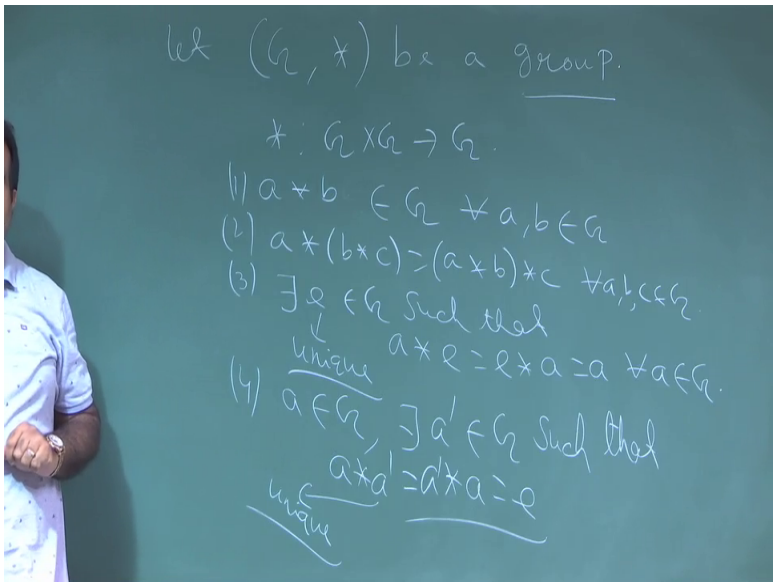
**Introduction to Abstract and Linear Algebra**
**Prof. Sourav Mukhopadhyay**
**Department of Mathematics**
**Indian Institute of Technology, Kharagpur**

**Lecture – 12**
**Order of an Element**

Ok. So, we are talking about group. We defined the group. Group is having four properties; closure, associativity, existence of identity and the existence of inverse for every element, then that is that algebraic structure along with the operator is called group.

(Refer Slide Time: 00:39)




Now, it is if the star is that algebraic structure. So, if this is a commutative then it is called commutative group or Abelian group, ok.

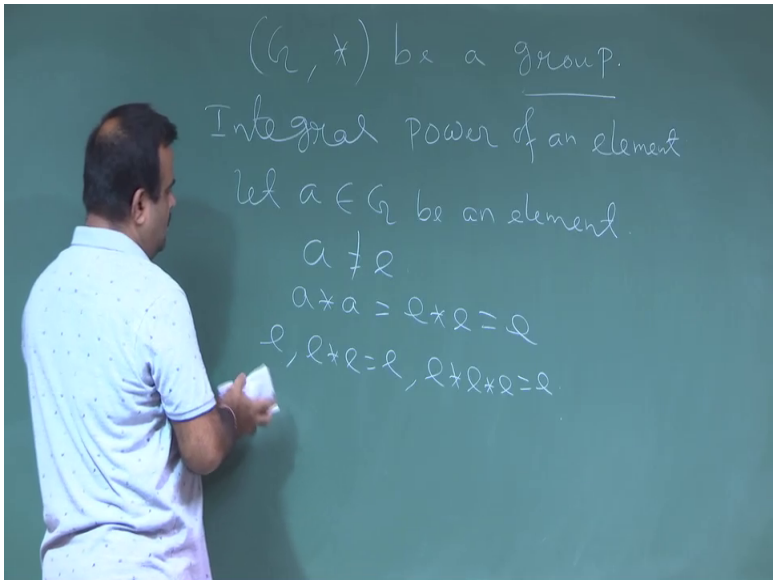
Now, suppose today we will talk about the ordering of a group, I mean the order of an element or and also the ordering of a group in the cyclic group, ok. So, to start with let G be a group. So, that means, what; that means, this is a binary operations this is closure.

So, that means, a star b is belongs to G for all a, b belongs to G this is closure property then we have associativity property this is also true for all a, b, c and then the we have existence of inverse there must exist a e such that such that a star e is e star a is equal to a

this is true for all a and this we have seen this is a unique there must exist a unique e such that this. This we have proved in the last class may be.

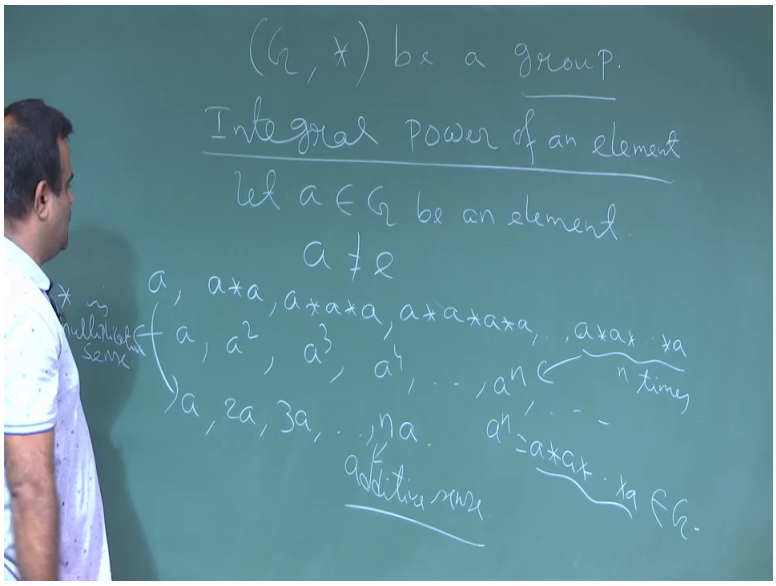
Now, the inverse. Inverse is basically for a given a belongs to G there exist a b which we denote by a prime such that such that if we operate a with a prime in both the way this is. So, it is also right inverse, left inverse and right inverse left inverse are same that is the inverse and this e this, this is also unique this is a unique. Now, if this four property satisfy then we say this algebraic structure G along with this operator binary operator this structure is form a group, ok.

(Refer Slide Time: 03:12)




Now, we talk about ordering of an element. So, so, the integral power of an element we talk about of an element from G. Let a be an element from G, any element. Now, if we suppose a is equal to e identity element, then if we operate a star a, this will basically e star e so, this is e. So, e e star e all are basically e e star e star e, ok, but if a is not e a is not the identity element then what we do we keep on this is the integral power of an element we keep on apply a with itself.

(Refer Slide Time: 04:19)

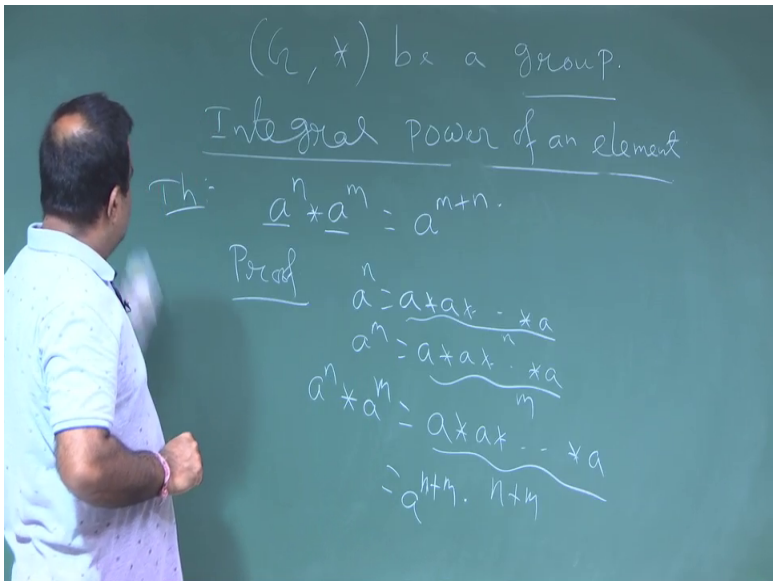



So, like we want we. So, a is an element so, a star a will also be an element because of closure property a star a star a three times we are operating like this a star a star a star a four times like this dot dot dot this way you continue, ok. Now, this is a, we have so, this is continued. So, in general this is a star a star a say this is n times. So, this we denote by say a a square, a cube, a to the power 4, a to the power n this one if our star is in multiplicative sense this is this is when the star is multiplicative sense multiplicative sense then we multiply; multiply means a into b kind of thing. So, a into a is a square like this.

So, this is just a notation, but if the star is it a additive sense then this will be written as the star is it the additive sense this operator then this will be a 2 a, 3 a, dot dot dot na so, this is the additive sense. So, if star is additive sense, but anyway in general we will just this a, a will mean the a a to the power n we mean the a star a star a n times and this will be belongs to G because of closure property. So, this is the integral part of a we keep on applying a with the with the elements and by closure property this will be a.

Now, we say this is so, this is how we defined the a to the power n this is the in integral part of the element a to the power n or in the additive sense n a if it is if the star is the additive sense, ok. So, now, you will have some property before we go to the defining the order of an element, ok.

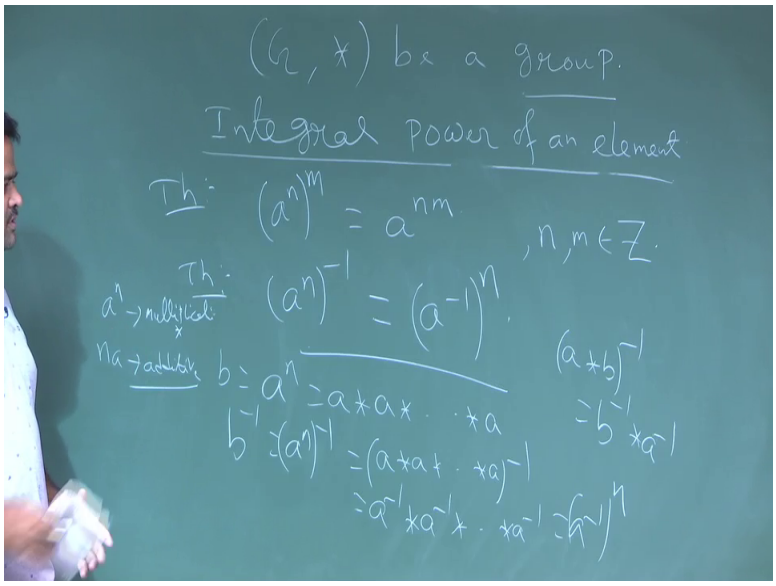
(Refer Slide Time: 06:54)




So, first property is a to the power n into means suppose now star is in multiplicative sense a to the power n is equal to a to the power m plus n, this is our star. So, this is also star, this is also star a a m times n times a this is quite obvious because this a to the power n is basically a star a star n times then we have a to the power m this is also a star a star this is n times and this is m times.

Now, if you multiply these two if you operate these two again and here to the power means we are taking the operation in multiplicative sense, but it could be additive sense also then it will be a a n a plus m a then it will be m plus n a, anyway. So, now, we if we do the star with this two then it will be basically a to the power a times a times a this is total is this n times m times total is n plus m times. So, this is basically a to the power n plus m this is just a this one.

(Refer Slide Time: 08:40)




Now, another result is suppose a to the power n to the power m. So, this is nothing, but a to the power n m. So, this nm are all coming from natural number set I mean or it could be integer. So, set of integer any number these are any integers, this could be negative also now this is also can be easily proved because this is a to the power n m times each of having n operator n times. So, total is n into m times.

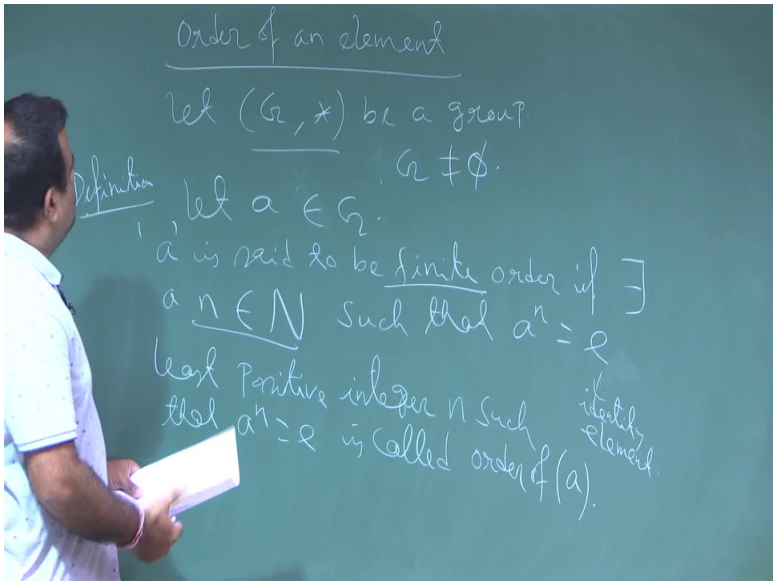
So, another result is a to the power n to the power minus 1 this minus means minus 1 means the inverse. So, this is nothing, but ok. So, this is this is what this is the in. So, what is a to the power n a to the say b is equal to a to the power n this is basically a star a star a n times, ok. Now, if you take the inverse of this is basically this is an element. So, this is basically inverse of this a star a star inverse.

Now, this is we know the result a star b inverse is equal to b inverse a inverse this is means inverse. It is it is the multiplicative sense operator. So, that that is why it is in inverse. So, that is why it write in this way to the power minus 1 otherwise if it is a additive sense then you have to write minus of a to the power n, but anyway. So, this is basically if we apply this and this is true for more than two also. So, then it will be a inverse a inverse n times. So, this is basically a inverse to the power n. So, this is this result is true, ok.

So, you can have some more result on this power of an element. This is power because we are telling this is power as we consider this operator as a multiplicative sense

otherwise if it is additive sense instead of a to the power n a to the power n is multiplicative sense multiplicative sense the star, but if the star is additive sense then it is n a additive sense. So, depending on the, but the meaning is a to the power n meaning is n times we operate a with itself same meaning n a means n times we operative a with itself.

(Refer Slide Time: 11:49)



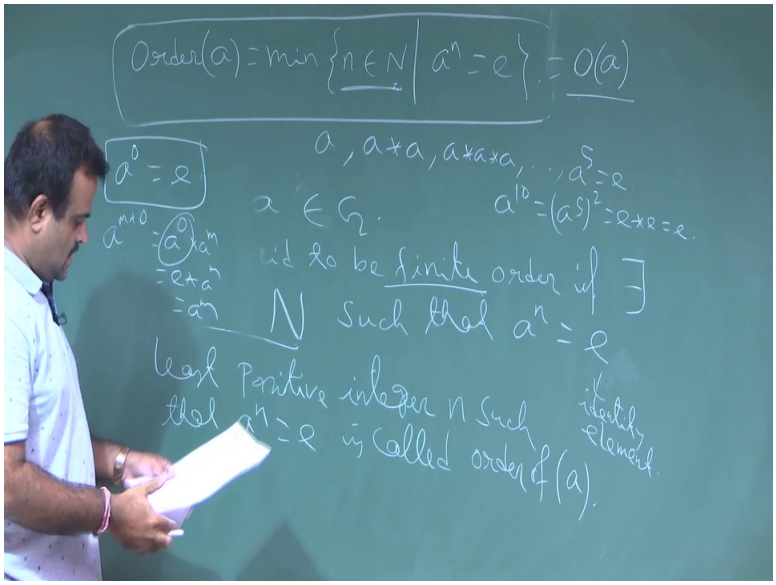

So, now we define ordering of an element order of an element ok. So, so, again let G be a group non empty group. Is there any empty group? I mean if G is empty then there is no element exists there. So, that G be a non empty group means G is not equal to phi, and let a be an element from G any arbitrary element we take now, it we will talk about ordering of an element.

Now, a is this is the definition now a is said to be finite order said to said to be finite order element if there exists a natural number N N such that a to the power N is equal to e e is the identity element from the group if we if we if there is only one group. So, we can write e g or e e is because there is you are just till now you are just G is the group. So, e is the identity element this is the identity element of the group ok.

So, if such an n exist if such natural number finite if there exists a finite order if such N exists, so, that means, what? That means, exist then we say this is having a finite order and the order of the group is basically the mean the least n which satisfying this, ok. And, the order of the group the least n least positive integer n such that a to the power n is

equal to e is called order of the group is called sorry order of that element order of a, order of that element, ok.

(Refer Slide Time: 14:55)




So, basically this is basically the order of an element a is basically the minimum least element among all n such that a to the power n is e this is the how we defined the order of the element. Quite minimum because see we are keep on say we have an element a. So, we are keep on applying a a square a cube and suddenly say a to the power 5 is giving us e first time this is the minimum one.

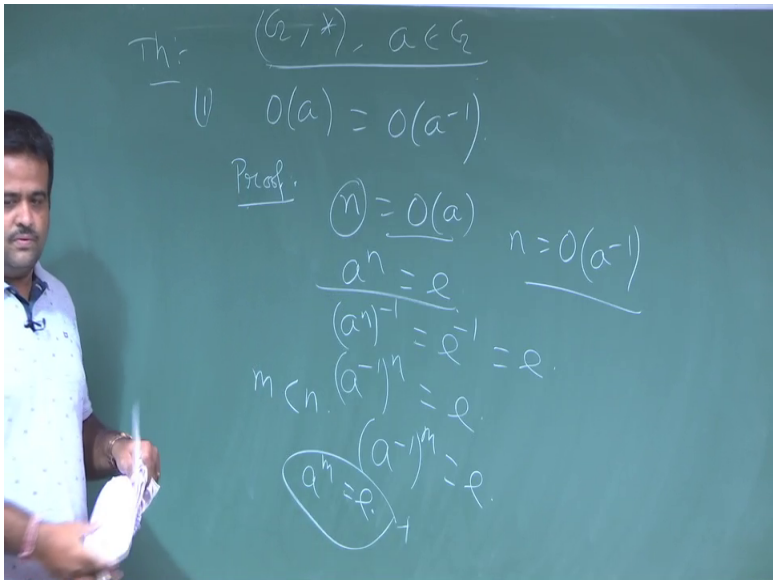
Now, if a to the power 5 is e then a to the power 10 is also e because this is basically a to the power 5 square. So, e square e star e e. So, any multiply if a if a to the power n is e then the a to the power 2 n is also a to the power 3 n is also e. So, these are basically giving us the identity element this power, but we need to that is why we need to choose the minimum one the least one we will give the least one is represent as order of the element and we denote this by this symbol or in short we sometimes denote this by order of a like this.

So, here order is 5 if the 5 is the first natural number such that a to the power 5 is e. Order may exist may not exist if such n such finite n exists finite n is there then we say order exists otherwise the order is infinity kind of thing.

Now, the convention is this is natural number because convention is a to the power 0 we take to be e if this is the convention a to the power 0 is 0 time we are operating with a we are not operating with a.

So, that is the convention we take them to be e because this field because we know the a to the power m plus n is a to the power n a to the power m, now, if you take n to be 0 or m to be 0 so, this is 0 so, this is 0. Now, this is basically e star a to the power a. So, this is the convention a to the power 0 is e ok. So, that is why we take the from natural number set this order, ok.

(Refer Slide Time: 17:56)



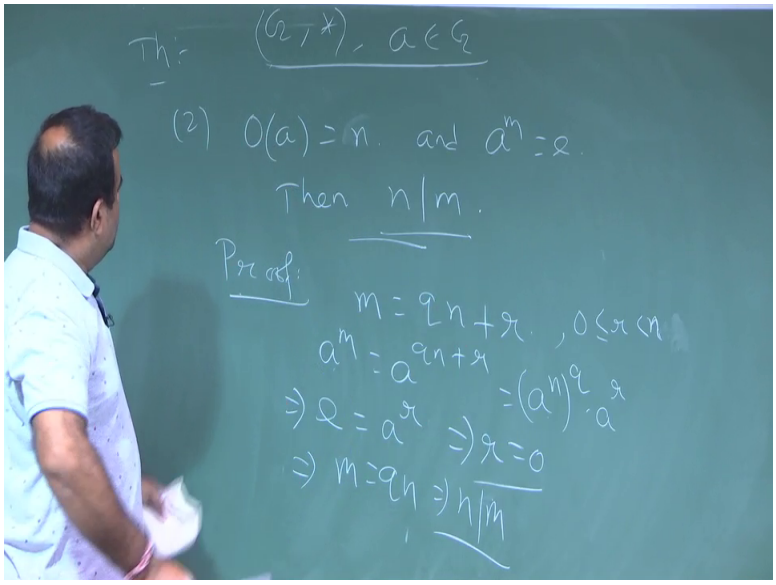

So, now, we will talk about if such finite n exists then we call this is the order of an element, ok. So, now, we talk about the, we talked some of the properties of this order of an element, ok. So, this is the first property. So, again we have a underlined group and a is an element from G that this first theorem is telling us order of a is same as order of a inverse they both have same order how to prove this? Is this trivial? Anyway, unless we convince nothing is trivial. So, how to prove this? So, order of a suppose n is the order of a. So, n is the minimum element which is giving us a to the power n to be e the identity element of the group.

Now, what we can do here we can just take inverse of this a to the power n inverse is equal to e inverse e inverse means what it is basically e. Now, we have seen this is this result this is basically e. So, this is basically e now this is giving us n is the integer which

is basically giving us a to the power a inverse to the power n is equal to e. Now, this n could be the order of a inverse, but for that we need to check whether there is any other m which is less than n such that this is e.

This is not possible because if this is happening then again we take the inverse then it will give us a to the power m is equal to e which is not possible because this is the minimum element from the natural number set such that this is happening. So, this is not possible this is the n is the. So, n is the order of this. So, this is the logic this is the proof, ok.

(Refer Slide Time: 20:18)

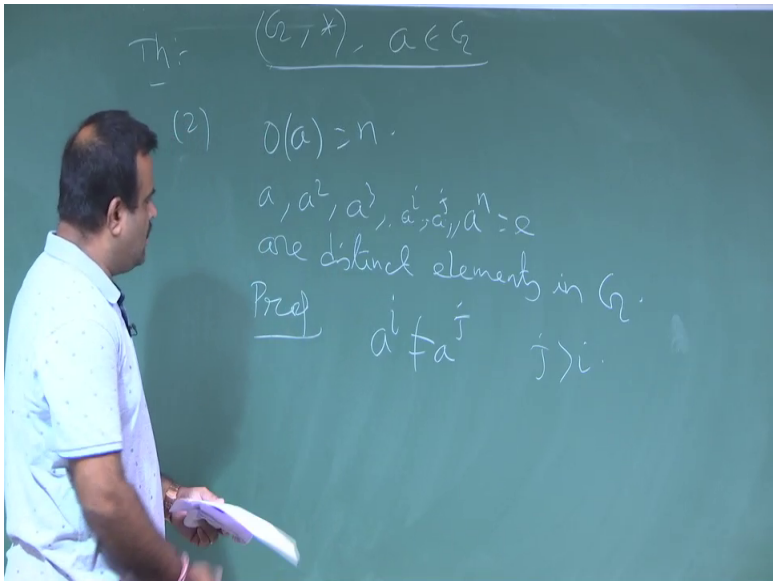



Now, the second one is second property is if the order of a is n sorry n and if a to the power m is e then n must divides m n must divides m because this you have to prove intuitively this is because m is the mean n is the minimum element minimum integer such that a to the power n is e. So, now, if any other integer divides m then n must divides this. So, how to prove this, ok.

So, we can write this is by the. So, if we want to divides n by m. So, n can be written as q m plus r, where r is the remainder 0 less than r less than n minus 1 less than equal to n minus 1 or less than n, ok. Now, what now we can just write a to the power m a to the power m is basically a to the power m is basically a to the power q n plus r. Now, here we can just write this as a to the power n to the power q into a to the power r.

Now, this we know this is e. So, this implies e is basically equal to this is we know e. So, this is a to the power r now r is less than n and n is the order of the group. So, n must be the minimum one so; that means, this imply r to be 0 otherwise if r is not 0 which is less than n then r could be the order of the element a. So, this implies this implies m is q n. So, this imply n divides m ok, this imply n divides m this is one of the property.

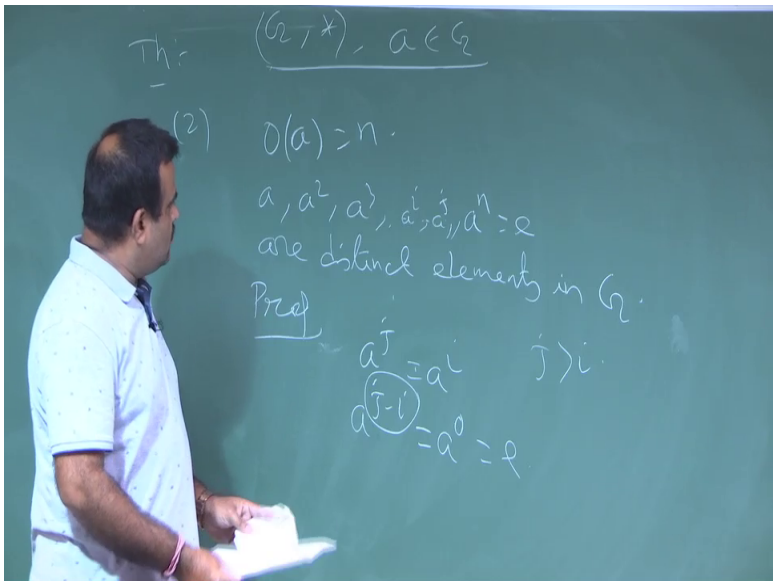
(Refer Slide Time: 22:59)




Now, the next one is just we will quickly go through some of the properties these are we can verify easily, ok. Now, this one the if we have a order of an group is n then a, a square, a cube this set a to the power n which is nothing, but e these are basically distinct element in G. These are distinct elements in G so; that means, no two element will be same; that means, if we take so, if you take to i and j here a to the power i a to the power j any arbitrary i and j.

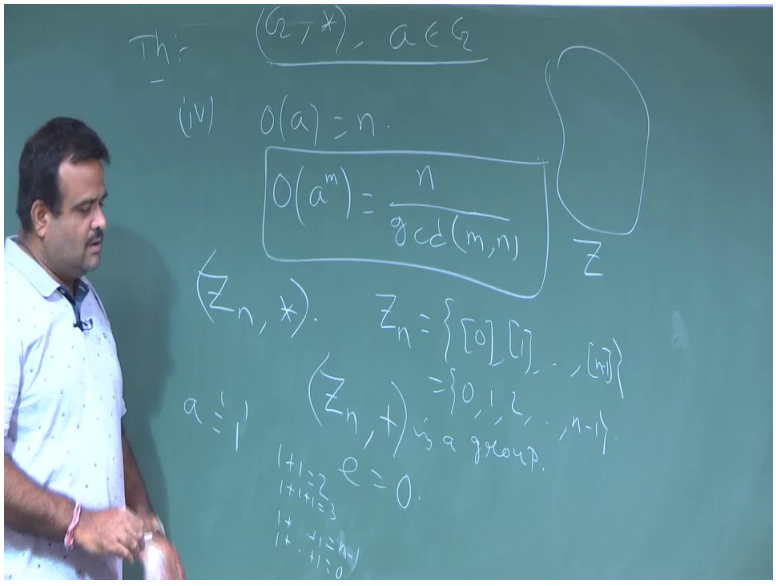
So, we our claim is this is telling that a to the power i should not be equal to a to the power j ok, where say j is greater than i.

(Refer Slide Time: 23:57)




Because if they are same suppose a to the power j is same as a to the power i then what we can say from here we can just say a to the power j minus i is basically a a to the power 0 which is you know this is e. So, that means, this is basically a j minus i is less than n and j minus i will be a order, but it is order is n. So, this is the argument. So, if n is the order then if we operate keep on operate n with itself then up to a to the power n this will form a distinct set of operation.

(Refer Slide Time: 24:46)



Now, the next result is this is number 4. Suppose, we have the order of an group a n then order of a to the power n is basically n by gcd of m comma n, ok. So, this is also as of the result this way I am not going to prove now, ok.

Now, we will talk about Z n Z n star. So, Z n star is basically we know Z n is basically 0, 1 this set ; that means, if we take an integer set and if we take a natural number n and if we divide this by n this is the all possible remainder sorry up to n minus 1 for simplicity we can write 0, 1, 2 up to n minus 1, ok.

So, now if we just. So, we know this Z n star this is a group, ok. Now, if we take a element one and this is a group with e is 0. Now, if you take a element 1 a is equal to 1 then the what is the order of this element? Order of this element will be n because if we take 1 plus 1 which is 2. So, these are all giving the distinct elements. So, 1 plus 1 plus 1 is 3 like this. So, up to 1 plus n times it is giving us n minus yeah n minus n. So, n means 1. So, n is c it is so, n minus 1 time it is this and n times it is giving us n which is mod n is 0 ok. So, this is basically giving us so, order of an element 1 is basically n. This is an example where the order of an element we have checked is to be n, ok.

So, in the next class we will discuss the cyclic group and the sub group also.

Thank you.