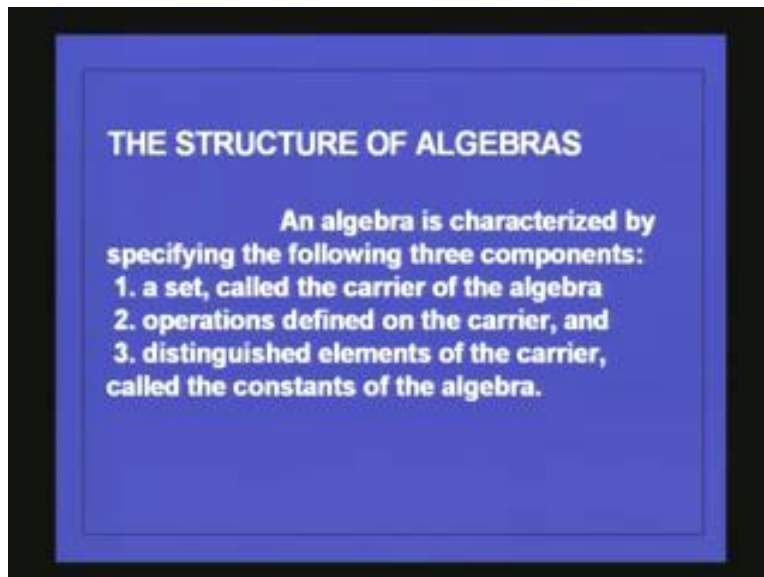


**Discrete Mathematical Structures**  
**Dr. Kamala Krithivasan**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**  
**Lecture # 35**  
**Algebras**

Today we shall start on a new topic called algebras. In this we shall study about semigroups, groups, rings, monoids, integral domains and fields and let us see what they are. But before that what is the need to study such algebras.

In any mathematical model we should have three things; one is a real world situation and a mathematical model and then connecting the mathematical model with the real world situation that is the connection between them, how the mathematical model which we are giving represents the real world situation. Not only that when we try to define a mathematical model it should have some sort of a structure and it should obey certain laws or operations on it and that should correspond with the operations and real life situation. So in such a thing people have considered algebras, what are algebras?

(Refer Slide Time: 02.17)



Algebraic structures or algebraic species, varieties of algebras, as you know some of them are semigroups, monoids, Boolean algebras, groups, rings, integral domains, fields and so on. Each one of them has a different structure and there are some operations on it, it has got some properties and having some properties implies some other properties and things like that. So let us see one by one. First of all we will see what algebra is in general and then we shall see the different varieties one by one.

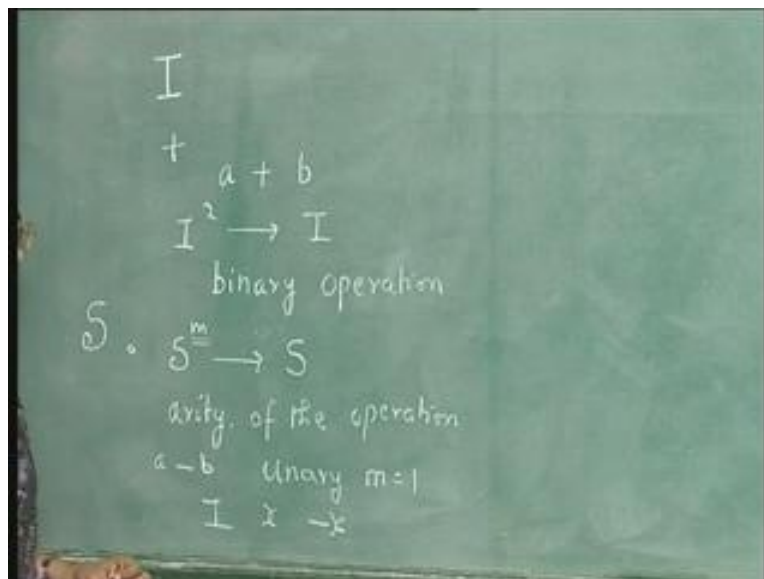
When you consider the structure of algebras, algebra is characterized by specifying three components; one is a set called the carrier of the algebra. The first component or the first one you have to specify is the carrier of the algebra. Something like, it can be the set of integers, it can be the set of real numbers, it can be set of complex numbers and so on. Hence that is the underlined set and that is called the carrier of the algebra. Then you have some operations defined on the carrier.

For example, if you take the set of integers it could be a carrier of the algebra then you can define an operation addition on this. That is, if you take two integers  $a$  and  $b$  you can perform this operation. This is actually an operation from  $I$  squared to  $I$  and it is called a binary operation. This operation of addition is called a binary operation.

In general, if you take the underlines set to be  $S$  then an operation represents a mapping from  $S^m$  into  $S$ . So, if you have  $m$  argument you get a value from  $S$  and this  $m$  is called the arity of the operation. You can specify an operation like this. So multiplication is a binary operation on integers. Addition is a binary operation, minus  $a$  minus  $b$  is a binary operation. You can also have unary operations. In binary operations the arity is 2 and in unary operations the arity is 1 that is  $m$  is equal to 1.

For example, if you take the set of integers if you have  $x$ , minus  $x$  the negative of  $x$  is a unary operation, this minus is a unary minus it is a unary operation. Or you can also have unary operations like you know.

(Refer Slide Time: 05.19)

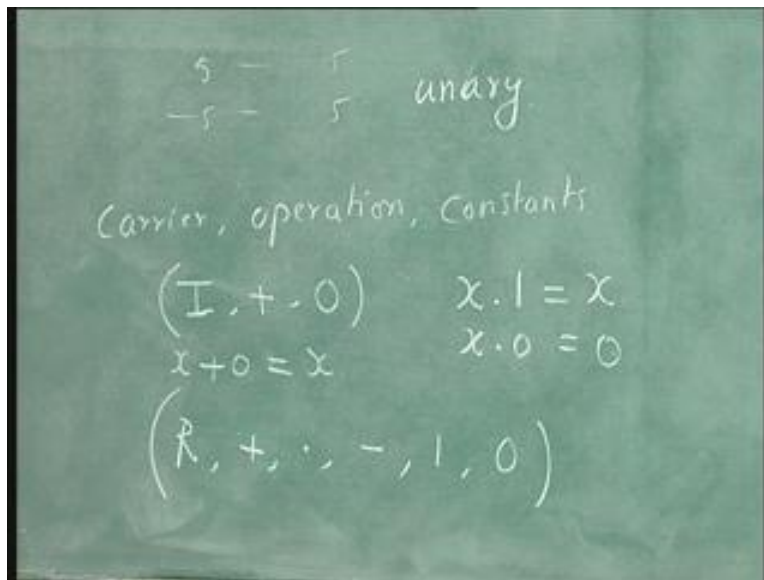


If you take the set of integers for  $x$  you define mod of  $x$  the absolute value of  $x$  this is the unary operation. So, if it is a positive number like 5 it will be 5, if it is a negative number like -5 it is again 5 so this is again a unary operation binding the absolute one. You can think of other operations of higher arity also. So in algebra first you have to specify the carrier then the operations then there are certain things called the constants of algebra.

For example, if you take  $I$  is a set of integers and the binary operation plus and take 0 as the constant you know that any  $x$  if you add 0 you only get  $x$ , this 0 has a particular structure or particular property when you add it to any number you get the same number that is called an identity element of the algebra. Another example will be, if you take the set of real numbers then you can take binary operation plus binary operation multiplication unary operation minus then 1 and 0 as the constant.

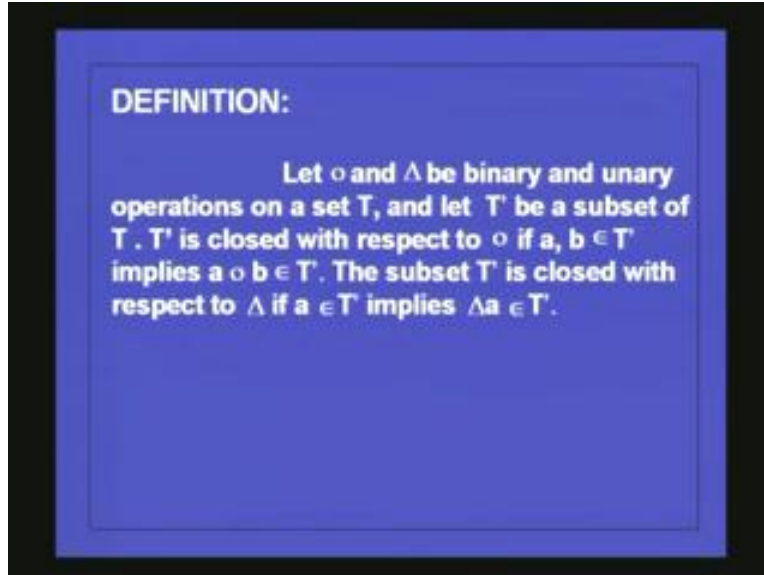
Therefore, if you take any number and any real number add 0 you will get the same number so 0 is the identity element for plus. Whereas if you take multiplication any number  $x$  if you multiply by 1 you get  $x$ .  $x$  is a real number you multiply by 1 you get  $x$ . So that is an identity for the operation. But then if you take  $x$  multiplied by 0 you get 0 that is called the 0 of the algebra. This is a 0 element for multiplication. As 0 is an identity element, element for the plus operation or sum operation and for multiplication, 1 is also an identity element and 0 is the 0 element. So some elements like that have special properties called as constants of the algebra.

(Refer Slide Time: 07.47)



You have some distinguished elements of the carrier they are called the constants of the algebra. So when you want to specify an algebra first you must specify the carrier or the underlined sets then the operations with their corresponding arity and then the distinguished elements which are constants of the algebra.

(Refer Slide Time: 08.13)



Now, suppose you have algebra like this one algebra  $A$  and one operation dot and some constant  $k$  another algebra  $A$  dash and dot. dash  $k$  dash like this then these two, you need not have a single operation **you may have several operations.**

**So in order to be very clear let me write it like this;**  $A$ , an algebra then some operations then some constants. Another algebra is  $A$  dash some operations on that, this algebra  $I$  can call as  $A$  and  $A$  dash. Now the algebra  $A$  and  $A$  dash have the same signature, when do you say this same signature?

You call it the same signature when you have one underlined set and seven operations here and also have seven operations here. The number of operations should be the same and they should also have the corresponding arity.

For example, the first operation here is this, the first operation here is this, if this is the binary operation this should also be a binary operation. Same number of operations you must have same number operation here also you must have and the arity of the operations should also match. Then if you have some constants the same number of constants you must have. The number of constants should be the same.

For example, if you take the integers plus dot unary minus  $1\ 0$  this is an algebra where the underlying structure is carrier is  $I$  two binary operations, one unary operation, two constants. If you take  $R$  plus dot minus  $1\ 0$  this again has the same components same six components it has got, this is the carrier, two operations both are binary corresponding to this and one unary and two constants and so on. You can also consider this, the power set of a set  $S$  union operation, intersection operation, complementation operation, then  $s$  and  $\phi$  the whole set and empty set where again this has got six components, this is the carrier of the algebra, these two are binary operations, this is the unary operation, two constants are there so all these have the same signature and are said to be of the same species.

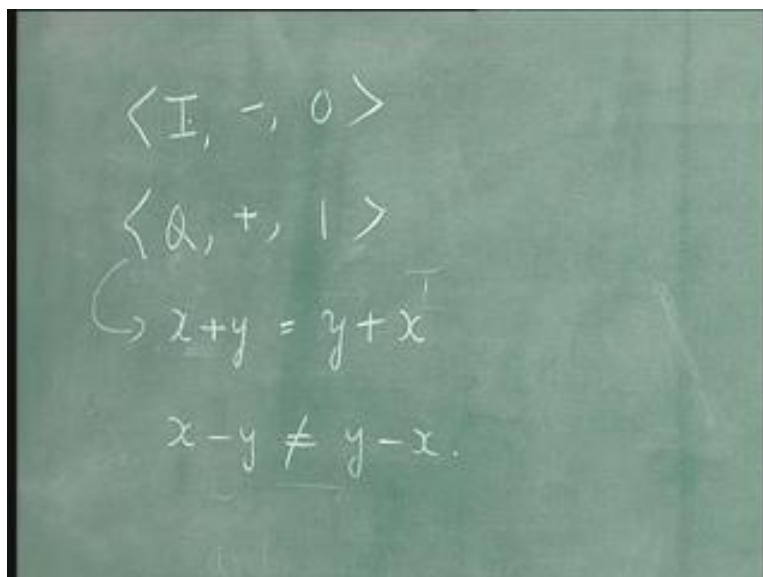
(Refer Slide Time: 11.35)



Now, look at this example;

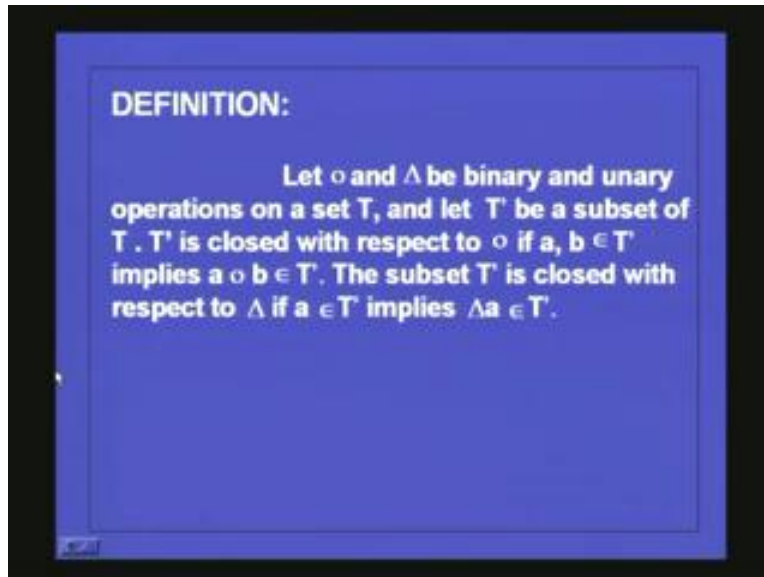
$\mathbb{I} - 0$  and set of rational numbers plus 1 something like that. These are of the same signature because you have one underlined, set one binary operation, one constant but they may not have the same property. For example, if you have here two rational numbers  $x$  plus  $y$  will be is equal to  $y$  plus  $x$  the commutative law will hold for this. Whereas if you take the set of integers and say  $x$  minus  $y$  that will not be equal to  $y$  minus  $x$ . So, that property may not hold here when we take the operation to be minus. So even though these two algebras are of the same species or they have the same signature there is a difference in that.

(Refer Slide Time: 12.22)



We want to consider algebras where they have some specific structure. That is, they will all follow some set of rules which are called axioms. For example, if you take semigroups they will follow a set of axioms. Similarly, if you take groups they will follow a set of axioms and so on. So we are interested in such algebraic structures and let us see the definitions. But before that we have to see what is meant by a closure.

(Refer Slide Time: 13.10)



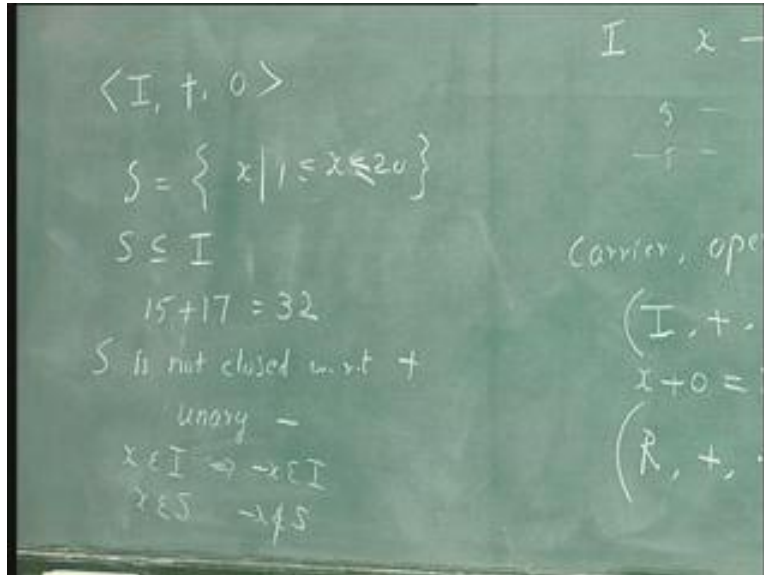
Let us consider a binary operation and unary operation. Let dot and this del be the binary and unary operation on a set. I am using the symbols small triangle to denote the unary operation and calling it as del. Usually inverted triangle is called as del but here I am using the triangle symbol to denote the unary operation and calling it as del. You are having a set  $T$  and you are having a binary operation dot and a del which is a unary operation. Now take a subset of  $T$  which is  $T$  dash. Then  $T$  dash be a subset of  $T$ .  $T$  dash is closed with respect to dot and if whenever  $a, b$  belong to  $T$  dash the operation when you perform on  $a$  and  $b$  then  $a \cdot b$  also belongs to  $T$  dash. Then you say that  $T$  dash is closed with respect to dot. Similarly for the unary operation the subset  $T$  dash is closed with respect to del if  $a$  belongs to  $T$  dash implies del  $a$  belongs to  $T$  dash.

For example, let us consider the set of integers and the operation plus. Let us consider this algebra and consider a subset for example take a subset  $S$  where the integers are that is  $x$  and  $x$  is between 1 and 20. So set of integers from 1 to 20 is a subset so  $S$  is a subset of  $I$ , is it closed with respect to plus?

You take 15 and 17 that gives you 32 which does not belong to  $S$ . So  $S$  is not closed with respect to plus whereas the original thing set of integers is closed with respect to plus. Similarly, if you take the unary instead of binary operation  $I$  if you take unary minus  $I$  if you take  $x$  belongs to  $I$  it also implies minus  $x$  also will belong to  $I$  this is true whereas if

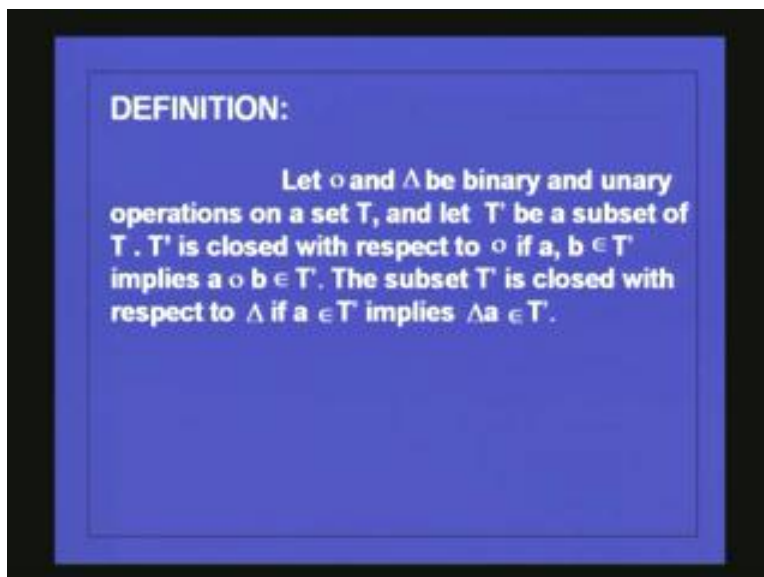
$x$  belongs to  $S$  then minus  $x$  will be minus if you take 15 it will be minus 15 and so on. So minus  $x$  does not belong to  $S$ . so it is not closed under this unary minus operation.

(Refer Slide Time: 15.49)



So you have to consider the case where when you consider a subset of a set whether that subset is closed with respect to that operation. Whereas if you take the set of integers and consider the operation max, max of  $a, b$  is the maximum element of  $a, b$  which belongs to  $I$ .

(Refer Slide Time: 16.05)



Whereas if you consider the set  $S$  and the same operation  $\max$  maximum of  $a, b$  will also be one of the element from 1 to 20 so  $S$  will be closed with respect to  $\max$ . Next, we consider what is meant by subalgebra. Let  $A$  is equal to  $S \cdot \Delta k$  and  $A'$  is equal to  $S \cdot \Delta \Delta k$  be algebras. It need not have a single binary operation or a single unary operation. You may have several operations but we generally take it like this for our convenience. But these two algebras are having the same signature so the same number of binary operations they will have and the same number of unary operations they will have,  $A$  and  $A'$  are of same signature.

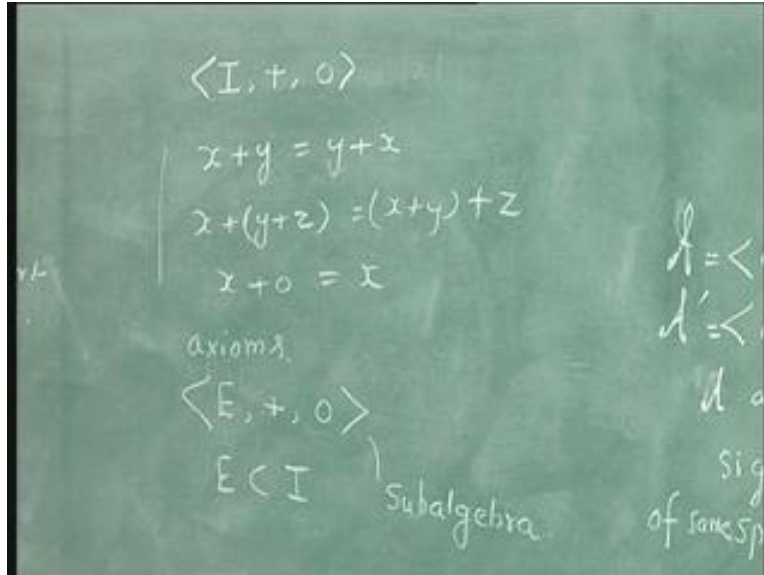
Now, this is a subalgebra if the carrier of this is a subset of the carrier of this.  $S'$  is contained in  $S$  and when you restrict the operation  $\Delta$  to  $\Delta'$  that is within that element  $S' \cdot a \cdot b$  is the same as  $a \cdot b$ . Then you also have  $\Delta' a = \Delta a$  for all  $a$  belonging to  $S'$ . That is, when you perform this operation  $\Delta'$  with respect to the elements belong to  $S'$  it is the same as performing the operation with respect to the same element in  $S$ . And the set of constant should be the same both should have the same constants.

If this definition is true then you find that  $A'$  is a subalgebra of  $A$ .  $A'$  is a subalgebra of  $A$  then  $A'$  has the same signature as  $A$  they are of the same species and they obey the same axioms. In general you have a set of axioms obeyed by this. For example, we will take the same example again, take the set of integers plus and 0 this is an algebra and it will obey the commutative law  $x + y$  is equal to  $y + x$ , it will obey the associative law  $x + y + z$  is equal to  $x + y + z$ . Then  $x + 0$  is equal to  $x$ . These are some of the rules which is obeyed by this and these are called the axioms.

Now, consider the set of even integers and plus 0 both have the same signature. There is a carrier one binary operation one constant the constants are the same. And when you take even integers this also obeys this,  $x + y$  is equal to  $y + z$  that rule will be obeyed. And  $x + y + z$  is equal to  $x + y + z$  the associative law also holds for even integers. And when you add a 0 to an even integer you get again the same integer so this rule is also obeyed. But  $E$  is a subset of  $I$ . The set of even integers is a subset of the whole set of integers so this is a subalgebra.

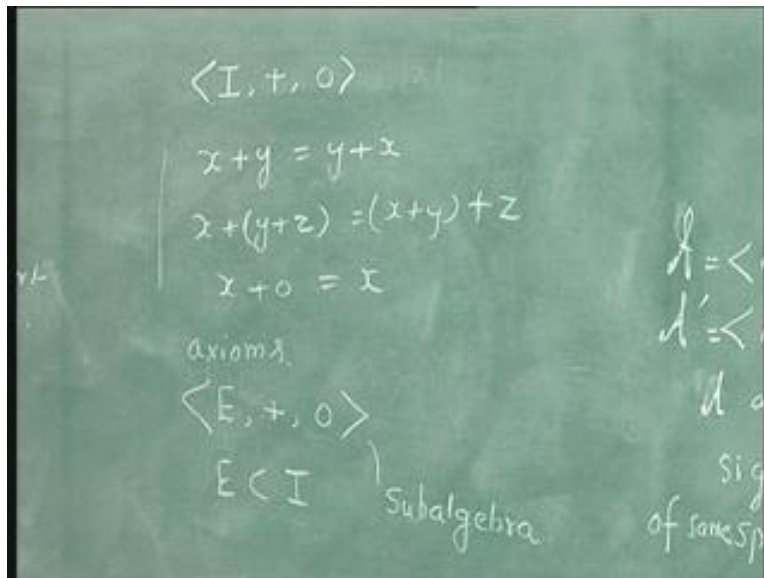


(Refer Slide Time: 20.14)



So continuing with this definition you find that the carrier of  $\mathcal{A}'$  is a subset of the carrier of  $\mathcal{A}$  which is closed under all the operations of  $\mathcal{A}$  and contains all the constants of  $\mathcal{A}$ .

(Refer Slide Time: 20.25)

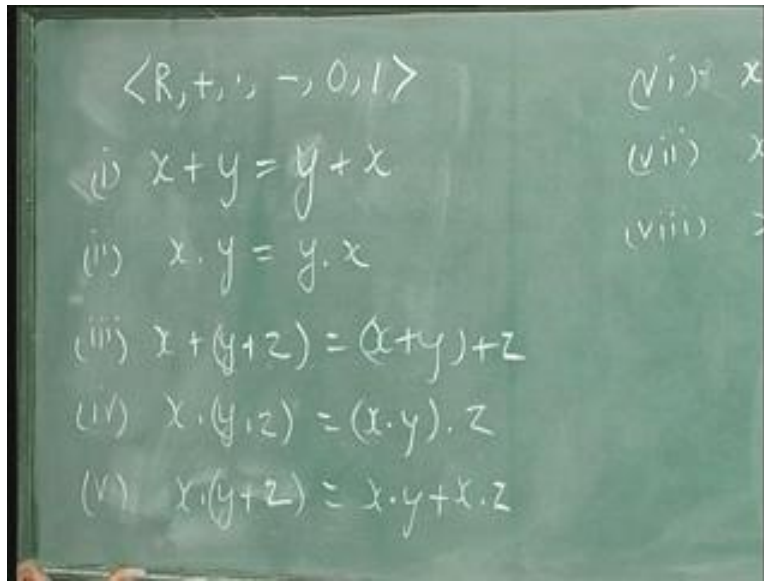


You must see that it should be closed. That is, when you add two integers you get an even integer, when you add two integers also their set belongs to this. So the closure is an essential property. All the operations of  $\mathcal{A}$  contain all the constants of  $\mathcal{A}$ . The largest possible subalgebra of  $\mathcal{A}$  is  $\mathcal{A}$  itself this subalgebra will always exist. If the set of

constants of A is closed under the operations of A then this is the carrier of the smallest subalgebra of A.

Consider this algebra  $\langle \mathbb{R}, +, \cdot, -, 0, 1 \rangle$   $\mathbb{R}$  is the set of real numbers, plus is the binary operation, addition, multiplication, binary operation, unary minus and then 0 and 1 are identity elements for plus and multiplication respectively. And this obeys the following axioms, there are eight axioms,  $x + y$  is equal to  $y + x$  commutative law holds for addition.  $(x \cdot y)$  is equal to  $y \cdot x$  commutative law holds for multiplication also. Then  $x + y + z$  is equal to  $x + (y + z)$  that is the associative law holds for addition.  $(x \cdot y) \cdot z$  is equal to  $(x \cdot (y \cdot z))$  that is associative law holds for multiplication also. Then multiplication is distributive with respect to addition that is given by this distributive law that is  $(x \cdot y) + x \cdot z$  is equal to  $x \cdot (y + z)$ .

(Refer Slide Time: 22.15)



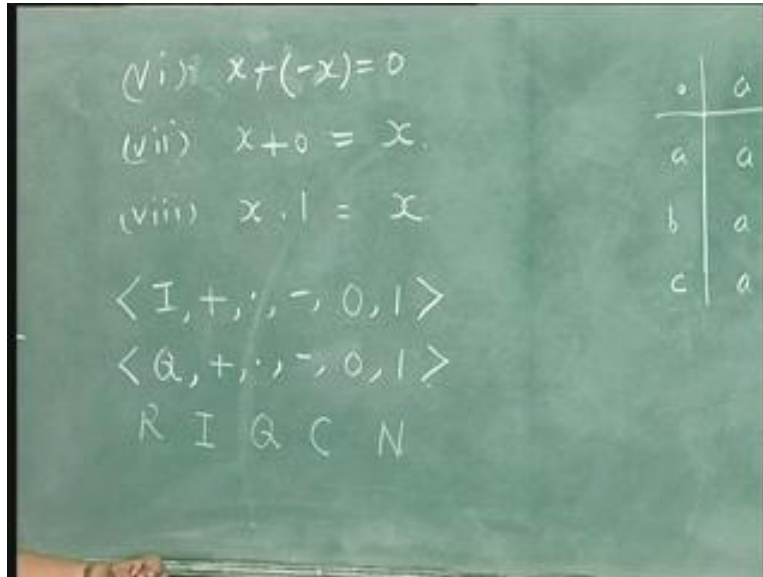
Then with respect to unary minus you have  $x + \text{minus } x$  is equal to 0 the 0 element. The identity element of addition and the 0 element of multiplication,  $x + 0$  is equal to  $x$  that is 0 is the identity for addition and  $x \cdot 1$  is equal to  $x$ , 1 is the identity element for multiplication.

We shall learn more about identity elements in a formal manner in a moment. Now, this algebra obeys these eight axioms. And if you consider the set of integers with the same operation and the same constant this has the same structure as this it is the same signature. And one by one you can verify and this will also obey all the eight axioms. So it is of the same variety or a same type because it obeys the same axioms.

If you consider the set of rational numbers then the same operations addition multiplication unary minus and the same two constant you will realize that this also obeys all eight axioms. Usually the set of real numbers is denoted by  $\mathbb{R}$ , set of integers is denoted by  $\mathbb{I}$ , set of rational numbers is denoted by  $\mathbb{Q}$ , the set of complex numbers is

denoted by  $C$  and the set of non negative integers  $0, 1, 2$  they are denoted by  $N$ . These are the symbols which are usually used in any book. But when you refer to a particular book you must see what notation that particular book is following.

(Refer Slide Time: 24.04)



Now look at this algebra; the power set of a set  $S$  union, intersection, complementation, the empty set and the whole set. How many elements are there? There is a carrier of an algebra that is okay. Then there are two binary operations; union and intersection are binary operations. Here also we are having two binary operations. There is one unary operation the complement of the set. You know what is meant by the complement of a set. Then this is an empty set which is like a constant the whole set  $S$  is another constant.

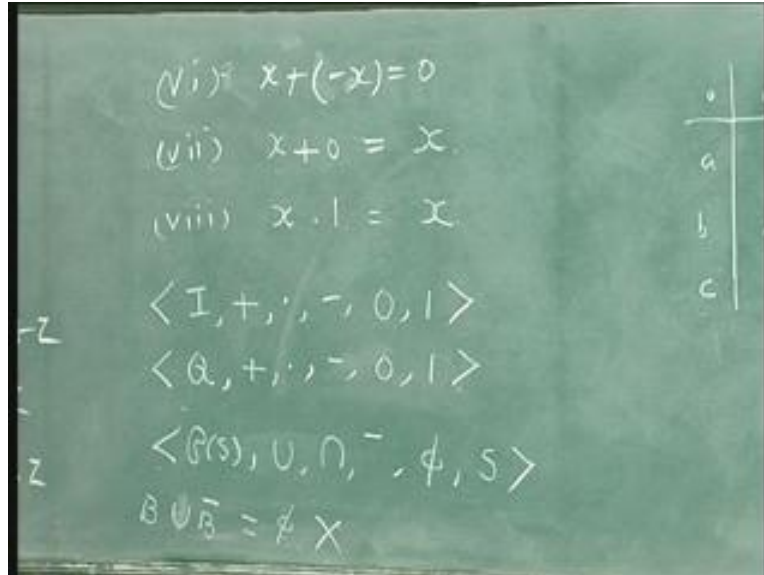
Now does it obey it has got the same signature?

It has got the same carrier two binary operations, one unary operation and so on. But it is not the same as these two because you verify the laws one by one whether they are obeyed, you will find that one law is not obeyed by this algebra.

With respect to union, commutativity, associativity you can prove. With respect to intersection also commutativity and associativity you can prove, distributive law also you can prove, but what about this?

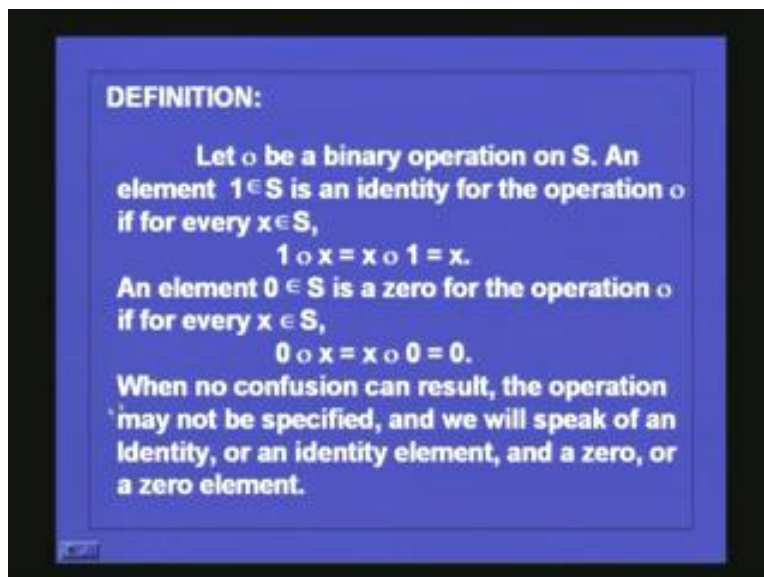
If you put  $x$  plus minus  $x$  that is some set  $B$  plus the complement of  $B$   $B$  bar that is here you are using union  $B$  bar that is equal to  $0$  corresponds to  $\phi$ , so you will get like this  $B$  union  $B$  bar is equal to the empty set which is not correct.

(Refer Slide Time: 26.16)



So the sixth law is not obeyed by this algebra so it is different from these two. When we want to consider algebraic structure they have to obey the same set of axioms. So I have been using the terms 0 element 1 element but let us see formally what are these 0 elements and 1 elements.

(Refer Slide Time: 26.34)

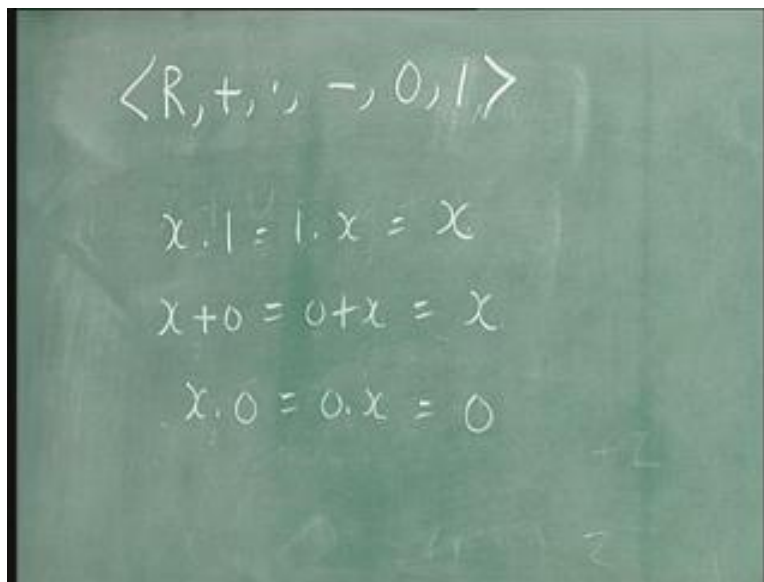


Consider a binary operation on a set  $S$ . Let dot be a binary operation on a set  $S$ . An element  $1$  belonging to  $S$  is an identity for the operation dot If for every  $x$  belonging to  $x$   $1 \cdot x$  is equal to  $x \cdot 1$  is equal to  $x$  in this case you call  $1$  as the identity element. An element  $0$  belonging to  $S$  is a  $0$  for the operation dot if for every  $x$  belonging to  $S$   $0 \cdot x$

is equal to  $x \cdot 0$  is equal to 0. So this dot sometimes you omit because there is no confusion. So you talk of an identity, identity element, 0 or a 0 element.

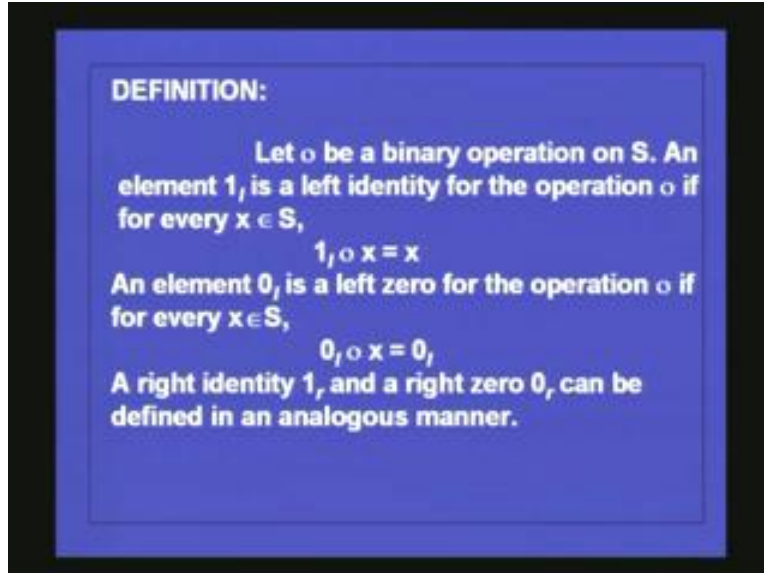
For example, take this multiplication the same real numbers and so on. You see that  $x$  into 1 is equal to 1 into  $x$  is equal to  $x$ . So 1 is an identity element with respect to multiplication. And  $x$  plus 0 is equal to 0 plus  $x$  is equal to  $x$ . So 0 is an identity element for plus operation. Whereas  $x$  into 0 is equal to 0 into  $x$  is equal to 0. So 0 is a 0 element for the operation multiplication. So 1 is an identity element for multiplication, 0 is a 0 element for multiplication but 0 is an identity for plus. This is how we define 0 and identity elements.

(Refer Slide Time: 28.15)


$$\langle \mathbb{R}, +, \cdot, -, 0, 1 \rangle$$
$$x \cdot 1 = 1 \cdot x = x$$
$$x + 0 = 0 + x = x$$
$$x \cdot 0 = 0 \cdot x = 0$$

You can also talk about left identity and right identity. Let dot be a binary operation on  $S$ , an element  $1l$  is a left identity for the operation dot if for every  $x$  belonging to  $S$   $1l \cdot x$  is equal to  $x$ .

(Refer Slide Time: 28.20)



An element  $0_l$  is a left 0 for the operation dot if for every  $x$  belonging to  $S$   $0_l \cdot x$  is equal to  $0_l$ . Similarly, you can define right identity and right 0. When do you say something is a right identity? You say when you have  $x \cdot 1_r$  is equal to  $x$ . When do you say something is a right 0? It is when  $x \cdot 0_r$  is equal to  $0_r$ . So in that case you call them as right 0s and right identities. When you have a table like this look at this example; you have three elements, the set  $S$  consists of three elements  $a, b, c$  and there is a binary operation dot which is given by this table.

What do you understand by this table?

$a \cdot a$  is equal to  $a$ ,  $a \cdot b$  second one you have to take from this  $a \cdot b$  is  $b$  and so on. Again  $a \cdot c$  is  $b$ ,  $b \cdot a$  is  $a$  you have to read this table in this manner.

(Refer Slide Time: 29.59)

Handwritten notes on a chalkboard:

- $x) = 0$
- $= x$
- $= x$
- $(0, 1 >$
- $(0, 1 >$
- $(\phi, S >$

$\cdot$	a	b	c
a	a	b	b
b	a	b	c
c	a	b	a

$S = \{a, b, c\}$   
 $a \cdot a = a$   
 $a \cdot b = b$

Now, this algebra where the operation dot is specified in this manner does it have an identity element does it have a 0 element. Look at this table you see that a dot a is equal to a, b dot a is also a, c dot a is also a. What does that mean?

That means a is a right 0 element for this. In the same manner you see that a dot b is b, we can write this here a dot b is b, b dot b is also b, c dot b is also b so what can you say about b?

b is also a right 0.

Does there exist a left 0?

Here there is no left 0 because if you have a left 0 you must have one row consisting of the same element. Here this column consists of the same element so it becomes a right 0. This column also consists of the same element so it becomes a right 0. If one row consists of the same element it will become a left 0. But here you do not have like that there is no left 0 here.

Now what can you say about b?

b dot a is equal to a, b dot b is equal to b, b dot c is equal to c. So when you multiply something by b on the left you get the same element a b c so b is a left identity in this table. Like that we can see left 0s like 0s in particular algebras. But if algebra has a left 0 and a right 0 then they are the same, I mean they will be equal and if you have a left identity and a right identity it will be a two sided identity.

(Refer Slide Time: 32.41)

**THEOREM:**  
Let  $\circ$  be a binary operation on  $S$  with left identity  $1_l$  and right identity  $1_r$ . Then  $1_l = 1_r$  and this element is a two – sided identity.

**PROOF:**  
Since  $1_l$  and  $1_r$  are left and right identities,  
$$1_r = 1_l \circ 1_r = 1_l$$

Let dot be a binary operation on  $S$  with left identity  $1_l$  and right identity  $1_r$  then they are equal  $1_l$  and  $1_r$  are equal. And this is called a two sided identity. Since  $1_l$  and  $1_r$  are left and right identities what do you have?

$1_l$  is the left identity so whenever you multiply something by  $x$  you must get  $x$ . Now instead of  $x$  I am taking  $1_r$ . So it will be  $1_r$  and  $1_r$  is a right um identity so when you multiply something by  $1_r$  you must get  $x$ . Now suppose I take  $x$  to be  $1_l$  so I get  $1_l$ . So from these you get left identity is equal to right identity.

(Refer Slide Time: 33.47)

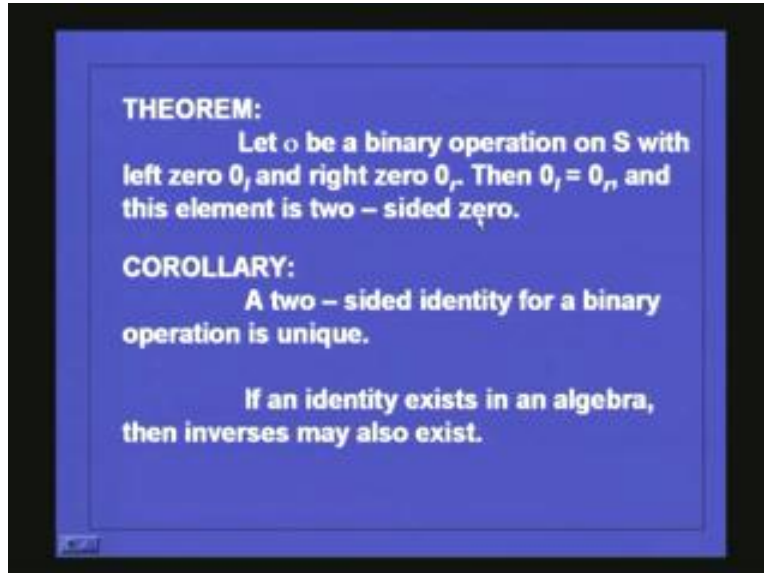
Handwritten mathematical proof on a chalkboard showing the equality of left and right identities:

$$1_l \cdot 1_r = 1_r$$
$$1_l \cdot 1_r = 1_l$$
$$1_l = 1_r$$



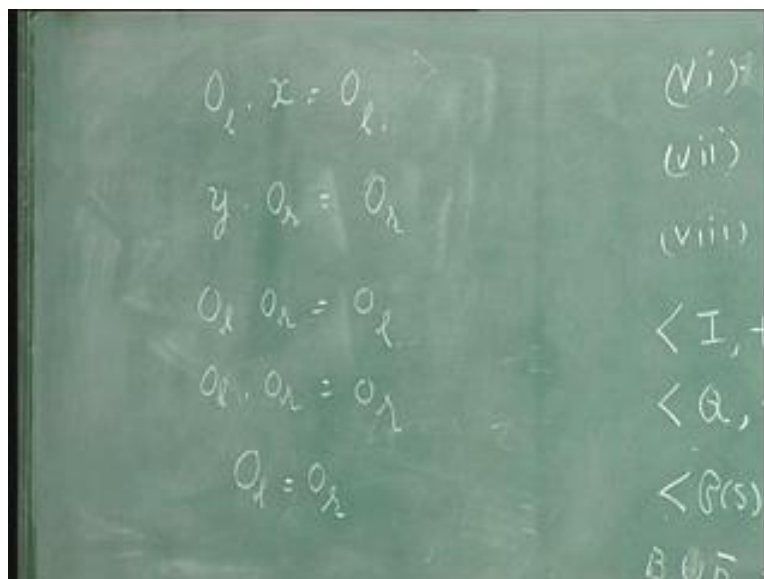
Similarly for 0 let dot be a binary operation on S with a left 0  $0_l$  and the right 0  $0_r$  then  $0_l$  is equal to  $0_r$  and this element is called a two sided 0. How do you see this?

(Refer Slide Time: 33.50)



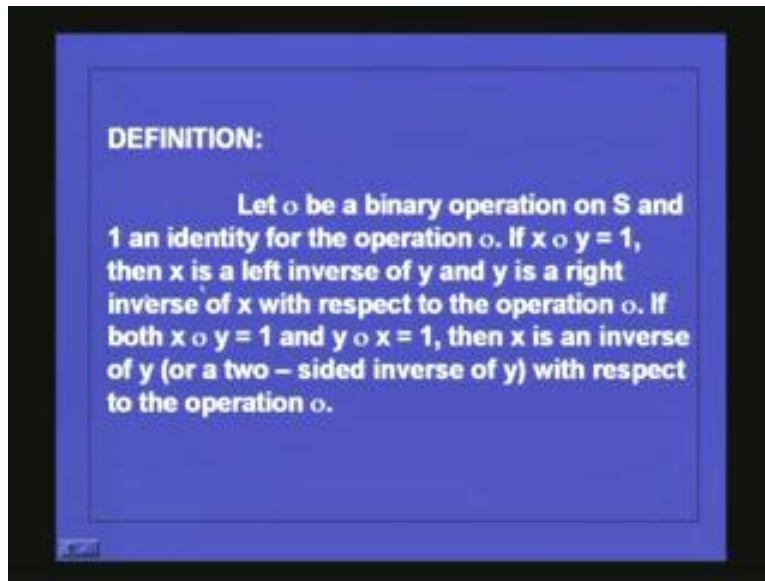
Again the same idea, when you have a left 0  $0_l$  if you take any element that will be  $0_l$ . Then if you have a right  $0_r$  that will be  $0_r$ . Now in this you put x is equal to  $0_r$  you get  $0_l$  into  $0_r$  is equal to  $0_l$ . In this you put y is equal to  $0_l$  you get  $0_l$  into  $0_r$  is equal to  $0_r$  and from these you get  $0_l$  is equal to  $0_r$ . So if you have both the left 0  $0_l$  and the right 0  $0_r$  they will be the same.

(Refer Slide Time: 34.41)



In this particular example you see that  $a$  and  $b$  are right 0s but there is no left 0 in that example. And you can very easily verify that a two sided identity for a binary operation is unique. Again in the same manner you can see, it is unique you cannot have two of them. If an identity exists in algebra then you may also have inverses of elements in that.

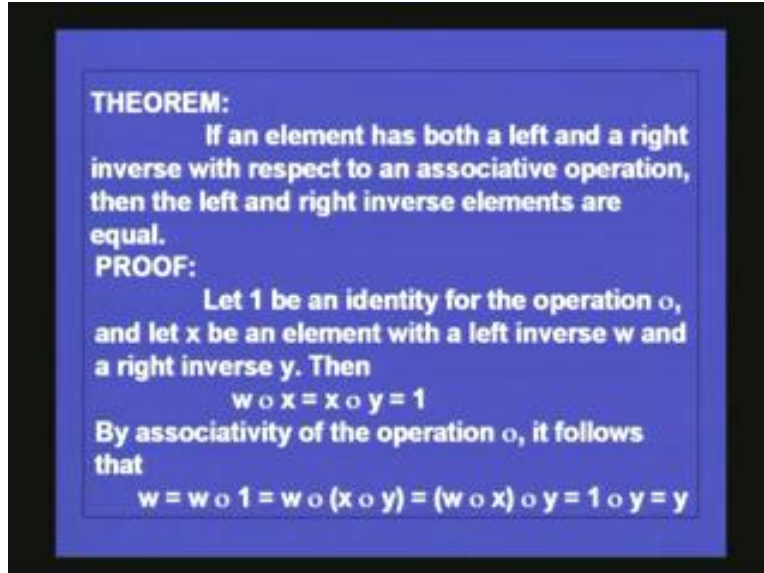
(Refer Slide Time: 35.28)



Consider a binary operation on a set  $S$  and consider an identity element for the operation. So if  $(x \text{ dot } y)$  is equal to  $1$  the identity element then  $x$  is called the left inverse of  $y$  and  $y$  is called the right inverse of  $x$  with respect to the operation. If both  $x$  and  $y$  is equal to  $1$  and  $y$  and dot is equal to  $1$  then  $x$  is an inverse of  $y$ , it is called a two sided inverse of  $y$  with respect to the operation dot.

So once you define identity element you can talk about the inverse elements so if you have a binary operation dot and you have  $x$  equal to the identity element then  $x$  is the left inverse of  $y$  and  $y$  is called right inverse of  $x$ . And for an element if you have both the left inverse and the right inverse it is a two sided inverse.

(Refer Slide Time: 36.36)



**THEOREM:**  
If an element has both a left and a right inverse with respect to an associative operation, then the left and right inverse elements are equal.

**PROOF:**  
Let 1 be an identity for the operation  $\circ$ , and let  $x$  be an element with a left inverse  $w$  and a right inverse  $y$ . Then  
$$w \circ x = x \circ y = 1$$
By associativity of the operation  $\circ$ , it follows that  
$$w = w \circ 1 = w \circ (x \circ y) = (w \circ x) \circ y = 1 \circ y = y$$

You can easily see this also, if an element has both the left and a right inverse with respect to an associative operation then the left and the right inverse elements are equal. So, we are considering a binary operation which is associative and it has got a left inverse. If an element has both the left inverse and a right inverse then they are equal, how do you prove that?

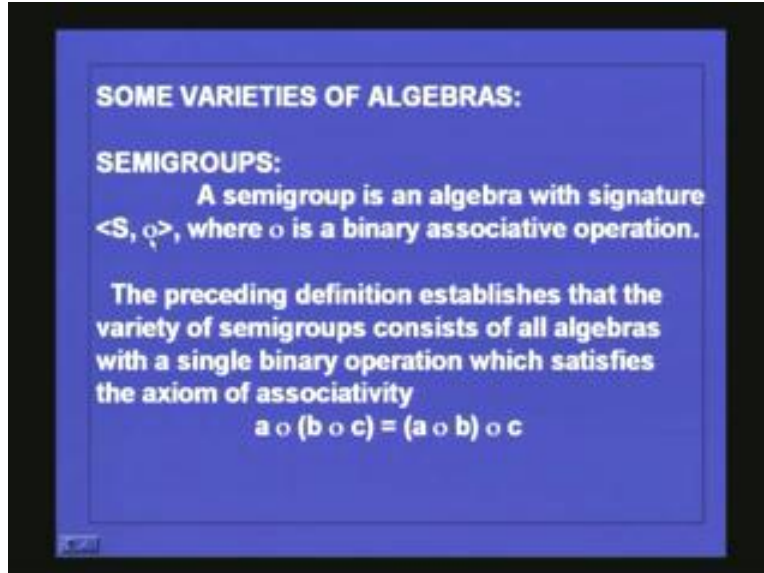
A similar result we have proved in the case of inverse functions, we were considering inverse functions, something like this if you remember we have considered the left inverse of a function the right inverse and showed that they are equal. This proof is also similar to that. So let the identity element be denoted by 1 with respect to the operation dot and let  $x$  be an element for which you have a left inverse  $w$  and a right inverse  $y$ .

For  $x$  you have a left inverse  $w$  and for  $x$  you also have a right inverse  $y$ . So  $(w \text{ dot } x)$  is equal to 1 and you also have  $(x \text{ dot } y)$  is equal to 1. The left inverse is  $w$  and the right inverse is  $y$  and we want to show that  $w$  is equal to  $y$ . How do you show that? And remember that this operation is associative so  $w$  is equal to you can write it as  $w \text{ dot } 1$  because it is an identity element and instead of 1 you can substitute  $(x \text{ dot } y)$  it is  $w \text{ dot } (x \text{ dot } y)$  and regroup because of the associative property you can regroup this and write it has  $(w \text{ dot } x) \text{ dot } y$ .

But what is  $(w \text{ dot } x)$ ?

$(w \text{ dot } x)$  is 1 so this will become equal to 1 dot  $y$  and so equal to  $y$ . So we have proved that  $w$  is equal to  $y$ . As mentioned earlier we are interested not only in the signature of the algebra but we are interested in algebras which follow a certain set of axioms, similar axioms. So we will consider such algebras one by one. The first one we shall consider is semigroups, these are called varieties of algebras.

(Refer Slide Time: 39.10)



First we will consider a semigroup. What is a semigroup?

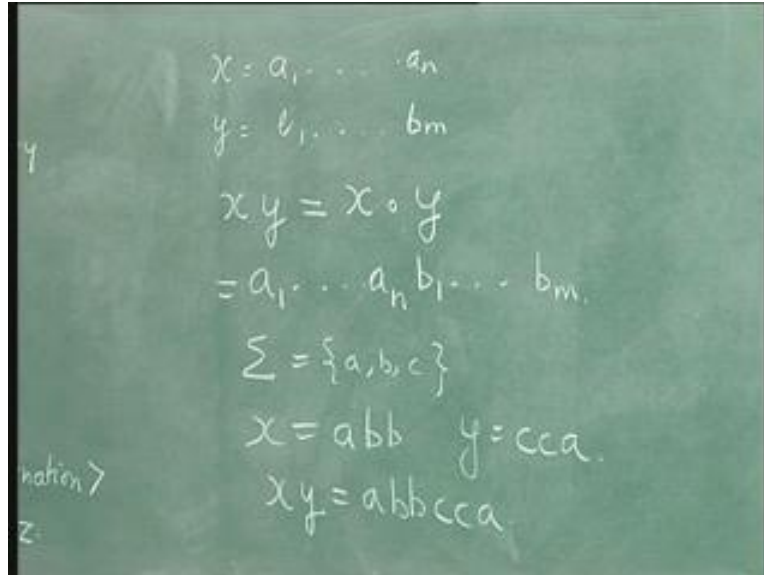
A semigroup is an algebra with signature  $\langle S, \cdot \rangle$  where this is a binary associative operation. So we see that the variety of semigroup consists of all algebras with a single binary operation which satisfies the axiom of associativity. That is  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ . So, two points have to be clear for semigroup. One is closure, the second is associativity.

If you take the set of integers and the addition operation you see that if you take two integers and perform the operation of addition the result also belongs to  $\mathbb{Z}$  so it is closed under plus and also associative property holds for addition. If you take integers and then take the multiplication operation, again with respect to multiplication integers are closed and also the associative property holds. Similarly, if you take the set of real numbers and plus and so on.

If you take  $\Sigma^*$  the set of all strings over  $\Sigma$  and concatenation operation, this is a binary operation. If you take like this you will realize that if you take two strings the concatenation of those strings is given by  $xy$  that also belongs to  $\Sigma^*$  so closure property holds and also associative property also holds for concatenation. If you take three strings  $x, y, z$  is equal to  $x, yz$ .

We have seen what is meant by concatenation in the earlier lecture in which if you take two strings  $x$  is equal to  $a_1, a_2, \dots, a_n$  and  $y$  is equal to  $b_1, b_2, \dots, b_m$  then the concatenation of  $x$  and  $y$  is denoted by  $xy$  and sometimes it is also denoted by  $(x \cdot y)$  and is given by  $a_1, a_2, \dots, a_n$  followed by  $b_1, b_2, \dots, b_m$ . or for example if you take the alphabet  $\Sigma$  to be  $a, b, c$  and if you take one string  $x$  is equal to  $abb$  and another string  $y$  is equal to  $cca$  something like this then  $xy$  concatenation is given by  $abbcca$ . Obviously we can see that concatenation is associative and also  $\Sigma^*$  is closed with respect to concatenation because if you concatenate two strings we again get a string from  $\Sigma^*$ .

(Refer Slide Time: 42.11)

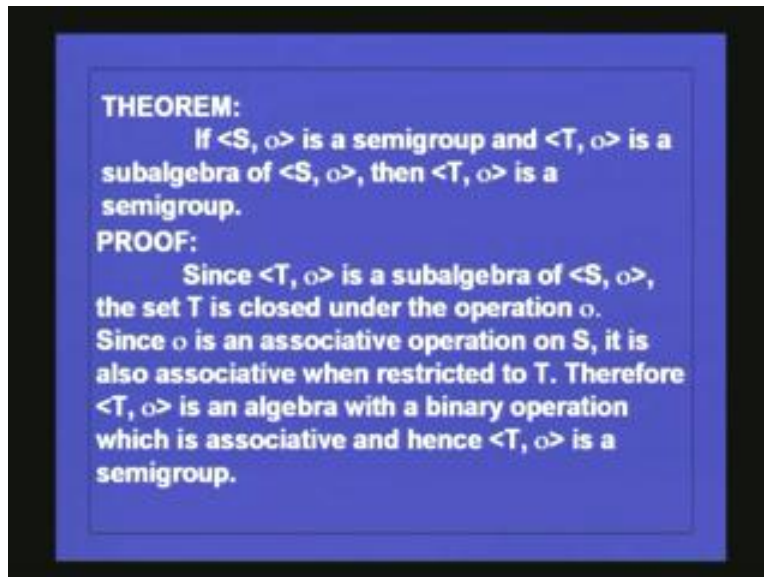


A chalkboard with handwritten mathematical expressions. On the left side, there are vertical labels 'y' and 'z' with arrows pointing to the right. The main text on the board is:

$$x = a_1 \dots a_n$$
$$y = b_1 \dots b_m$$
$$xy = x \circ y$$
$$= a_1 \dots a_n b_1 \dots b_m$$
$$\Sigma = \{a, b, c\}$$
$$x = abb \quad y = cca$$
$$xy = abbcca$$

So these are some examples of semigroups. The two properties are closure and associativity.

(Refer Slide Time: 42.21)



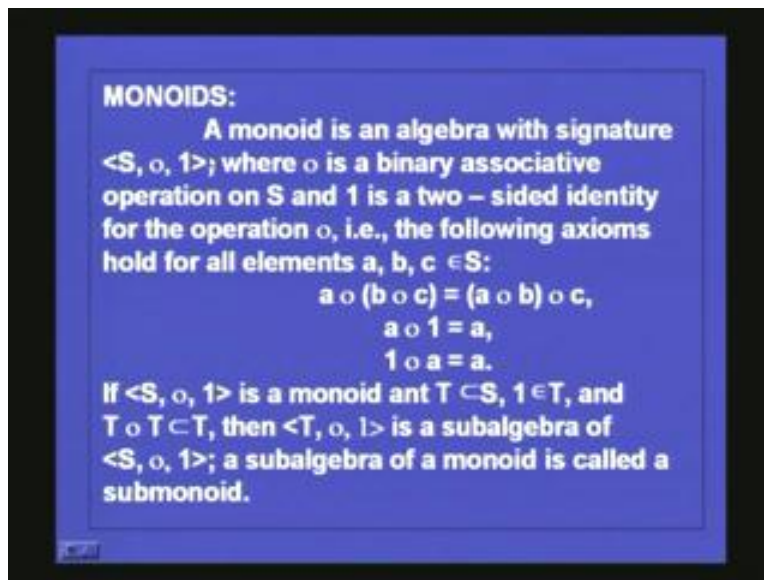
**THEOREM:**  
If  $\langle S, \circ \rangle$  is a semigroup and  $\langle T, \circ \rangle$  is a subalgebra of  $\langle S, \circ \rangle$ , then  $\langle T, \circ \rangle$  is a semigroup.

**PROOF:**  
Since  $\langle T, \circ \rangle$  is a subalgebra of  $\langle S, \circ \rangle$ , the set  $T$  is closed under the operation  $\circ$ . Since  $\circ$  is an associative operation on  $S$ , it is also associative when restricted to  $T$ . Therefore  $\langle T, \circ \rangle$  is an algebra with a binary operation which is associative and hence  $\langle T, \circ \rangle$  is a semigroup.

Now, if  $S$  dot is a semigroup and  $T$  dot is a subalgebra of this, you have a subalgebra of this then  $T$  dash  $T$  dot is also a semigroup. When do you say that something is algebra? The closure property should hold. So  $T$  dot is a subalgebra of  $S$  dot. The set  $T$  is closed under the operation dot since dot is an associative operation on  $S$  it is also an associative operation when restricted to  $T$ . Their associative property is not going to be altered whether you are going to consider  $S$  or a subset  $T$ .

Therefore  $T$  with the binary operation dot is an algebra which is associative and hence  $T$  with dot is a semigroup. So a subalgebra of a semigroup is also a semigroup. Next we consider one more restriction and see what is meant by a monoid. For semigroup we had two properties; closure and then associative property. Then third is existence of an identity element. If you also have an identity element then it is called a monoid. So, if you take a semigroup say  $S$  with dot it has got the closure property it has got the associative property. Apart from that if it also has an identity element then it is called a monoid.

(Refer Slide Time: 44.10)



A monoid is an algebra with signature  $S$  with dot where dot is a binary associative operation on  $S$  and  $1$  is a two sided identity for the operation dot that is, the following axioms hold for all elements  $a, b, c$  belonging to  $S$ ,  $a$  dot  $(b$  dot  $c)$  is equal to  $(a$  dot  $b)$  dot  $c$  this is the associative property. Then  $1$  is a two sided identity so  $a$  dot  $1$  is equal to  $a$  and also you have  $1$  dot  $a$  is equal to  $a$ . In this case the algebra is called a monoid. Examples of monoid are again we have taken the set of integers plus the identity element for this is  $0$  so the third property of identity also you take, this has a structure like this, a carrier, a binary operation which is associative and then an identity element  $x$  plus  $0$  is  $x$  and  $0$  plus  $x$  is also an  $x$ .

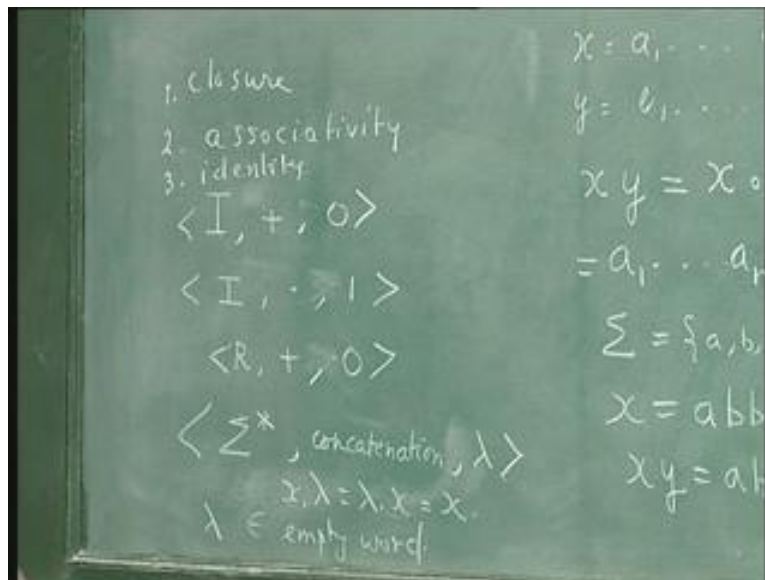
Similarly, in this case when you have multiplication if you take  $1$  the associative property holds closure property obviously holds then  $x$  dot  $1$  is equal to  $x$  and  $1$  dot  $x$  is equal to  $x$  as  $1$  is an identity element with respect to multiplication operation so this is also a monoid similarly  $R$  plus  $0$  is also a monoid.

If you take concatenation operation in sigma star and then take the identity element as lambda or the empty word, we have already seen that with respect to concatenation and sigma star as the associative property. But you see that if you take the empty word

$\lambda x \text{ dot } \Lambda$  is equal to  $\lambda$  dot  $x$  is equal to  $x$  where  $\lambda$  is the empty word.

$\Lambda$  is also sometimes denoted by  $\epsilon$  that is called the empty word. Here the empty word serves as the identity element. So  $\Sigma^*$  is again a monoid with respect to concatenation operation where the identity element is given by  $\lambda$  or sometimes it is also denoted by  $\epsilon$  which is the identity element. Sometimes you say that  $\Sigma^*$  is a free monoid generated by  $\Sigma$ . That is the usual terminology used in automata or formal language theory.

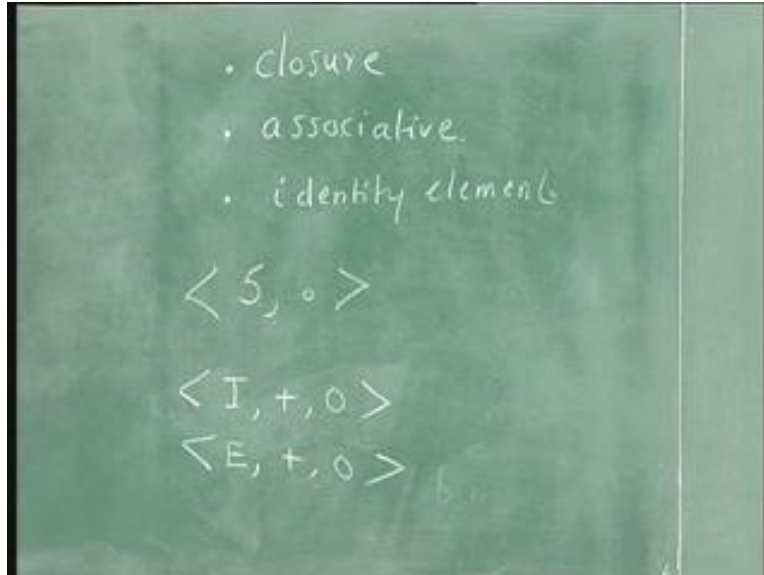
(Refer Slide Time: 46.46)



And again what is a submonoid?

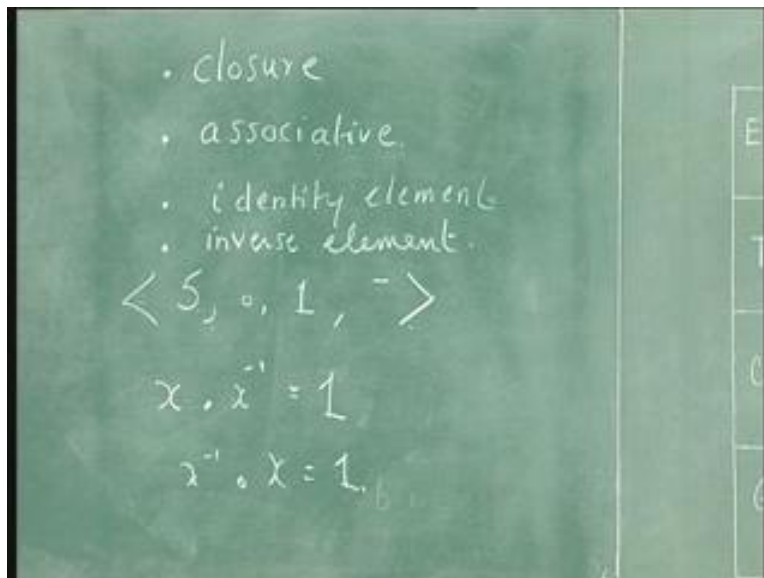
You see,  $S \text{ dot } 1$  is a monoid and  $T$  is contained in  $S$ ,  $1$  is also belonging to  $S$  that is is a subalgebra which is closed. Then  $T \text{ dot } 1$  is a subalgebra of  $S \text{ dot } 1$ . Then this subalgebra of a monoid is called a submonoid. For example, if you take the set of integers plus 0 this is a monoid and if you take the set of even integers plus 0 then this is a submonoid of this.

(Refer Slide Time: 47.38)



Next we add one more condition which is the existence of an inverse element that is called a group. So we have considered an algebra with carrier  $S$  a binary operation an identity element  $1$  and then one unary operation also is the existence of inverse. So, for each  $x$  there is an inverse element  $x^{-1}$  such that  $x \cdot x^{-1}$  is equal to  $1$  and  $x^{-1} \cdot x$  is equal to  $1$ . If each element has an inverse element such that this holds then the whole thing is this algebra is called a group. So a group has to satisfy four properties.

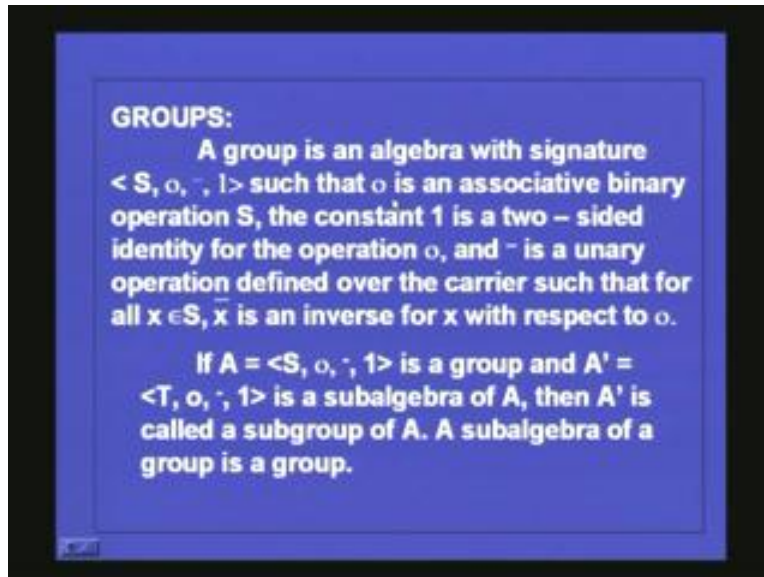
(Refer Slide Time: 48.41)





A group is an algebra with the signatures  $S, 0, \text{minus}, 1$ . Usually we write the constant in the end but this is the identity element this is a unary operation that is inverse element such that dot is an associative binary operation  $S$ .

(Refer Slide Time: 48.56)

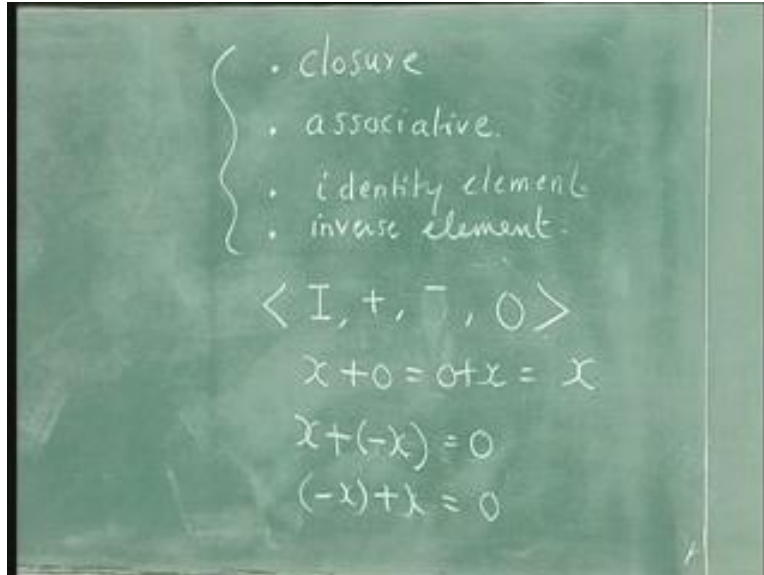


The constant one is a two sided identity for the operation dot and this is a unary operation defined over the carrier such that for all  $x$  belonging to  $S$  for every  $x$  you have an  $x$  bar which is an inverse of element with respect to  $\circ$ . So, if again this idea of a subgroup  $A$  is equal to  $S$  dot dash  $1$  is a group and  $A$  dash is equal to  $T$  dot dash  $1$  is a subalgebra then  $A$  dash is called a subgroup of  $A$ , the subalgebra is called a subgroup.

Now, let us consider some examples of groups. So the group has to satisfy these four properties, you have seen that it has to satisfy the four properties. Some examples of groups are, take the set of integers then the plus operation what is the element  $0$ ? This is the identity element with respect to addition and the unary operation is (minus  $x$ ). So usually, you can write the operation first and then the operation. Hence, let us see whether it is satisfying all the four properties.

If you take two elements it will be closed, the addition of two integers will give you another integer and addition is associative that is also true again existence of the identity  $x$  plus  $0$  is equal to  $0$  plus  $x$  is equal to  $x$ . Then inverse element for every  $x$  minus  $x$  is the inverse element. If you take (minus  $x$ ) the negative of that number then  $x$  plus (minus  $x$ ) is equal to  $0$  and (minus  $x$ ) again plus  $x$  is equal to  $0$ . So every element  $x$  has an inverse (minus  $x$ ). For  $0$   $0$  is its own inverse. Anyway the identity element is its own inverse. So the set of integers with the addition operation and the negative operation and the unary minus as a unary operation there is an inverse element then the identity element defines the group.

(Refer Slide Time: 51.29)



Take the set of even integers plus minus 0 this is again another group and this is a subgroup of that. Now, in the case of sigma star concatenation and lambda which is the identity element you cannot talk of it as a group because you cannot define the inverse element in this case. So it is a monoid but it is not a group.

Let us consider one more example of group. Let  $S$  be the set of all nonsingular matrices of some fixed size say  $n$  by  $n$ . The elements belong to a set of real numbers. Elements of the matrices belong to the set of real numbers. You can take integers or whatever it is. The set of all nonsingular matrices of size  $n$  by  $n$  the elements of the matrices belong to the set of real numbers.

Now, if you consider this  $S$  and the binary operation matrix multiplication inverse of the matrix and the identity matrix of size  $n$  by  $n$  this is identity matrix size  $n$  by  $n$  then this forms a group.


(Refer Slide Time: 53.51)



If you multiply two  $n$  by  $n$  matrices  $A$  and another  $n$  by  $n$  matrices  $B$  the product of  $A$  and  $B$  will be another matrix  $C$  which is another  $n$  by  $n$  matrix. So  $A$  into  $B$  will be  $C$ . If  $A$  and  $B$  are  $n$  by  $n$  matrices  $C$  also will be an  $n$  by  $n$  matrix and if  $A$  and  $B$  are nonsingular  $C$  will also be nonsingular. So the closure property holds, you have to check the closure properties one by one. So closure property holds and associative property you know that with respect to matrix multiplication if  $A$   $B$   $C$  are  $n$  by  $n$  matrices  $A$   $B$   $C$  is equal to  $A$  into  $B$  into  $C$  and this is known a fact and all are nonsingular matrices of size  $n$  by  $n$ . So the associative property also holds.

Now, if you take the identity matrix of size  $n$  by  $n$  which is  $1$   $0$   $0$   $0$   $0$   $1$  etc  $1$  this is the identity matrix of size  $n$  by  $n$  denote it by  $I$ . Then if you take any matrix  $A$  into, **I will give you**  $A$  and  $I$  into  $A$  will give you  $A$  so this is an identity element for this. For any nonsingular matrix an inverse matrix exists and that is denoted by  $A$  inverse. And there is a procedure to find the inverse matrix and so on. We know that if  $A$  is a nonsingular matrix  $A$  inverse will also be a nonsingular matrix and  $A$  into  $A$  inverse will be equal to  $I$  and  $A$  inverse  $A$  will be  $I$ .

(Refer Slide Time: 55.53)


$$\begin{aligned} & I \\ A \times I &= A \\ I \times A &= A \\ A \times A^{-1} &= I \\ A^{-1} \times A &= I \end{aligned}$$

Thus, for each nonsingular matrix  $n$  by  $n$  you have an inverse matrix of size  $n$  by  $n$  such that the product is equal to  $I$ . So for every nonsingular matrix you also have an inverse element. So, also these four properties are satisfied and this is an example of a group.

We have seen what is meant by a semigroup, a monoid, a group. We shall study some more properties of groups and some theorems about groups in the next lecture.