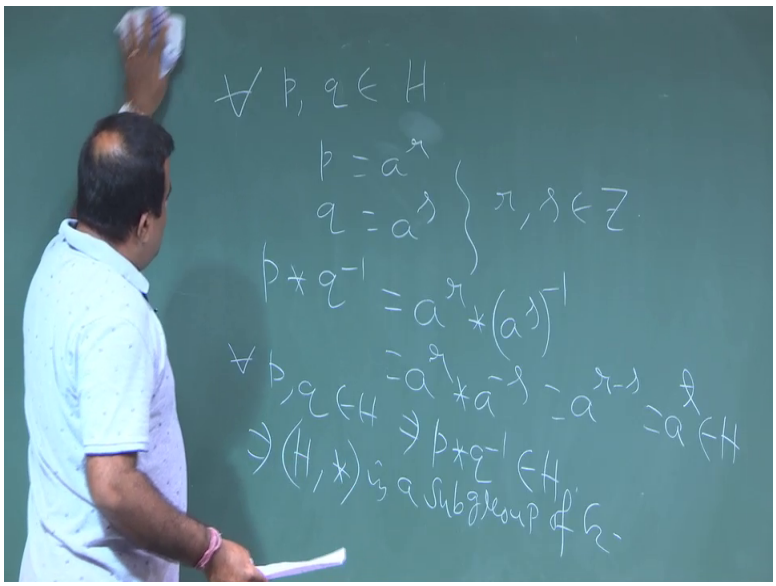
So, this set now this set is a non empty set because a is there, this is not equal to phi since a belongs to H. Now, this we can show to be a subset subgroup. So, H and star is a subgroup of G and this subgroup is called cyclic subgroup generated by the element G. So, how to prove this is an subgroup? So, this is a non empty set now to show this is a subgroup we will use one of the necessary and sufficient condition that theorem.

(Refer Slide Time: 22:19)



So, we take two element from this set r and s belongs to H. So, that that means, r will be of the form a to the power n or some or we take p, q here r, s we can use as index p, q.

(Refer Slide Time: 22:34)

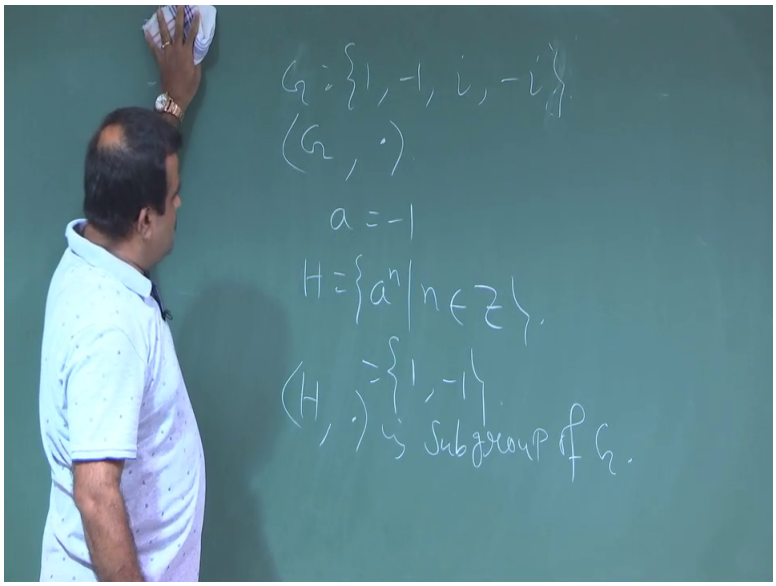


So, p will be of the form a to the power r q will be of the form a to the power s where r, s are integer any integer, ok. Now, we operate p star q inverse now this is nothing, but a to the power r star a to the power s inverse now we know this result a to this power r star a to the power minus s. So, this is basically a to the power r minus s. So, this is of the form

a to the power t where. So, this is belongs to H because t is an integer. So, this is belongs to H.

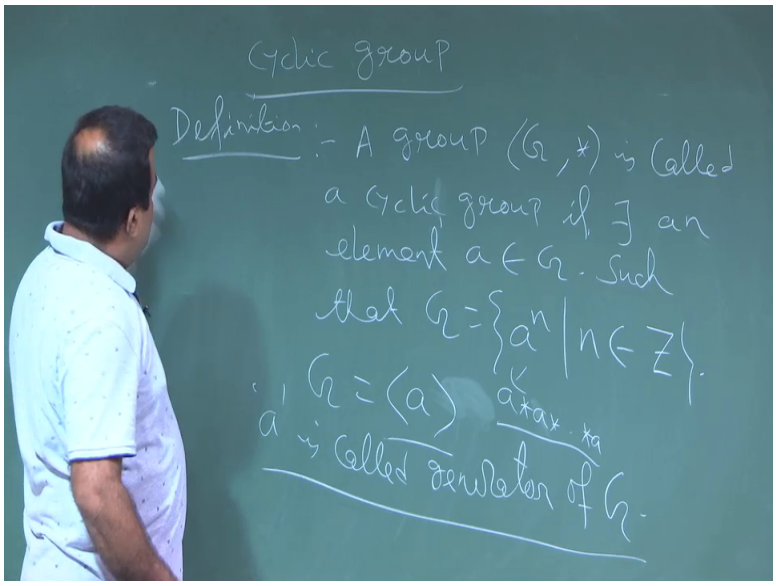
So, for any two for all p, q we have seen for all p, q belongs to H implies p star q inverse belongs to H. So, this implies by that theorem this is sufficient condition H is a their sub group subgroup of G and this subgroup is called cyclic sub cyclic group generated by the cyclic sub group generated by the element a.

(Refer Slide Time: 24:06)



Now, if you take an example like say if you take s to be our G to be 1, minus 1 i, minus i. So, we know this is a group under multiplication this is a group under multiplication. Now, if you take an element a to be minus 1. Then what is the H? H means that set generating by a. This is nothing, but 1 and minus 1 now this is basically a sub group we can easily verify this is a subgroup of G.

(Refer Slide Time: 25:11)

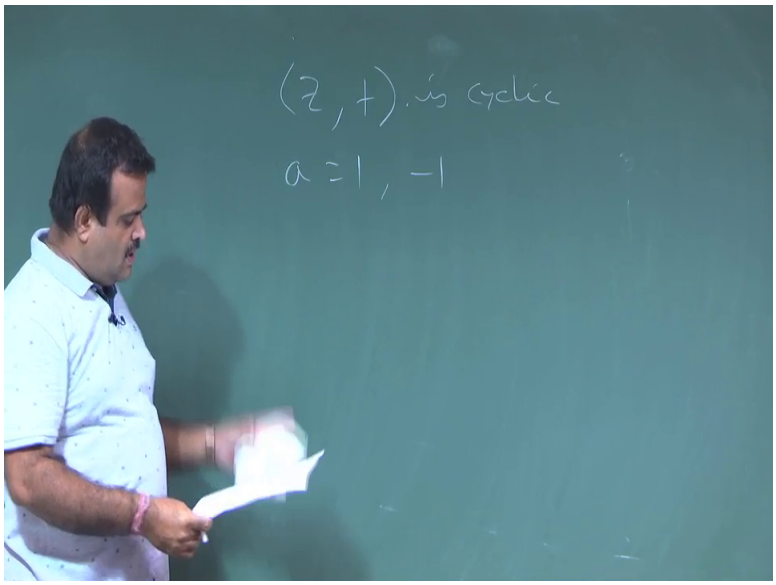


So, now we define what do you mean by a cyclic group. So this is the definition and this that subgroup which is generated by that element a; a is called a generator of that group. Let so, and group a group G is called a cyclic group cyclic group if there exists an element which generates are group a from G such that such that that a generates the group; that means, G will be written as a to the power n, n is a integer.

Again, this operator is in multiplicative sense that is why we are taking. If it is not my if it is additive sense then this could be a n a, but anyway this is the terminology a star if we are taking start to be multiplicative sense that is why we are allowed to use a to the power n. So, this is nothing, but a star a n times this symbol is nothing, but n times a.

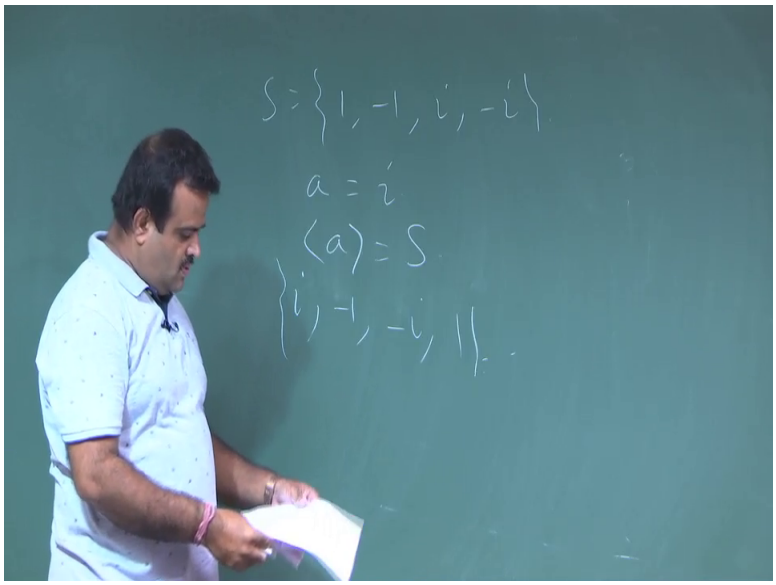
So, this a is generating the group; that means, this G is basically the this is the cyclic group this is the symbol of the cyclic group generated by the element a and. Now, if we have a generator and this a is called a generator of that group a is called that element a is called generator because the it is generating the group, ok. It is generating the group that is why it is called a generator.

(Refer Slide Time: 27:40)



For example if you take the group Z set of all integer with the if you take this group. This is a group this is a cyclic group because this is the generator 1 is the generator, 1 or minus 1 any one of this is a generator because this can generate the group, ok.

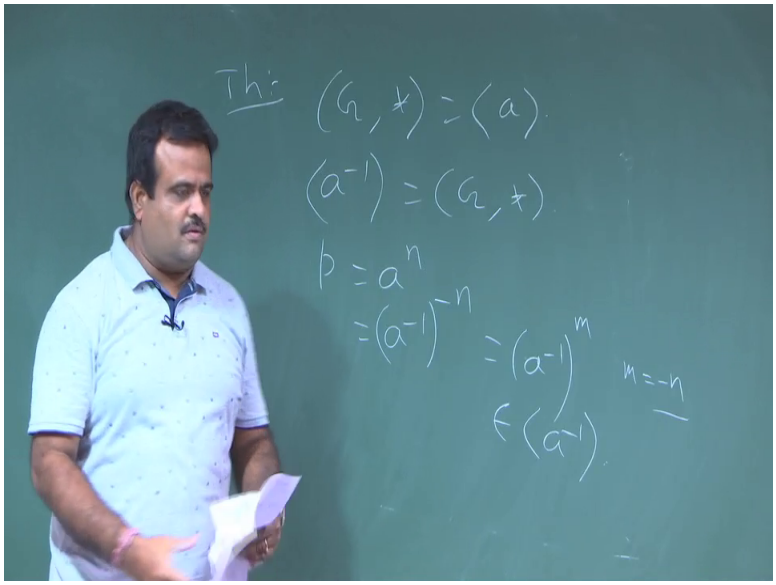
(Refer Slide Time: 28:08)



Now, if you take this the set which we have talked about. S to be say 1, minus 1, i, minus i ok, this is a group. This is a cyclic group. Why? Because who is the generator here i or minus i is a generator if you take a to be i then it can generate the group ah. So, this is basically S because i if we keep on operating i square is basically minus one then i cube

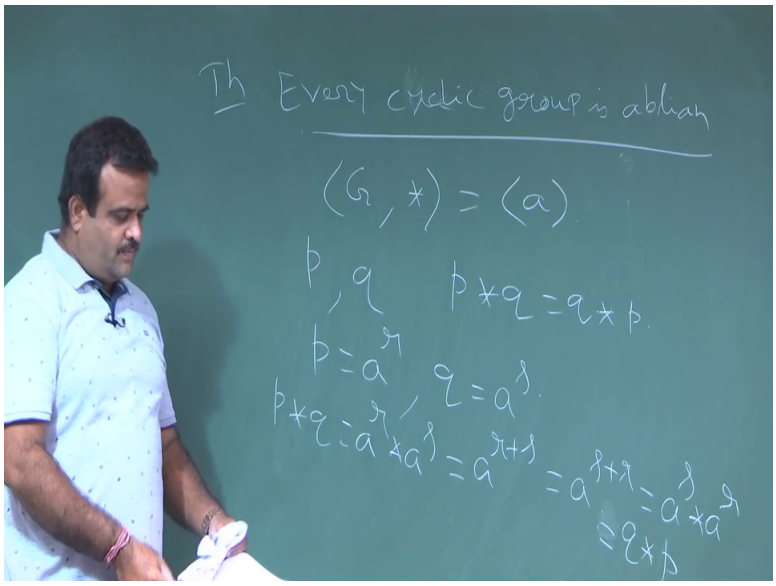
is basically minus i then i to the power 4 is basically 1 like this. So, it is a it is you are giving us the it is generating the whole group.

(Refer Slide Time: 28:51)



So, now quickly to listen on this first we calculate this. So, suppose G is a cyclic group and a is a generator. So, that means, a generate this then a inverse is also a generated why because if a generate this group. So, any element if you take from G p. So, p will be a to the power some n then it can be written as a to the power minus to the power minus n. So, minus n is again a integer. So, a to the power inverse some n; where m is equal to minus n. So, that means, it is belongs to a minus ok. So, if a is a generator then a inverse is also a generator of that group.

(Refer Slide Time: 29:48)



Now, this is a cyclic where this is a commutative group if we have if G is a cyclic group. This is a theorem every cyclic group is every cyclic group is Abelian. So,why? Because if you take a cyclic group then we have a generator. Suppose, a is a generator of that group a is generating. Now, Abelian means if you take two element p, q we have to show p star q is equal to q star p.

Now, how to show this? Now, a is an element. So, a will be written has some a to the power r q will be written as some a to the power s now p star q is nothing, but a to the power r star a to the power s which is nothing, but a to the power r plus s which is nothing, but a to the power s plus r which is nothing, but a to the power s star a to the power r which is basically q star p ok. So, this is commutative.

So, thank you.