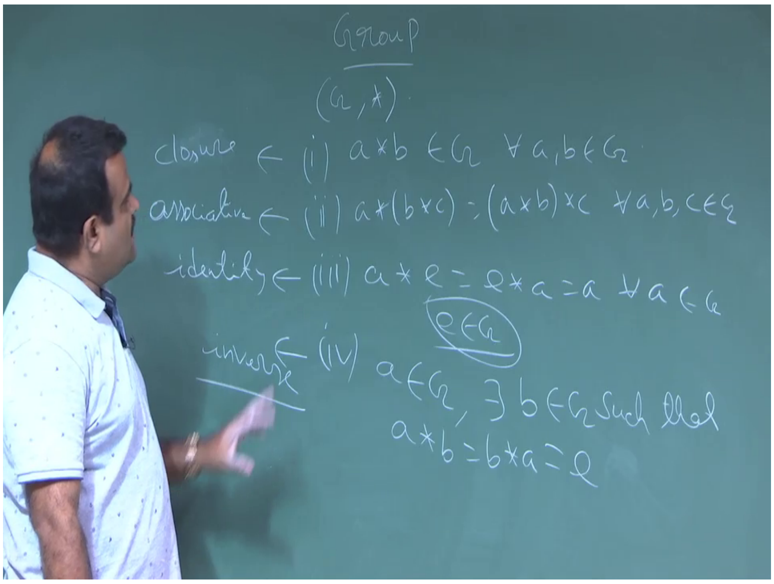
Introduction to Abstract and Linear Algebra
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture – 11
Group

Ok. So, we are talking about group. In the last class we defined the group.

(Refer Slide Time: 00:21)

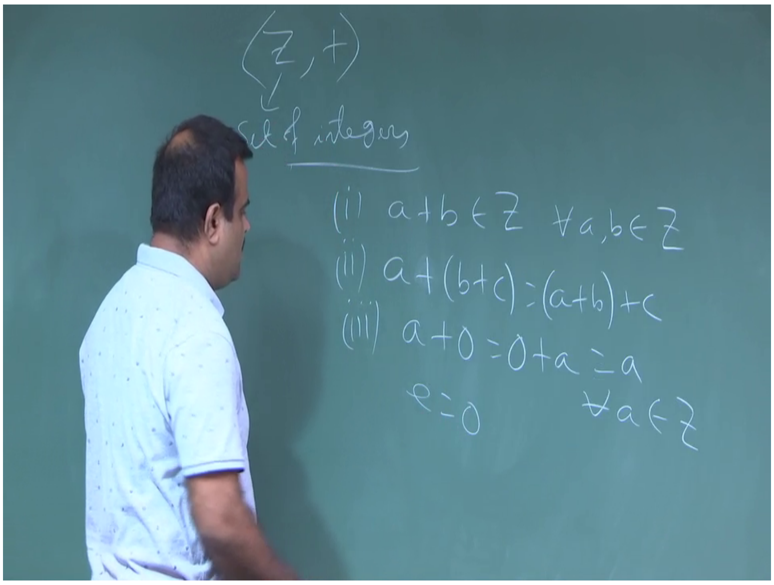


So, today we will take some example of groups and then we will discuss some of the properties of the group element. So, just to recap so, group is basically we have a set G and we have a operator. So, we have this properties closure four property must satisfy for this algebraic structure; first one is closure this is the closure property, then the associativity property for all a, b, c belongs to G, then the identity existence of identity a star e is equal to e star a.

So, such e exists. So, this is the identity element e is belongs to G such a e exist. Then the inverse so, every element has a inverse. So, if a is belongs to G then there exist a b such that, a star b is equal to b star a is equal to e for all no not for all this is the, this is inverse of a. So, b is called a inverse of a if this four property satisfied, then we called this algebraic structure is a group.

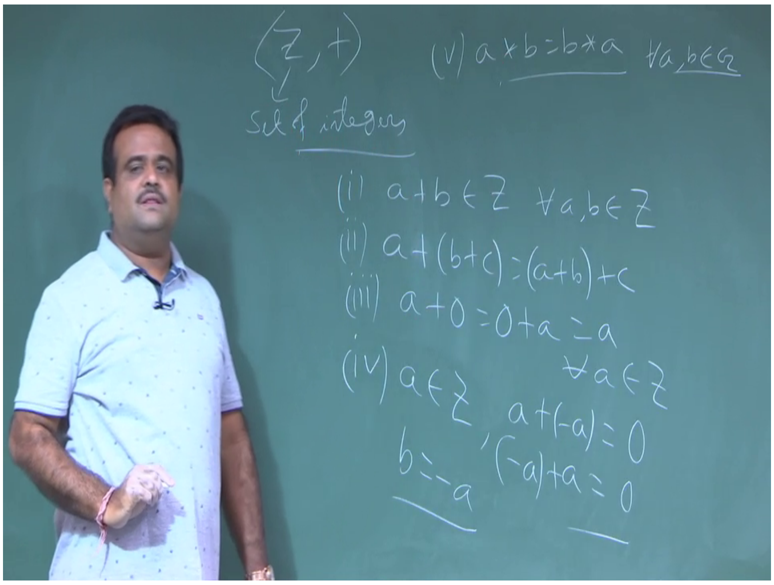
So, now we will discuss we take some example of a group and then we talked about. So, this is just to this is the closure property closure property this is the associativity property this is the existence of identity and this is the existence of inverse, ok. We will see will we will prove that this e is unique the identity element is uniques and also we will see that is b is unique. So, every element has a unique inverse. So, those theorem those result will prove, but before that let us take an example of a group.

(Refer Slide Time: 03:08)



So, this is let us take some example of a group Z plus Z Z is the set of integer. So, you want to check whether this is a group or not. So, for that first half of closure property so, we know if you take two integer their addition is also an integer this is a real number addition so, a plus b, b is belongs to Z for all a b. So, this is the closure property is satisfying and we know the plus is a associate plus is associate operation identity element. So, we know that 0 sharp as a identity element because a plus 0 is 0 plus a is equal to a this is for all a. So, 0 is the 0 is our e. So, 0 is our e; e is the identity element. So, there exist identity element.

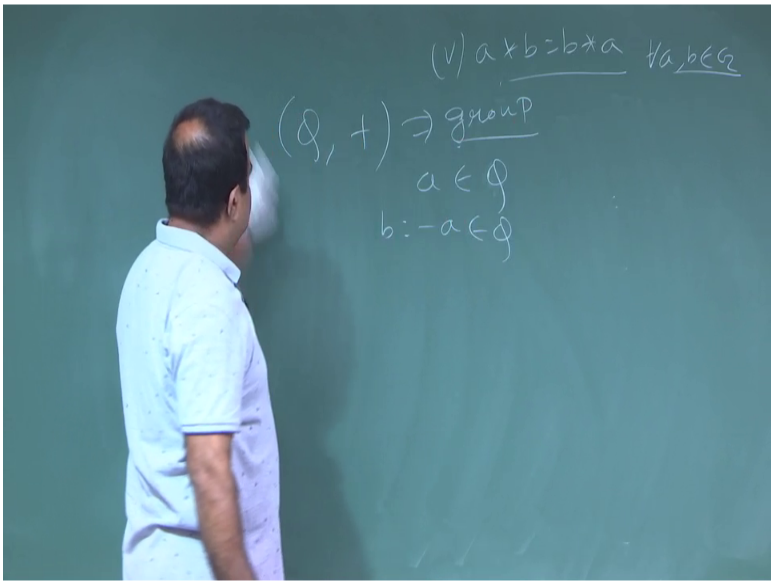
(Refer Slide Time: 04:17)



So, e now, the inverse if we take an element a from Z now we must have a b from Z such that a compose with b must give us identity. So, that means, in the what is b? B is minus a basically. So, a plus of minus a is equal to 0 or also we can write minus a plus a is equal to 0. So, this is basically our b is basically minus a. So, every element has a inverse. So, that inverse is basically minus a under this operation plus.

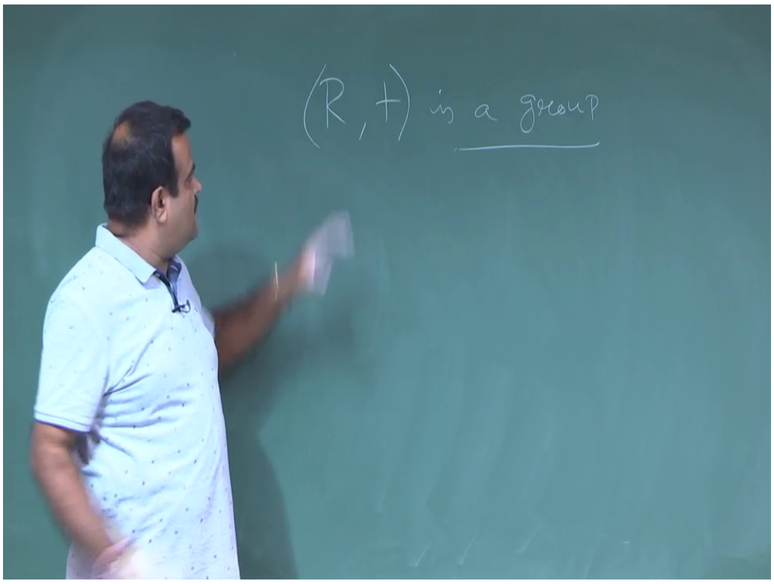
So, this is basically a group not only group this is also Abelian group because we have for Abelian group we need to have the property the another property fifth property a star b is equal to b star a for all a, b if this is satisfied then this star is Abelian or commutative and then the corresponding group is called Abelian group.

(Refer Slide Time: 05:36)



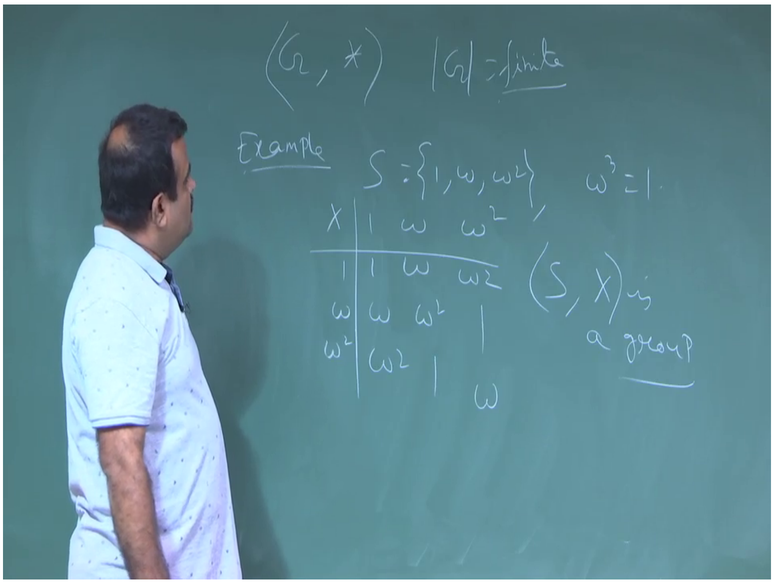
Now, another example of a group is the set of all rational number along with the plus or dot this is also a say no dot multiplication we have a issue with the inverse 0 with the 0 will come to that. This is also a group because if you take any two natural number rational number if you add it up it will give a rational number closure associativity is satisfied because this plus is associate operation then 0; 0 is also a rational number 0 is the identity. So, this is a group when the inverse is also exist if you take a rational number a then minus a is the inverse. So, this is a group this is a another example of a group.

(Refer Slide Time: 06:32)



Similarly, R R plus set of all real number. This is also a group. These are all groups now these are all infinite group. Now, can you have some finite group like finite group means number of element is finite the cardinality of G cardinality of that G is finite.

(Refer Slide Time: 06:58)



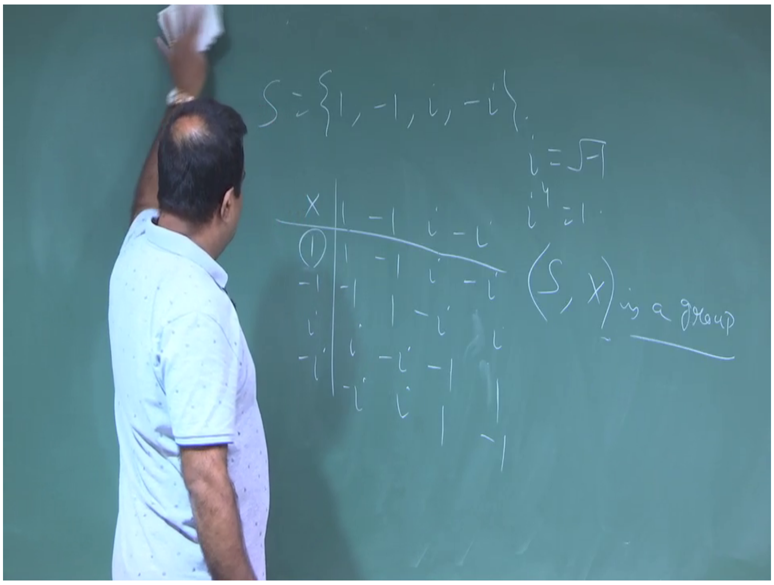
So, you want to just construct some finite group. Finite group means cardinality of G must be this set is finite set, ok. So, we just take some example of finite group say if we have a S – 1, w, w square. So, w is the cube root of identity. So, w this is w cube is equal to one.

Now, we define the multiplication when we just take the real number multiplication we just take the multiplication on this. So, so, multiplication means so, this into. So, if you take this w, w square one w since this is finite we can have the table to denote this operation. So, if you multiplied with 1 this will give us this if you multiplied with the w this is w, w square now w cube is basically 1. So, this is w square w cube is 1, w to the power 4, w to the power 4 is nothing, but w.

So, this is closure and we can very well check this is also associativity is satisfying and then we can check the identity. One is the identity element here because if we multiply 1 with this it is giving us the. So, 1 is the identity and the inverse every element has a inverse what is the inverse of w? W inverse is basically w cube and what is the inverse of w square sorry w square what is the inverse of w square? w square inverse is basically w. So, every element has a inverse.

So, this set is group is a group and they are finite number of elements. So, this is a finite group.

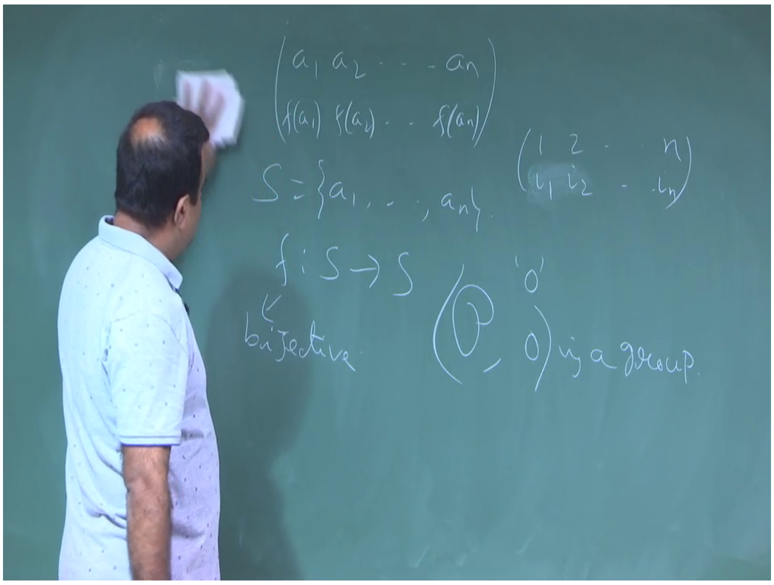
(Refer Slide Time: 09:12)



Another example we can take one finite group like say 1 minus 1 i minus i and if you take the multiplication, and i to the power i is basically square root of minus 1. So, is i to the power. So, i to the power 4 is basically 1, ok. So, this is the complex number and if we define the multiplication on this then we have say 1 minus 1 i minus 1 1 minus 1 i minus 1. So, 1 minus 1 i minus 1. So, if you multiply with the minus 1, 1 minus i plus i. So, plus i we are not writing. So, again this is i minus i i square i square is minus 1 then minus i square plus 1, then minus i plus i then minus i square is 1 then plus i square is minus 1.

So, this is we can very well check this is a group this is closure property, associativity property and identity element is basically 1 and inverse is basically every element has a inverse because for i what is the inverse the one is here. So, i inverse is minus i. Similarly, minus i inverse is i. So, this is one example of a group. So, S this is a group.

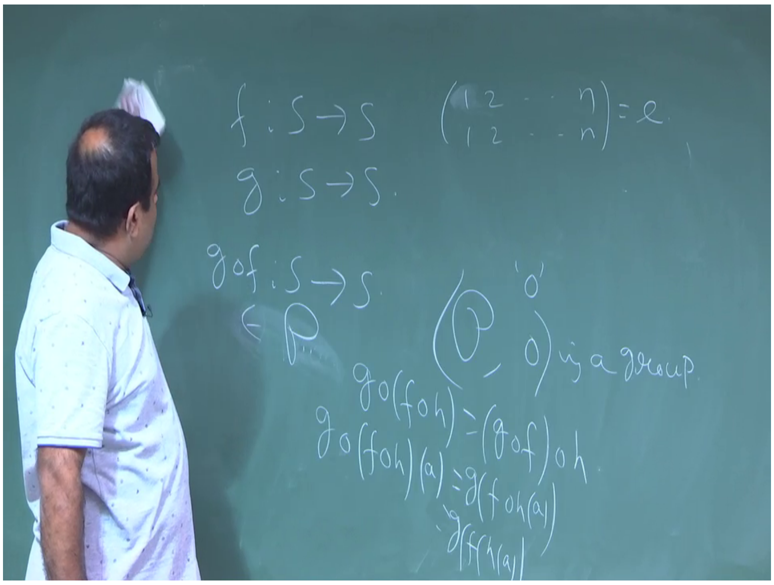
(Refer Slide Time: 11:20)



Now, another example could be the permutation, ok. If you take the permutation suppose there are n numbers, so a 1, a 2, a n now if we take this permutation f of a 1, f of a 2, f of a n. So, basically our S set is a 1, a 2, a n and permutation is a mapping from S to S bijective function it is a bijective function any bijective function on S to S is called a permutation.

Now, if we for simplicity we can take this as 1, 2, 3 up to n and these are some f 1 say i 1, i 2, i n for simplicity we can take. Now, if we define the composition, composition up to permutation like we know how to define the composition up to permutation we can see that this set of all permutation if we denote by this P along with this composition this is a group, ok.

(Refer Slide Time: 12:43)

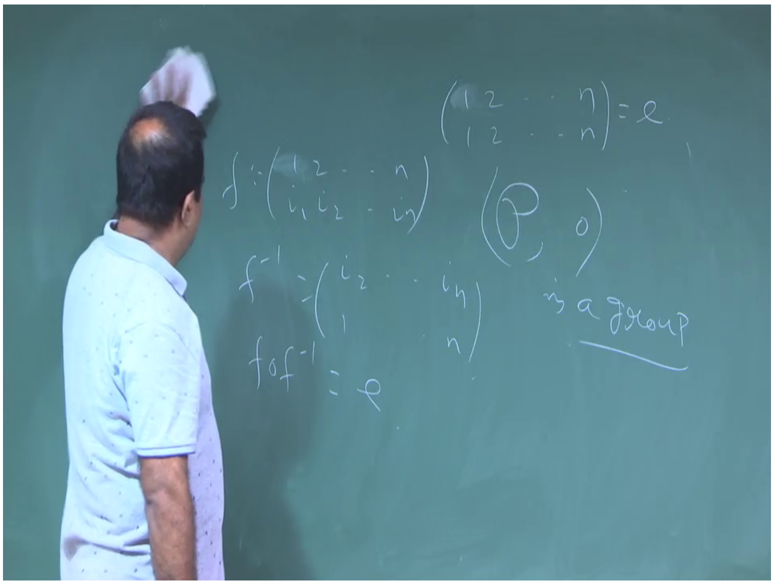


So, why so, what is the closure property means if we take two bijective function from S to S, S to S if it is two bijective function then we know this composition is also a bijective function. So, this is also a permutation. So, this is also belongs to this the closure property is satisfying.

Now, associativity property means, if you take this we can easily verify g cross f cross h is equal to this is also we can easily check that because this is nothing, but if you take a g cross f cross h on a this is nothing, but what we first apply this g of f of this and this is nothing, but g of f of h of a and if we do on this it will give us the same element. So, this is associativity and then identity element we know the identity permutation like this one 1, 2, 3, 4, n, 1, 2, 3, 4, n this is the e this is our e identity permutation because if we compose with any other permutation it will give us the, that permutation.

So, this is an identity element now inverse we know if we have a permutation and then we know the inverse permutation also exist because this is a bijective mapping.

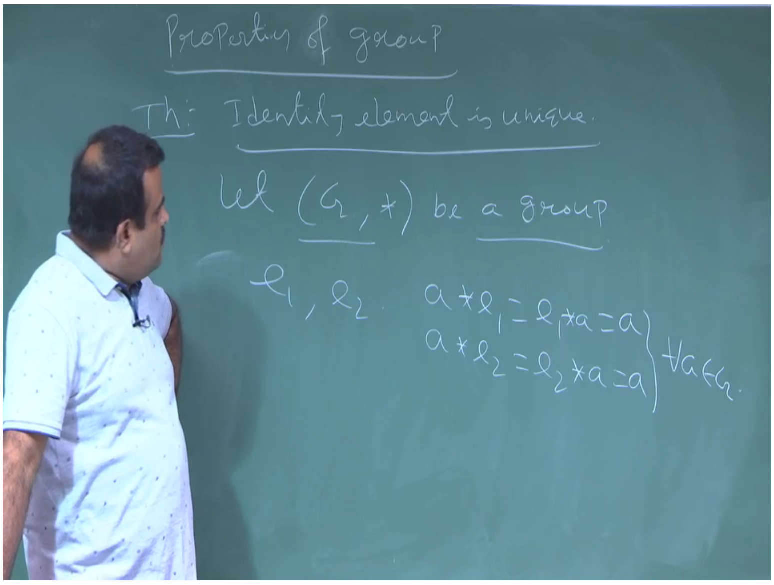
(Refer Slide Time: 14:18)



So, f inverse exist and f inverse will give us a so, so, 1, 2, to n, i 1, i 2, i n this is this is a then f inverse is basically i 1, i 2, i n we have to change the ordering to make it 1 to up to n this is our f inverse and this if we do the f compose f inverse, it will give us e that identity permutation. So, inverse exist. So, this is a group set of all permutation along with this composition this is a group, ok. Anyway there are many other examples of group.

Now, we move to the some of the properties of the group like identity element is unique, then the inverse of an element is also unique, then some of the other properties.

(Refer Slide Time: 15:17)

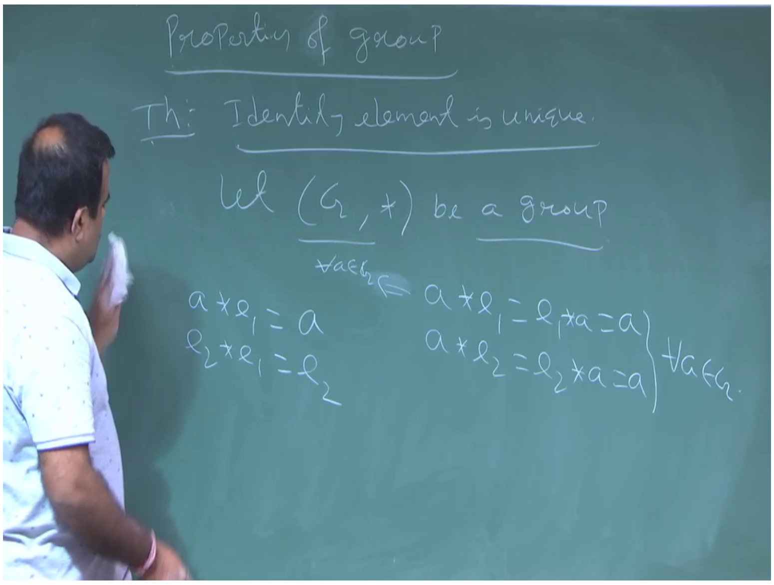


So, these are basically called properties of properties of a group, ok. So, first theorem is first property is identity element is unique identity element is unique. So, that means what? Suppose, we have a group G that G be a group. So, group means it has identity element and that our claim is that identity elements has to be unique, if possible say it is not unique.

Suppose, there are two identity element e 1 and e 2 suppose there are two identity element e 1, e 2. So, both are identity element; that means, what a star e 1 is equal to e 1 star a is equal to a and also e 2 is also identity element. We assume if possible let us assume there are two identity element then we will see e 1 is basically same as e 2 that we have to show and a star e 2 is equal to e 2 star a is equal to a and this is true for all a belongs to G.

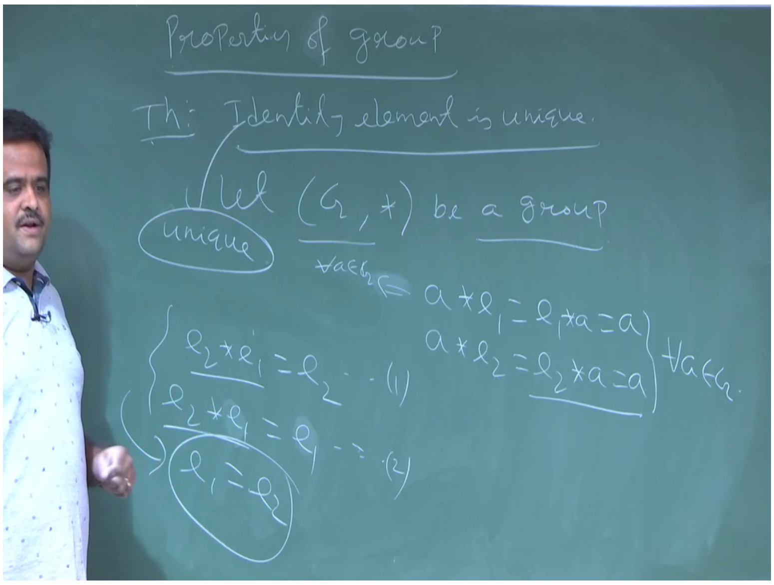
So, now we have to show that this two are same. So, how to how to show that?

(Refer Slide Time: 17:11)



So, now, we know that e star a star e 1 is equal to a. So, now, we just take it to be a to be e 2. So, e 2 star e 1 is equal to e 2 because this is true for all a, this is this is operation is true for all a all a belongs to g. So, it must be true for e to also. So, this is e 2.

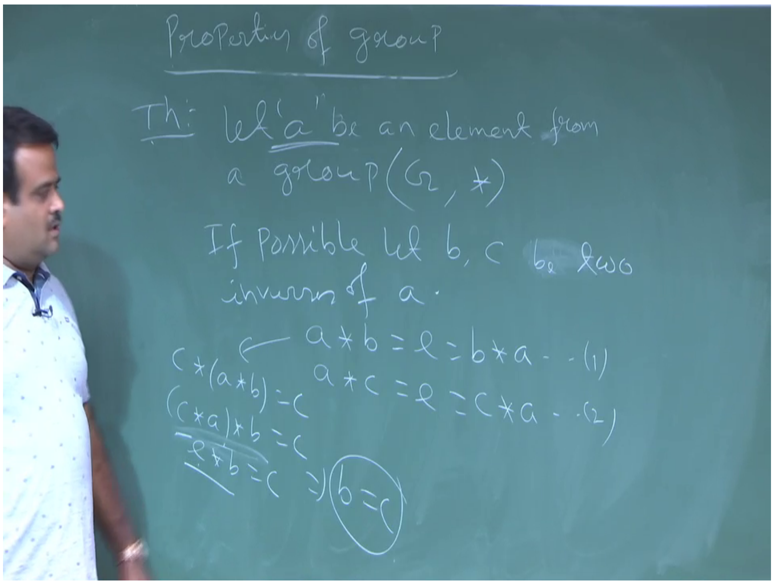
(Refer Slide Time: 17:46)



Now, this is equation-1. Now, we have here this one e 2 star a is equal to a. Now, this is also true for all a now if you put a to be e 1. So, this is basically e 1. So, now, these two are same because it is a binary operator. So, from these two we can say e 1 is equal to e 2, ok. So, this is the proof of this e 1 is equal to e 2.

So, that means, this e is unique the identity is unique. So, we will not have two different identity elements. So, identity element is unique.

(Refer Slide Time: 18:54)



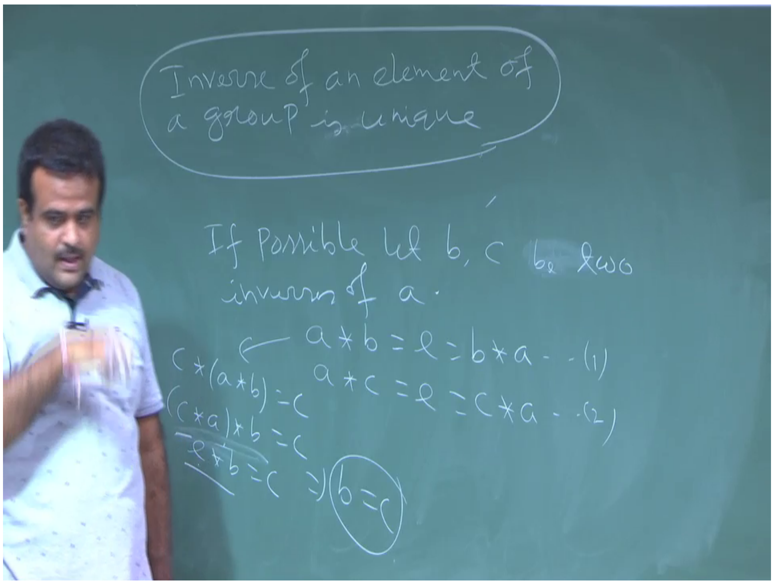
So, now, we will show that inverse is unique for a given a we have a inverse. So, for a given a let a be an element form a group G. So, we take a, we take an element a.

Now, we will see that ah. So, a is an element from a group so, that means, a must have a inverse. So, suppose there are two inverse if possible let b and c b and c be two inverse inverses of a. So, that means, what inverse we know inverses if we operate with a it will give us e in the both way and also if we operate with. So, b c is also another inverse. So, a, c is equal to e is equal to c, a.

So, now this is basically so, now, this is equation-1 and equation-2 now from here we need to show b is equal to c. So, how we can show this? So, if you operate c on both side from equation-1, from here if you operate c. So, c star a star b is equal to basically c now this way what is this is basically now star is associate. So, c star a star b is equal to c now, c star ac c is also an inverse. So, c star is basically identity. So, e star b is equal to c now, e star b is nothing, but b this should be simpler b is equal to c.

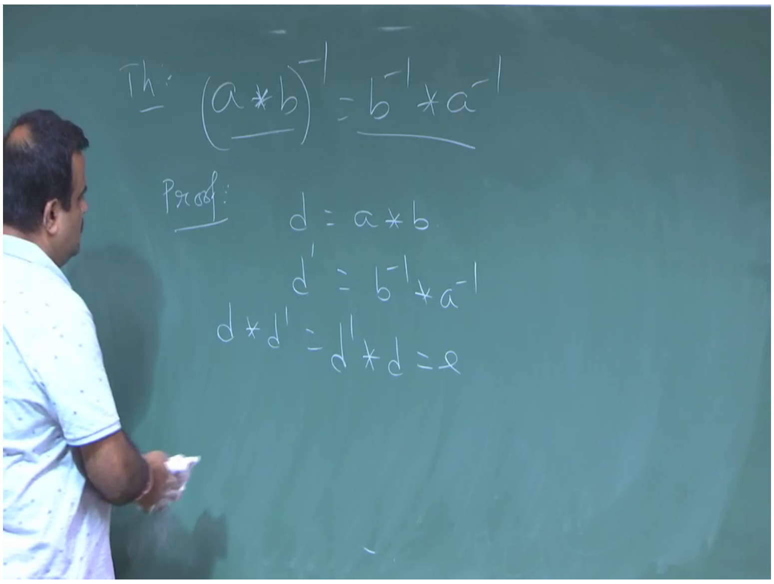
So, the inverse is also unique. So, every element has the inverse and that inverse is unique corresponding to that element. So, to write so, inverse is unique.

(Refer Slide Time: 21:30)



Inverse of an element of a group of an element of a group is unique. So, every element has a unique inverse.

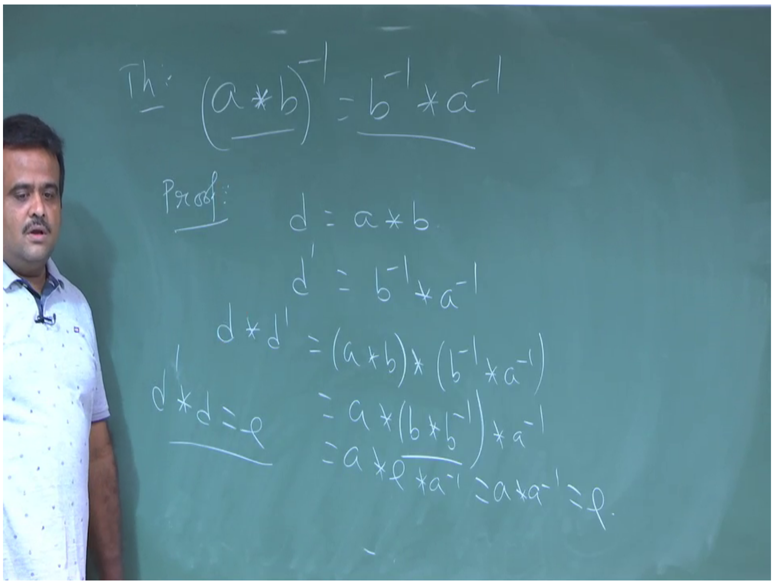
(Refer Slide Time: 22:08)



Now, so, another property is these are basically properties of a group so, theorem. So, a star b inverse we can write in this sense if the operator is in multiplicative way, ok. Suppose, the operator is multiplicative way we can write this way. So, b inverse star a inverse how to prove this. So, we have to show inverse of this is this now we take this as a some element d a star b and now we have to show.

So, this is say this is this is d star, we say d star d star is equal to now, if we can show d operate d star is basically d star operate this d is equal to identity element then we are done, then we can say d star is the inverse of d. So, the this way you can write. So, how to show this? So, we can just take d operate d star.

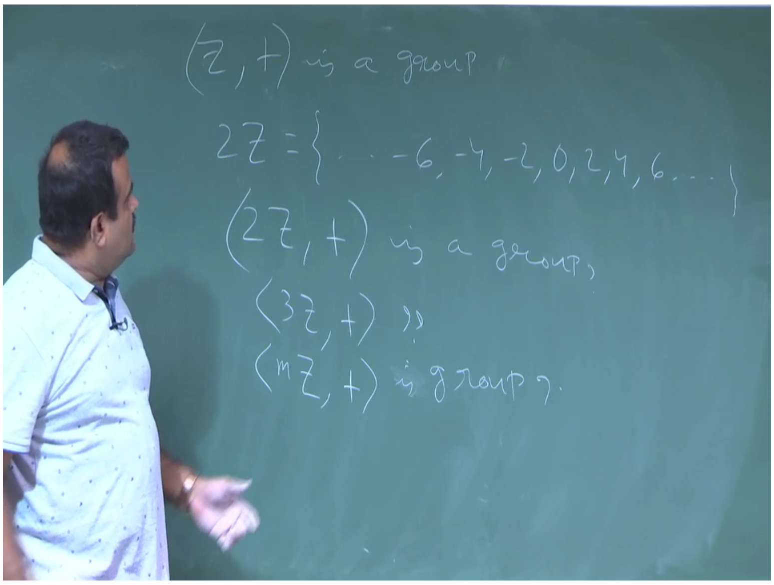
(Refer Slide Time: 23:23)



So, d is basically what d is basically a star b star d star d inverse star a inverse. So, this we can by associative law we can just write a b star b inverse. So, this is basically a this is the identity element because this is a group every element every. So, this is b inverse. So, b, b star is equal to identity. So, this is a star this is identity element.

Similarly, we can show d star, d prime d is equal to identity element. So, basically d prime is the inverse of d. So, basically d prime is the and d prime is nothing, but this so, this is the inverse of this ok. So, this is the, this is all the properties based on the inverse.

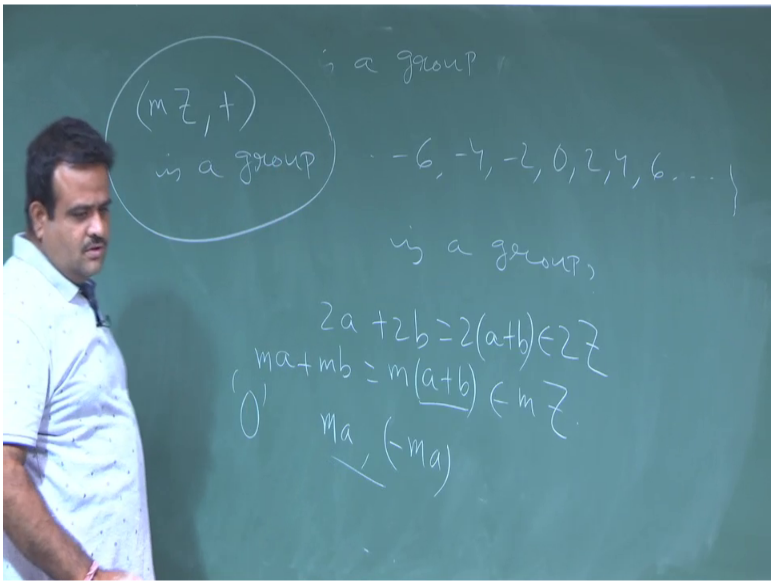
(Refer Slide Time: 24:41)



Now, we will defined order of a element in a group. So, before that let us just define say what do you mean by 2 z. We know that Z plus this is a group; now, if we take 2 Z, 2 Z is nothing, but the all even integers like minus 6 minus 4 minus 2 then 0, 2, 4, 6 like this all even integer.

So, this the question is this a group not only 2 Z if we have m Z say 3 Z is this a group 3 Z means we have just multiplied of 3 then m Z or k Z is this a group. So, now what values of m this will be group? This is our concern ok. So, now, if you take say this 2 Z is a group because associativity property is because this is associate now the question is the closure property.

(Refer Slide Time: 26:11)



Now, if you take 2 say 2 a plus 2 b. So, this will be 2 of a plus b. So, this is also belongs to 2 Z. Now, if we take 3 Z or m Z ma plus mb this is also m of a plus b this is also this is Z. So, this is also belongs to mZ an identity element 0 is the identity element for mZ and inverse? Inverse is also because if we have m a then minus of ma is the inverse of this because m plus minus ma is this. So, that means, this is also this is a group in general. So, mZ is a group mZ plus is a group ok. So, this is one of this is one of the example of a group.

So, in the next class we will discuss the discuss the order of an element, then order of an group so, cyclic group, then we will discuss the subgroup. So, we will discuss in the next class.

Thank you.