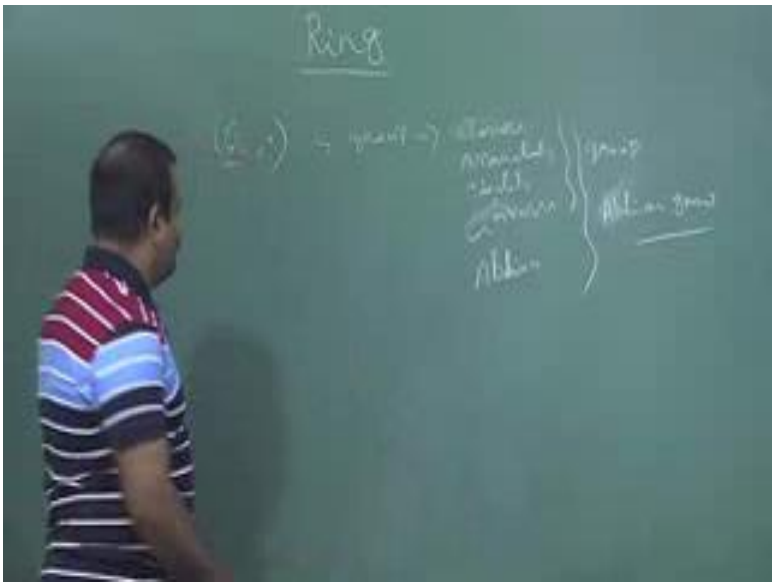
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 13
Abstract Algebra (Continued)

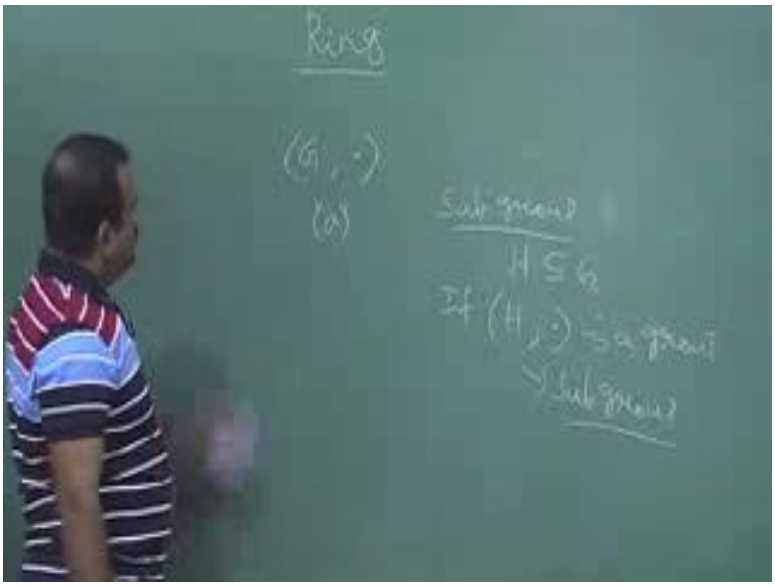
We will just talk about another algebraic structure is called Ring. So, before that just recap what we said about group and some more properties on the group.

(Refer Slide Time: 00:36)



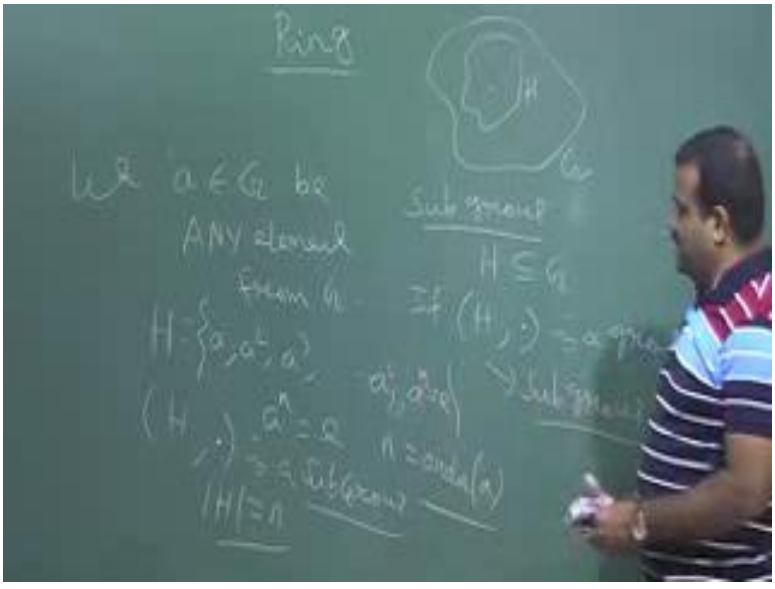
We have seen for a group, we need to have a operator we have a set G and we have a operator; binary operator dot and if it is groups is group if it satisfies the properties we have seen closer, closer, associativity, identity element, existence of identity element and inverse. So, if this 4 property satisfied then, it is a group and along with this if the extra property; commutative property or Abelian property, Abelian which is commutative sorry, Abelian then this is called the Abelian group, it is called Abelian group or the commutative group and then we talk about a cyclic group basically it is having a generator a. So, it is having a generator a, which generates the group.

(Refer Slide Time: 01:52)



Now, if we take so now, we talk about sub group; sub group is basically so if you take a subset of G which is basically say H. So, H is a subset of G now if H along with these form a group is a group then we called this is a, then it is called a sub group because it is a basically subse.

(Refer Slide Time: 02:37)



Now if we take an element from a, any element let a be a any element from G, now, if you take this set a square, a cube, like this a to the power i like this, so this is a subset because the closer property of G, all the elements must belongs to G. So, basically it is a

subset. So, we have a set G and we are taking a subset H from here which is basically the elements are basically generating by this element a.

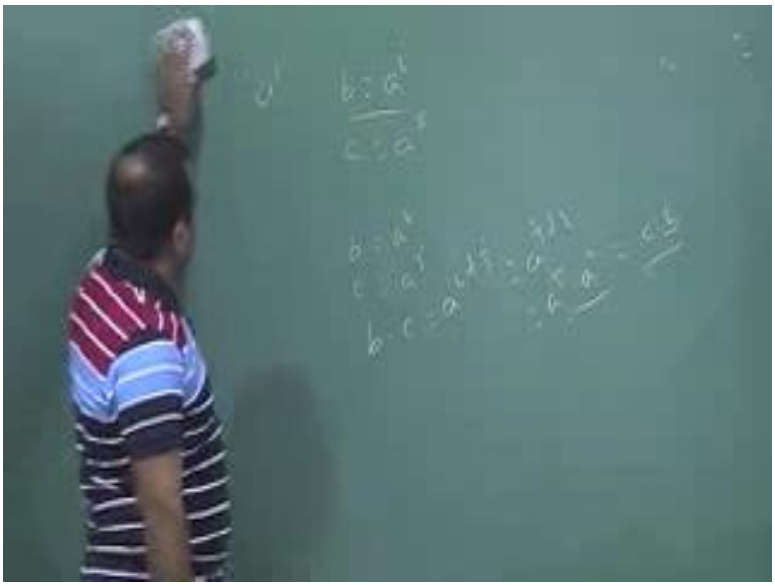
And then after sometimes it will give us the identity element say suppose that is a to the power n is equal to e. So, n is the least integer, least a, minimum natural number for which a to the power n is equal to e then n is called order of this element a or basically it is order of this. So, these will form a subgroup then this H along with this is a subgroup and this order of the subgroup is basically this n this is basically cardinality of H and this is also called order of that element. So, if you take any element and if you take the subset or subgroup generating by this element by keep on applying this element then it will form a subgroup and this subgroup is basically order of that element and there is a theorem which is telling Lagrange theorem that order of a subgroups divides order of the groups.

I will come back to ring. So, before that let us just talk about some properties of a group.

(Refer Slide Time: 05:03)

This theorem at any order of a subgroup divides order of a group so; that means, order of that cardinality of H divides a cardinality of G provided they are finite if they are infinite then this has no meaning because both are infinite I mean both could be infinity. So, provided there finite and order of this group order of subgroup divided. So, this is divide we will formally define.

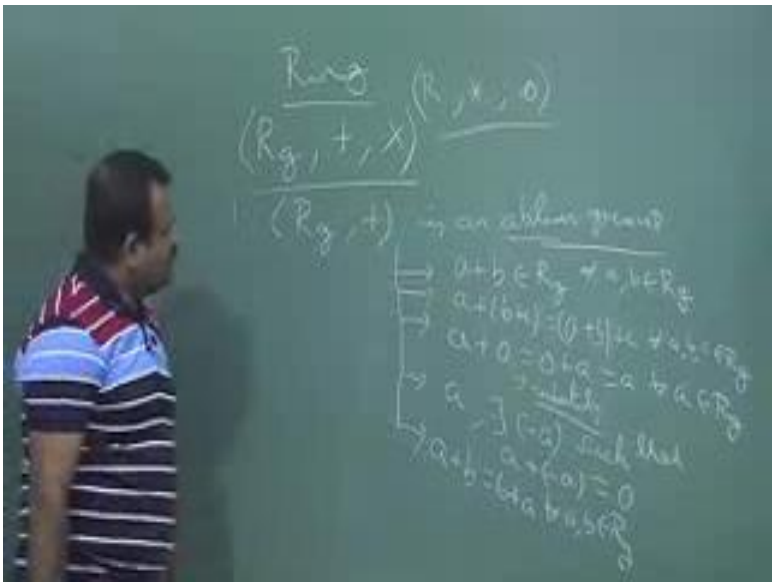
(Refer Slide Time: 06:03)



This is a subgroup, now we have seen a group is cyclic if it has a generator ‘a’ such that all the elements is of this, form c is another element, c will be of this form. So, basically a generates the groups then it is called a cyclic group if such a exist and then a is called a generator and this is Abelian group because in that case everything in this form every 2 element b c of this form a to the power i c will be a to the power j. So, b into c is basically a to the power i plus j which is basically a to the power j plus i which is basically a to the power j into a to the power i. So, this is basically c into b. So, it is always Abelian. So, every cyclic group is always Abelian.

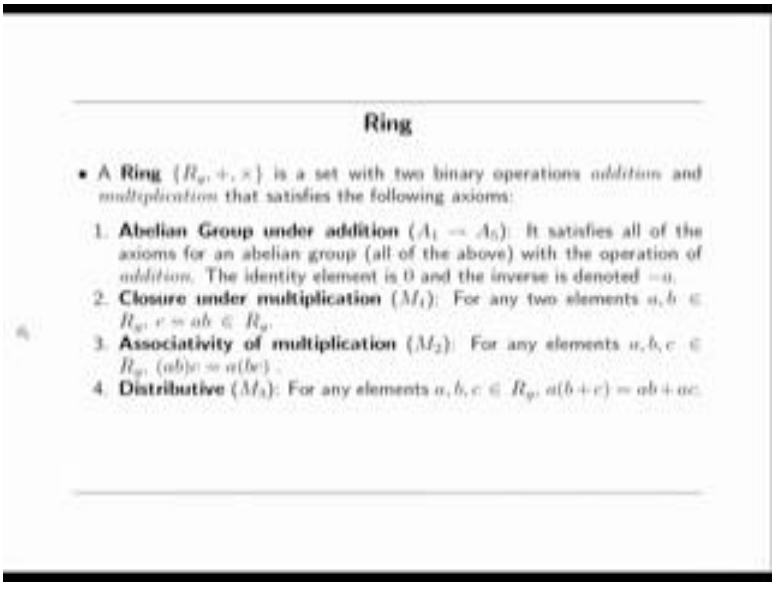
So, now, we will talk about the ring.

(Refer Slide Time: 07:00)



For ring, we have, we need to have a set g or this set is denoted by the Rg will just this is a ring that is why it is R and g is the set. So, Rg, but here we have 2 operation - one is plus another one is, one is additive cells another one is multiplicative cells. Here we have 2 binary operation - one is plus, one is multiplicative cells.

(Refer Slide Time: 07:33)



And this is our set and this is satisfied; if this satisfy following 4 properties then it is called a, this algebraic structure is called a ring. So, first property is telling it must be a Abelian group under the plus operation and then second property is telling with dot

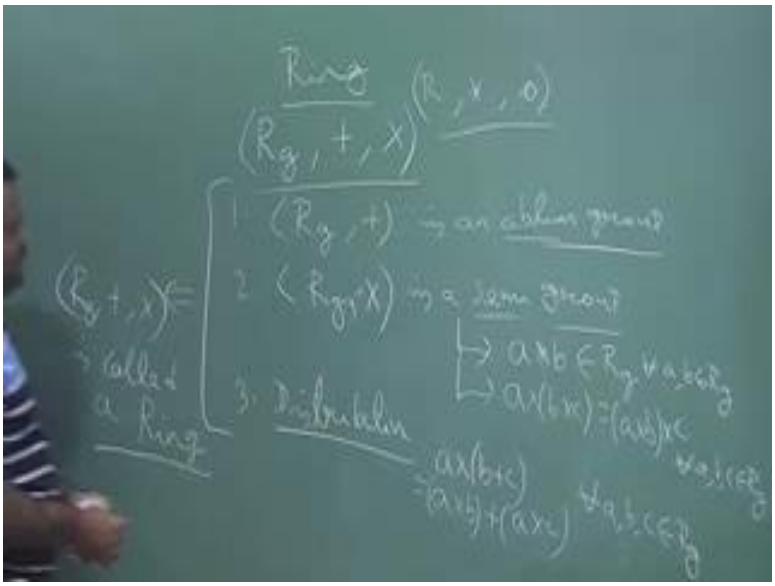
operation or with the multiplicative since it must be a closer property must satisfy that so; that means, it is a semi ring, another dot and some extra property like distributed property this is dealing with both the operation.

If this is satisfied then it is called ring. So, what it is telling? So, first of all this R, this set along with this must be a, is an Abelian group. So, Abelian group means it must satisfy these 4 properties, 5 properties like closer. So, if we have 2 elements a b, so a plus b must belongs to Rg for all a b belongs to Rg, this is the closer property and second one is associativity a plus b plus c must be equal to a plus b plus c and this must go for all a b c this is the associativity property. And third one is existence of identity, there must exist a identity element e which is for additive sense it is referred as 0, so a plus e that 0 is equal to 0 plus a is equal to a for all a belongs to this set and this is basically identity element under the plus operation.

And then the existence of inverse, so every element should have inverse under this operation. So, for a given a there must exist a inverse which is denoted by minus a such that such that a plus of minus a is equal to identity element. So, this is basically b. So, a operate b should give us the identity element. So, this is the existence of inverse. So, if this 3 4 property satisfied and it is a group.

Now, we need to have Abelian group so; that means, you should have the commutative property so; that means, a plus b must be equal to d plus a for all a b belongs to Rg. So, if this 5 property satisfied then it is a group under this binary operator plus. This is not a real number plus this is a operator we are just referring as a plus for simplicity, but do not, do not think that it is a real number plus always will check with a real number plus will form a ring or not. Yes it will form a ring, but this plus is you can think general operation instead of plus this we can use some star some another operator like this, we have a group R, we could use that. But anyway to simplicity we will refer plus and this as if additive sense one operation and another operation is in multiplicative cells this is for the simplicity purpose, but we put one can always derive all these things using the general symbol, but anyway what is there in the symbol. So, this is the Abelian group. So, it must satisfy these 5 properties.

(Refer Slide Time: 11:51)



Now next is this is on with the plus operation and then the next is with the dot operation it must be a semi group with the multiplicative sense, semi group. So, semi group means it is not satisfy 2 properties basically, one is closer property so; that means, for any 2 element a cross b or dot this is multiplicative sense it is basically this cross is belongs to Rg for all a b belongs to this set. So, this is the closer property and then the associativity also must satisfy.

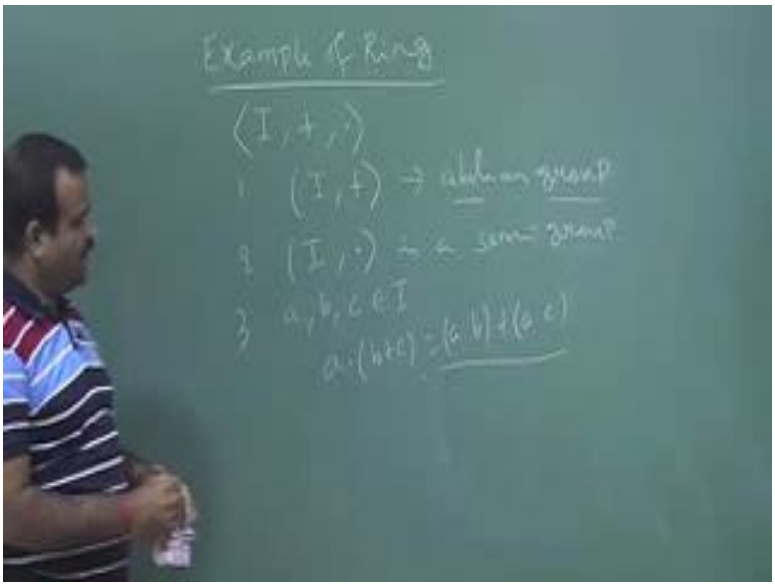
This is basically telling us a dot dot of this. So, this is the associativity if this satisfied then we call this is a semi group and then along with some property which is related to. So far there is no combination of these 2 operators. So, for there we are dealing with independently these 2 operators, now this property is telling the distributive property which is involves there together both, this is the distributive law or distributive property it is telling us. So, a dot I mean a cross b plus c equal to a cross b plus a cross c and this is true for all a, b, c belongs to Rg.

We have to understand this. So, b is an element in R, c is an element in R. So, if you operate b plus c and class is the closer close under R is closer under plus. So, this will be an element in R. So, since it is an element in R and we know this operator is closer, so we operate a with that another element in R. So, this will be also an element in R. So, this element must be same as if we element this, so this is a in R, b in R. So, if we operate this, this will be in R because closer property is satisfied under this multiplicative

sense and then this is a in R, c in R. So, this a cross a, a multiplies c is also R this is not real number multiplication this is that some operators, but for simplicity we are taking the real number sense like plus dot.

Then these two are, this is belongs to R this is belongs to R then we know plus is a when closer. So, we can add this to I we can take under this operation this will give us the element in R, but that element must same as this element and this must true for all a b c all the a b c then if this all this are satisfied then R is called a ring R along with plus Rg is called a this algebraic this algebraic structure this algebraic we called a ring. So, we can take some example of ring.

(Refer Slide Time: 16:13)



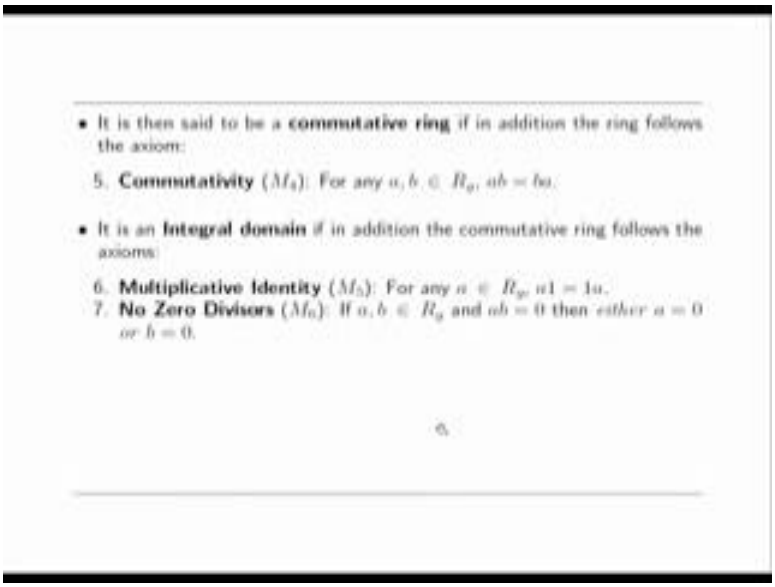
We can take some example of rings. So, like if you take this set or if you take this set I, set of integer and plus real number plus real number dot is this a ring. So, we have to check I plus this is an Abelian group, this we can easily verify this is an Abelian group. So, and second one we have to check this along with this dot is a semi group or not. So, for semi group we need to have that closer property and associative property. So, this is a semi group because if we take any 2 integers if you multiply this 2 it will give us a integer closer property is satisfy an associativity is also satisfied by the associativity law of the dot the real number multiplication is a semi group.

Now you have to check the distributive property, distributed property is telling if you take any three integer a b c then a dot b plus c is equal to a dot b plus a dot c this is also

true, this is true from the law of this 2 operator - plus and dot of real number. So, this is an example of a ring.

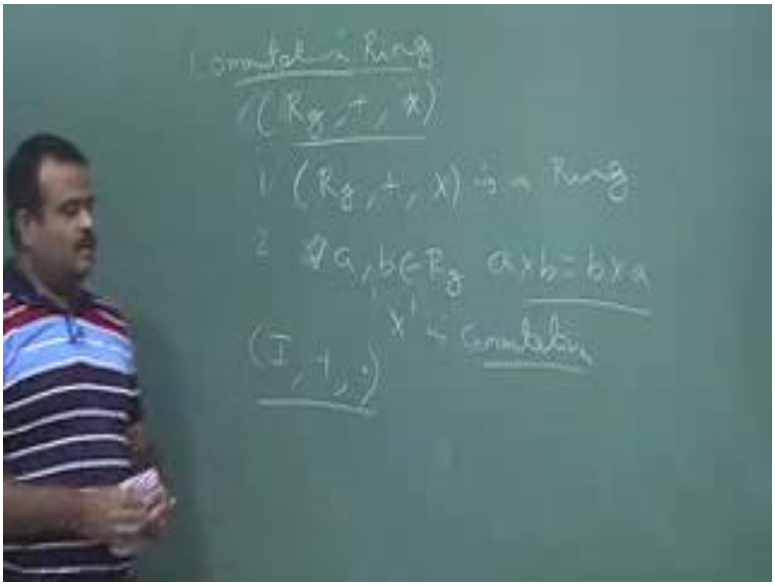
So, now, come to the slide. So, this is the distributive property.

(Refer Slide Time: 18:17)



Now we call - a ring is a commutative ring if on top of this all these properties if we satisfy the commutative property under the dot under the multiplicative sense because we know already it is Abelian group under plus. So, if it is commutative ring means it must be commutative under this dot.

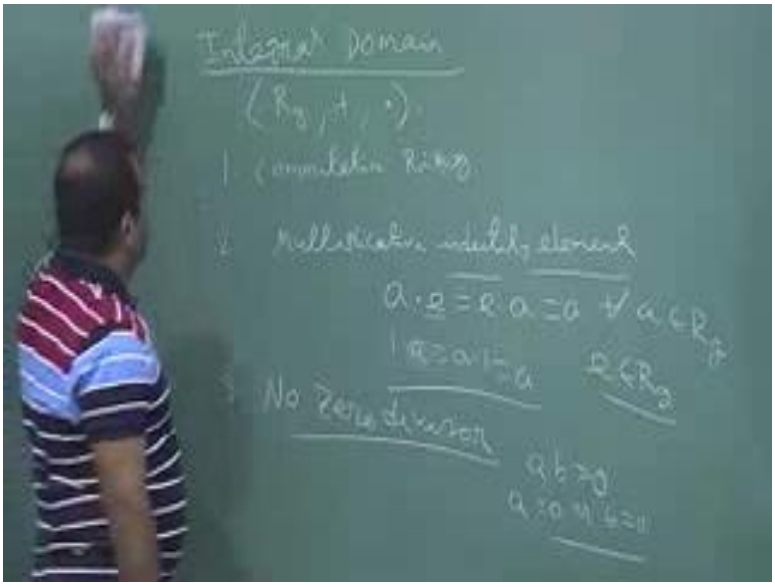
(Refer Slide Time: 18:49)



Commutative ring or the Abelian ring you can say. So, first of all this Rg and you can use this and this, this will be commutative ring first of all it has to be a ring, it has to be a ring and then if this we know ring means it is already commutative with this plus operation. So, now, the commutative means it is it must be again commutative under this multiplicative sense so; that means, for all a b belongs to that group a cross b a dot b is equal to b dot a so; that means, this is an Abelian this is commutative; commutative operation. So, if this is satisfied. So, this is also a commutative ring, this set of all integer plus dot this is a commutative ring because this operation is the real number multiplication is commutative.

Now after commutative ring we will define what is called integral domain, this is also another algebraic structure which is basically having 2 property, 2 operator integral domain.

(Refer Slide Time: 20:33)



Integral domain, so we say a ring I mean we say a group along with these 2 operation is an integral domain, first of all it has to be a commutative ring and the multiplicative identity should invite should exist. So, multiplicative identity; multiplicative identity means this, we already know this is a group. So, it has a inverse, it has a identical even under this operation, but whether it has a inverse, it has a identity element under this dot.

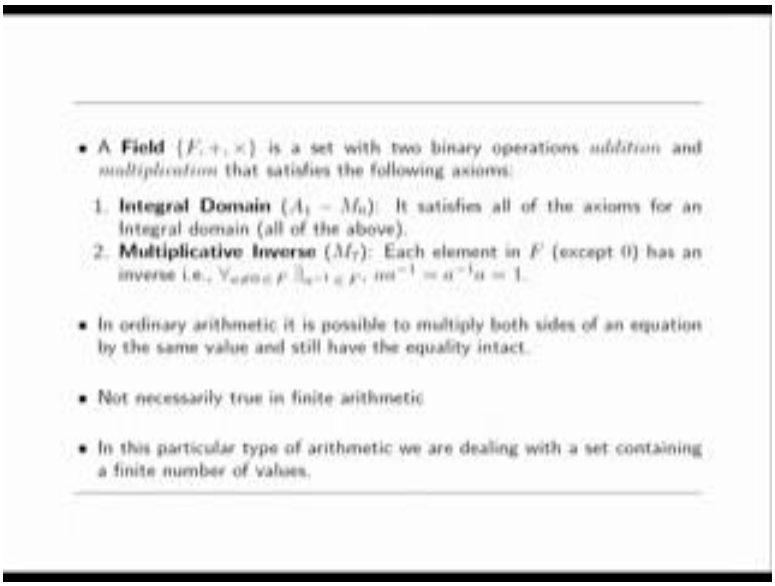
So, multiplicative identity that means, there exists a e is referred as 1 basically because this is in multiplicative sense there exist e such that a dot e must b e dot a must a and this

must be true for all a and this e usually refer as 1; I mean just the symbol e is a element, e is an element in Rg. So, e is unique. So, e is raising it is multiplicative sense, it is 1, it is symbolically it is just a symbolically because it is a general definition, it is a definition it is not that it is we are dealing with only real number. So, 1 into a is equal to a into 1 is equal to a. So, then it is called multiplicative identity. So, this is this property in 5.

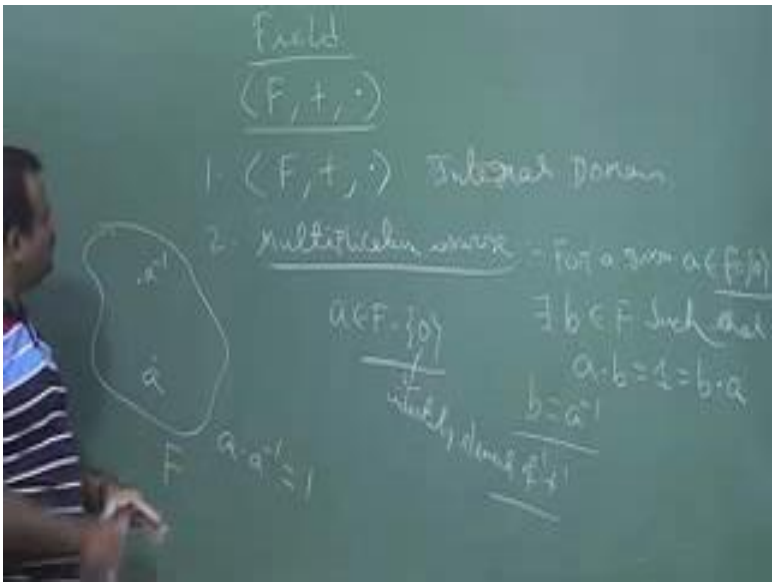
So, for every element if we operate this with the identity element and it should give us a, this should be equal to a and it should not have no zero divisor. This is another property so; that means, if you take any 2 element a b from this set and if a b is equal to 0 then either a is equal to 0 or b is equal to 0, so this is no zero divisor. So, if a dot b this is the multiplicative sense is 0 then either a is equal to 0 then b is equal to 0 then it is called knows no zero divisor property then this if all this property satisfied then it is called a integral domain. So, another is no 0; that means if we if we have a dot b is 0 then either a 0 or b is 0. So, then if this 4 property satisfied then it is called an integral domain.

Now, we will talk about field.

(Refer Slide Time: 24:13)



(Refer Slide Time: 24:21)



We talk about field. So, for field also, field is also algebraic structure here also we have a state and we have 2 operator plus and dot and so it also must satisfy some properties. So, first of all, it has to be a integral domain, it has to be a integral domain and this it should every element should has inverse under the multiplication we know every element has inverse under plus because it is an integral domain that means, under plus it is an Abelian group. So, since it is an Abelian group every, every element has inverse.

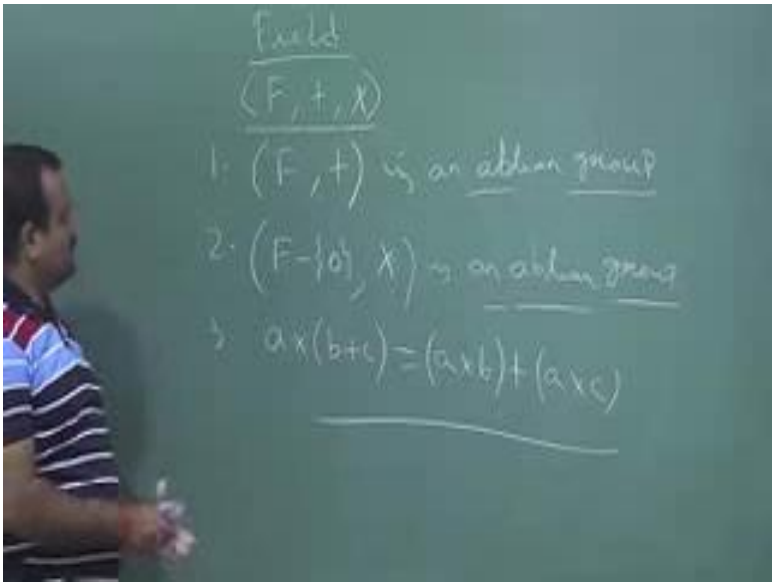
So, we want the inverse also under this dot, so that means so inverse multiplicative inverse, existence of multiplicative inverse. Every element should have a multiplicative inverse; that means, every element should have inverse under this dot operation, so that means, for a given element for a given a belongs to F, there exists a b which is in F such that such that a operate with b is equal to identity element of multiplicative sense is equal to b operate with a.

So, this is a basically in, b is usually symbolically here referred as a inverse. So, this is the multiplicative inverse others with the other. So, if this exists if for every element, for a given element a it has the inverse. So, basically this is or F, given a, a if we have a eliminate a which is b basically inverse will refer and if you multiply this, it should give us it should give us identity element of 1 and this is not for all element this is other than the identity element of plus so other than 0. So other than this identity, so a is basically a is coming from F minus 0. So, because this 0 is the identity element under plus I

identified identity; identity element of class, it has no inverse basically. So, other than this 0, it should have a inverse. So, this should be there. So, now, if this satisfied then it is called a field then this F along with this operation is called a field.

Basically what we have? We have this. So, this integral domain is a field. Basically for field, this must be an Abelian group, is an Abelian group and also F minus 0 is also an Abelian group I mean we can use this in any way this is in multiplicative sense is also an Abelian group then we called this is a field.

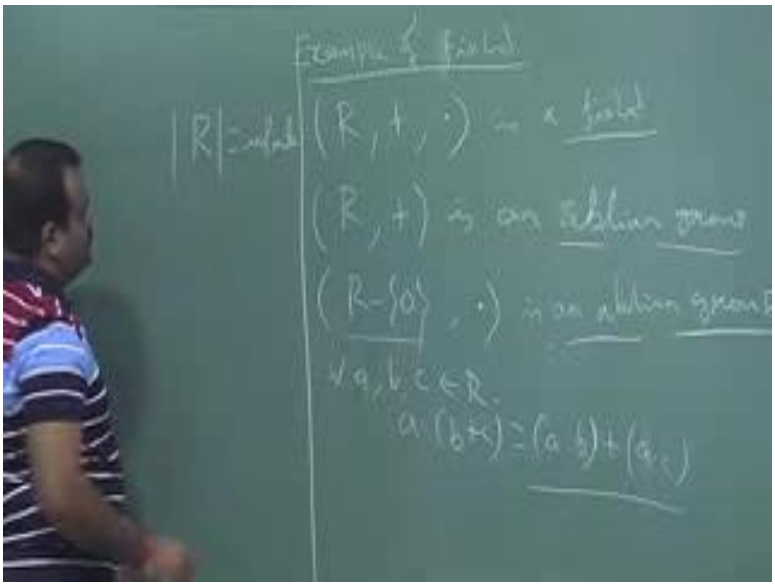
(Refer Slide Time: 28:07)



So, if this and an also the distributed property like a dot a cross b plus c is equal to a cross b plus a cross c because this is the property in the integral domain it was there. So, it is if these satisfy then it is called a field.

Now, let us take some example of field. So, field has good application in cryptography especially finite field, finite field means if the element number of element in G is finite the cardinality of this set F.

(Refer Slide Time: 29:39)



Example of field, so set of real numbers plus and dot multiplicative sense is a field why? Because we have seen this is an Abelian group and also if we just remove this 0, 0 is the identity element for plus because 0 has no inverse under multiplication because 1 by 0 is not defined in real number system, we can have extended real number system then we can define 1 by 0 as a symbol infinity, but anyway real number is not consisting 1 by 0 as a element. So this is basically anyway we do not need to bother about this because for field, the 0, this identity element of this plus is not having the inverse, I mean we do not care about that. So, this a, this is also an Abelian group.

Now, this is also Abelian group and also we have this distributed property, if you take any 3 element a b c from this real number set, we know b dot b plus c is equal to a dot b plus b dot c sorry a dot c, this is the property of the plus and dot in this. So, this is an example of a field, but this field is the infinite field because cardinality of this is infinity where infinite number of points in the real number. So, infinite, but if the cardinality of R is finite then it is called finite field. We will talk about finite field talking the number 3.

(Refer Slide Time: 32:01)

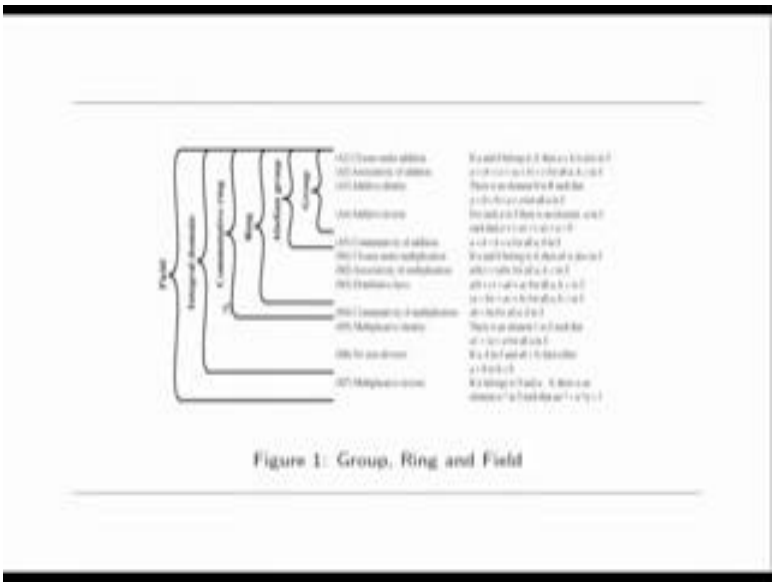


Figure 1: Group, Ring and Field

This is the hierarchy of the algebraic structure. So, if we have this closer property. So, we have basically 2 operator addition and the multiplication. So, this is the closure property under addition and this is the associativity property under multiplication this is the sorry associativity property under addition and this is the identity element of addition and this is the additive inverse. If this we have this 4 then it is a group and along with that if this plus is commutative then it is called Abelian group up to this and then for ring, we have another operator which is multiplicative sense which is dot.

Now if it is for ring it must be a closer and the associatively and the distributed law, then up to this then it is called a ring and then if it is commutative ring means we have this dot is also commutative operator a dot b is equal to b dot a and then for integral domain, we have the inverse multiplicative inverse. So, a dot 1 is sorry, multiplicative identity. So, a dot 1 is 1 dot a is equal to a 1 is the multiplicative identity and no zero divisor if a b is 0, 0 is the identity element of plus then either a is 0, b is 0. And then if we along with this if we have this multiplicative inverse for each element in a other than 0 then it is called a field. So, this is the hierarchy of the field.

Thank you.