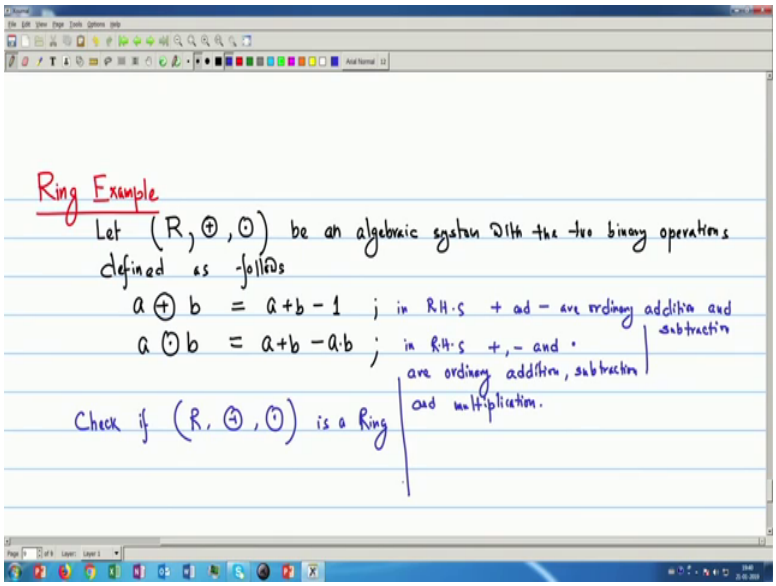
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 52
Ring and Modular Arithmetic (Contd.)

See, in the last lecture we have read the definition of ring and mainly the differences of the other algebraic systems like, semi group Monoid group where the set, a non-empty set we have considered with one binary operations defined on it. And, then what are the axioms are satisfied by the set with these options. Ring is mainly different from others algebraic systems, because it is in it involves two binary operations on the non-empty set. And, and we have read the what are the properties that it must hold.

There, we have the two binary operations, we have called the addition and multiplication, but that are not always the ordinary addition and multiplication it may be ordinary addition or multiplication.

(Refer Slide Time: 01:39)



So, first we will see one such example, that where the operations are two binary operations, but not the our ordinary addition and multiplication. So, first we consider the ring examples; that means one example with two binary addition operations, which are not ordinary addition or multiplication.

So, we consider one example that is trick let say R is a ring R is a or better I write R normally the way we write R I give two operations like that. So, let R I am telling plus dot be a ring or initially I take that it is an algebraic system with the two binary operations defined as follows, because I am not taking these are ordinary addition or multiplication.

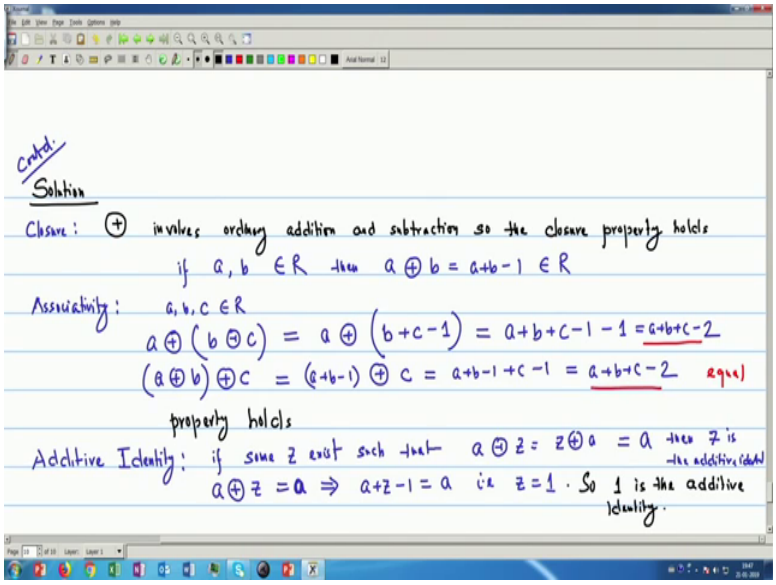
So, what are those operations? The operations I am taking that one addition I am defining that a addition b is a plus b minus 1. Here, this right hand side of the equation in RHS plus and minus are ordinary addition and subtraction, ordinary addition subtraction.

And, the multiplication we defined a dot b is a plus b minus a into b a b; that means, multiplication. So, similarly in R.H.S plus minus and better I give a dot and dot are ordinary addition, subtraction and multiplication. So, the here the plus and dot within circle we have we are taking two binary operations are define like that. So, they are not simple ordinary addition or multiplication, but it involves some addition subtraction and multiplication.

Now, we check whether this algebraic system becomes a ring or not. So, check if R plus dot, if the algebraic system is a ring.

So, if we remember the properties of ring. So, 1 by 1 we try to check that thing ok.

(Refer Slide Time: 07:20)



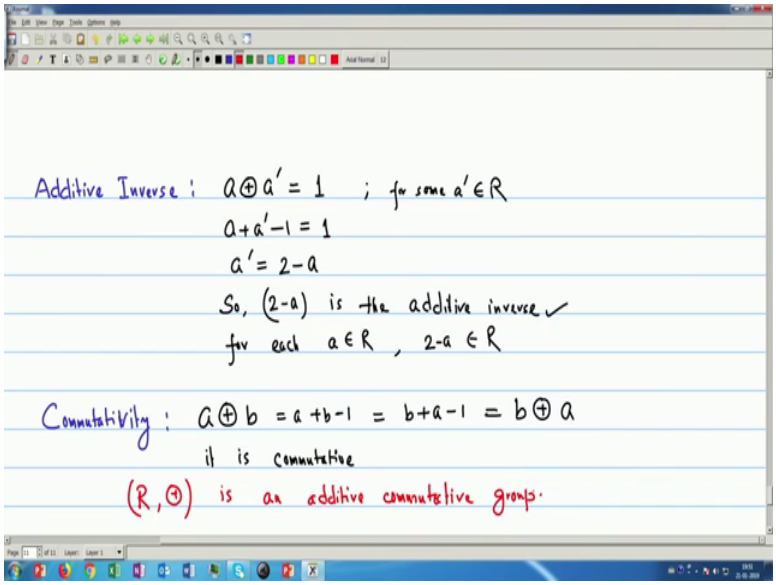
So, we give the solution this is a continuation. Now, first the closure; so, the closure with respect to addition. So, here addition is this addition. So, this involves these operations involvers, ordinary addition and subtraction. So, it so the closure property holds, that is that if a b belongs to R, then a plus b equal to a plus b minus 1 belongs to R.

Now, we see that associative property ok. So, this is my I write this is closure then we see the associativity. So, if a b c belongs to R first we see that a b plus c, this becomes a and this part is a plus sorry b plus c minus 1 b plus c minus 1. Again, if we apply we will be getting a plus b plus c minus 1 minus 1. So, this becomes a plus b plus c minus 2.

Now, if we take a plus b first and then c, we will be getting a plus b minus 1 c is a plus b minus 1 plus c minus 1 is equal to a plus b plus c minus 2. So, these are equal, what you see that these two are equal. So, though associativity property holds associativity property holds. Now, additive identity we see the so, if say some Z exists such that a plus Z equal to a equal to a then Z is the additive identity.

Then, Z is the additive identity. So, if I write a plus Z. So, a plus Z equal to a which implies that a plus Z minus 1 equal to a that is Z equal to 1. So, one is the identity of or additive identity. So, one is the additive. So, we notice that, here these addition in a circle is the addition operations we are assuming is the additive identity. Now, what about additive inverse?

(Refer Slide Time: 14:15)



So, if we remember the what definition that, if I have some element say inverse element. So, that a addition a dash equal to my identity and identity becomes 1.

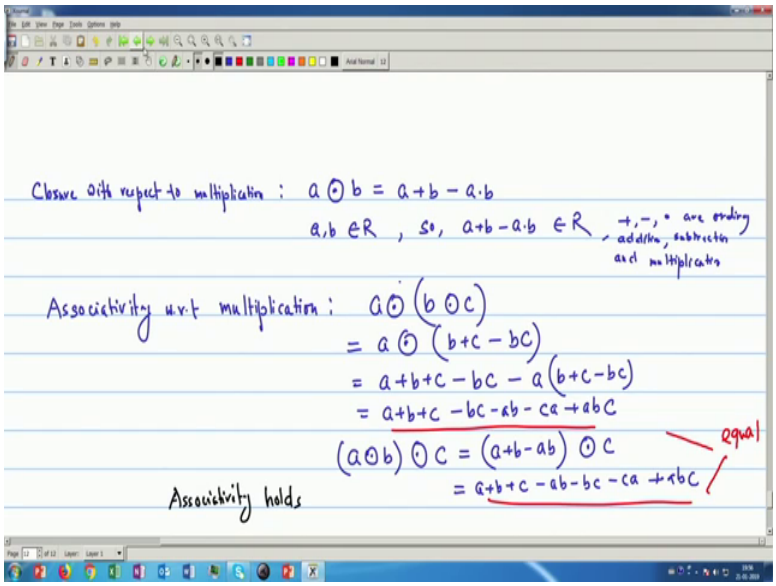
So, what is a dash for some we have to check whether some a dash exists or not for some a dash belongs to R. So, here a plus a dash minus 1 equal to 1, so a dash equal to 2 minus a. So, 2 minus a is the additive inverse. So, obviously, for each a for each a belongs to R, 2 minus a belongs to R and it exists. So, the additive inverse also exists. So, we have seen the closure associativity, additive, identity additive inverse. Now, we have to see the commutativity with respect to the addition.

So, we see the we will see the commutativity with respect to addition. So, a; obviously, a addition b equal to a plus b minus 1 equal to b plus a minus 1, equal to b sum a. So, it is commutative. So, it is commutative. So, we get that up to this property we holds, it is a this it is a additive. So, R is a an additive commutative group.

Since till this time we have consider only one operation and that is this addition commutative group. Now, I have another operation is multiplication. So, now, we check the multiplication properties or the properties with respect to my multiplication.

And, again we notice that this multiplication is not the ordinary multiplication, it is actually a multiplied by b means a plus b minus a b and that a b is my normal multiplication or the product normal product. So, if we remember now with respect to multiplication, we have to check the first the closure.

(Refer Slide Time: 18:30)

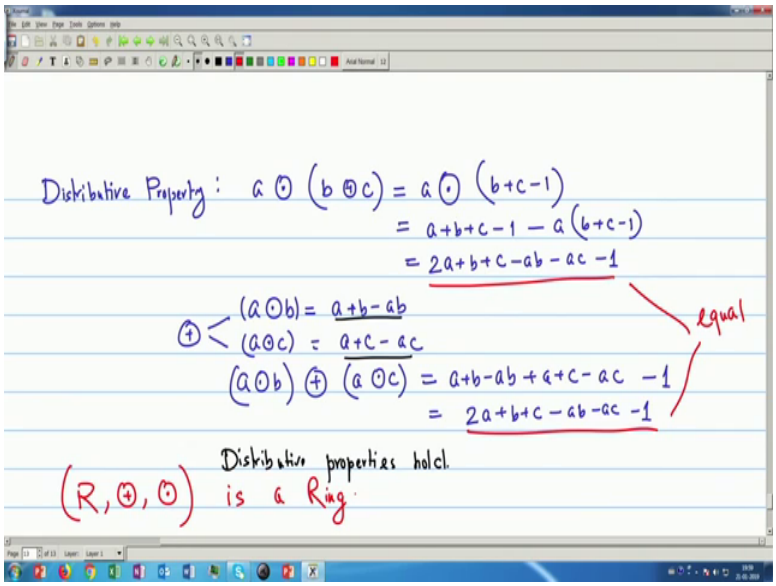


So, this is closure with respect to multiplication closure, with respect to multiplication then if I take that a now this time this is my multiplication is a plus b minus a into b. So, since a b belongs to R.

So, it is normal ordinary addition and subtraction and multiplication. So, a plus b minus a b belongs to R, because plus minus and dot an ordinary addition, subtraction, and multiplication. Now, what about my associativity or I can write associative properties with respect to multiplication with respect to multiplication? So, we write a c this equal to a this is b plus c minus b c equal to a plus b plus c minus b c minus a normal multiplication b plus c minus b c.

So, this becomes a plus b plus c minus b c minus a b minus c a plus a b c. Now, if I consider the ordering of multiplication is changed; that means, a dot b first then multiplication c. So, this becomes if you check this also becomes a plus b minus a b c which gives that a plus b plus c minus a b minus b c minus c a plus a b c. So, we see that the these two are equal. So, associativity holds.

(Refer Slide Time: 22:36)

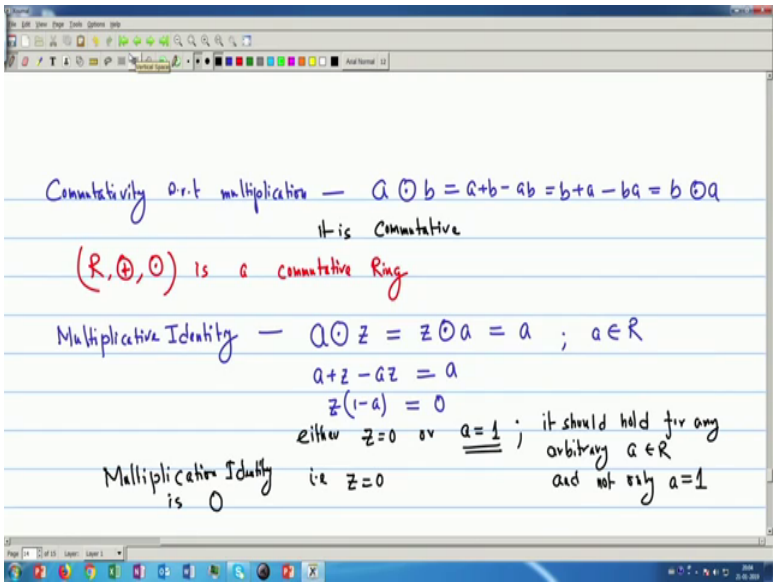


Now, what is my distributive properties with respect to the addition and multiplication defined?

So, we can write that this is since multiplication is distributive over addition. So, this we can where a b c belongs to R. So, I can write a and this becomes b plus c minus 1. This is equal to a plus b plus c minus 1, because a plus b minus a b plus c minus 1. So, this becomes 2 a plus b plus c minus a b minus a c minus 1. Now, we see the if we do the a dot b this becomes a plus b minus a b, if we take the a dot c, then this becomes a plus c minus a c, now if we these two if we add; that means, a b plus a c.

So, this becomes a plus b minus a b plus a plus c minus a c minus 1, because my addition is a plus b minus 1. So, here this is a this is my a this is my b. So, this becomes 2 a plus b plus c minus a b minus a c minus 1. So, again we see that these and these they are equal. So, the distributive properties hold. So, it becomes a ring the so, R these algebraic system is a ring. Now, whether it is a commutative ring or not, now over ring if I add the commutativity with respect to multiplication.

(Refer Slide Time: 26:22)



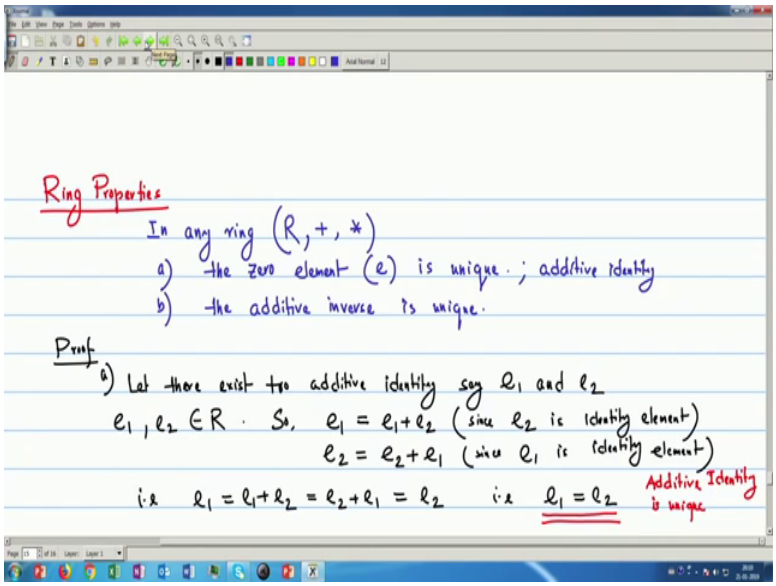
So, this is if I take a b belongs to R. So, this a b is a plus b minus a b equal to a plus or I can write b plus a same thing, I can write b plus a minus b a equal to b a. So, it is commutative. So, it is a commutative ring R. Now, if we add the if we see the multiplicative identity, we check whether it exist or not multiplicative identity; that means, I have some a dot Z if I take that type Z exists equal to a equal to a.

So, a plus Z minus a Z equal to a since already commutative. So, Z into 1 minus a equal to 0 and this is for all a belongs to R. Now, see here this become 0; that means either Z equal to 1, this is either Z equal to 0 or a equal to 1. Now, see this a equal to 1 that this property should hold for any arbitrary a not only for 1. So, this should hold for. So, I can write that it should hold for any arbitrary a belongs to R and not only a equal to 1.

So; that means, that is Z equal to 0. So, my multiplicative identity is Z equal to so, multiplicative identity exist and it is 0 multiplicative identity is 0. So, the properties that, we see that it has multiplicative identity is also exist. So, in this way we can check that it is a ring; it is a commutative ring and with a multiplicative identity exists.

Now, we see the some properties of so here some example we have studied that with addition and multiplication, which are binary operations, but not the ordinary addition or binary multiplication.

(Refer Slide Time: 31:08)



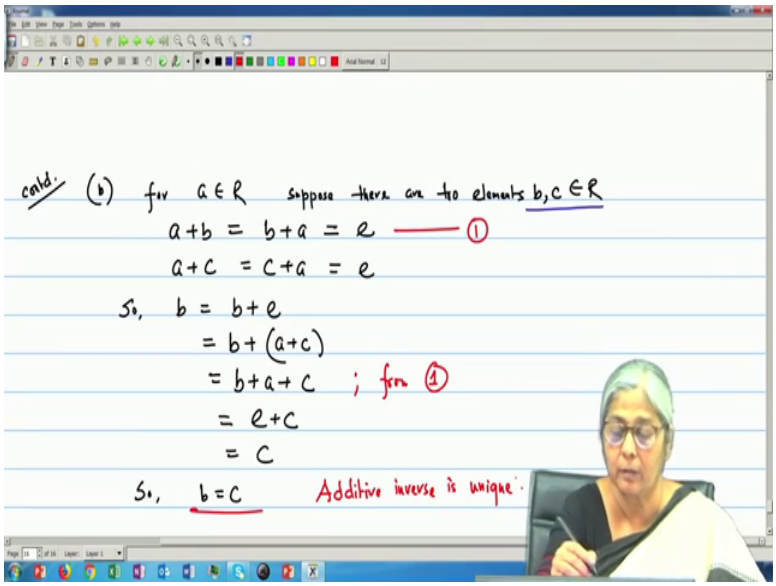
Now, we see some properties that we called the ring properties. Now, we have defined ring we with two binary operations. Now, these we can write that in any ring R plus star that telling that as if some addition and multiplication. The, the properties are that 1 we can write the 0 element for addition, because we know that 0 is the additive identity. So, if I write that 0 element is e I write the additive identity is e it is unique.

Same way I can write the additive inverse. So, e is the additive identity. The additive inverse is unique. Now, I can prove I give a proof the proof is very simple. So, for a part let there are two let there exist two additive identity; say e 1 and e 2. So, if some a belongs to R so, then a plus e 1; that means, I can write if I consider that e 2 is since it is identity; that means, e 1 and e 2 both belongs to e 1 e 2 belongs to R.

So, I can write e 1 equal to since it will belongs to R; that means another element of R. So, I can write this is e 1 plus e 2. Since, e 2 is the identity element, since e 2 is identity additive identity.

Similarly, I can write e 2 equal to e 2 plus e 1. Since, e 1 is the identity element so; that means, that is e 1 equal to e 1 plus e 2, since it is commutative with respect to addition. So, I can write equal to e 2 plus e 1 equal to e 2 that is e 1 equal to e 2. So, the for e part we see the multiplicative identity is unique sorry additive identity is unique this is addition additive identity is unique.

(Refer Slide Time: 36:30)

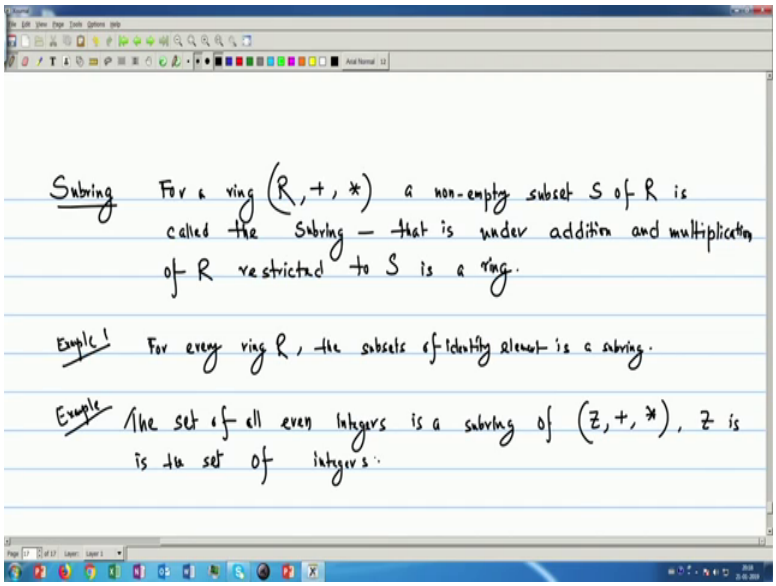


Now, the what about the additive inverse that we can write that for additive inverse that means, my b part. So, for a belongs to R. Suppose, there are two elements similarly I can take two elements b belongs to R, or I can take two elements b and c I can take two elements b and c belongs to R. Such that a plus b equal to b plus a equal to e the identity, similarly a plus c equal to c plus a equal to the identity.

So, if I write. So, b equal to b plus e, since it is a inverse equal to b plus I can write e is my a plus c. So, this becomes b plus a plus c. Now, my b plus a is e from here b plus a equal to e. So, this is e plus c equal to c only so; that means so, b equal to b equal to c. So, again; that means that my additive inverse is also unique.

Now, we can see that sub ring, we can see that just we can define the way, we have define the subgroups sub monoid, sub semi group, and we can define the sub ring.

(Refer Slide Time: 40:00)



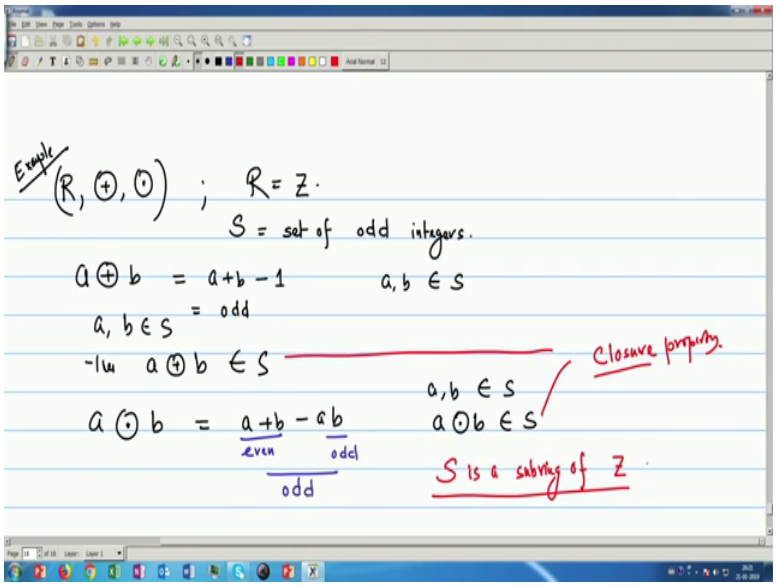
So, for a ring R again plus star a non-empty set a non-empty subset say S of R is called the subring, that is under addition and multiplication.

That means here the plus and star and as usual that it may or it may not be the ordinary addition or multiplication the R multiplication of R the restricted to S is a ring; that means, that in other words I can tell that with S is a subset of R, then with respect to the this addition and multiplication defined over R, that S is also closed and S is becomes a ring.

So, this is a subring, then example I can for every ring R. The subsets of identity element is a subring or our known example we see that other algebraic systems we have seen, the set of all even numbers, even is a subring of Z plus star where Z is the set of integers, or even I can take the set of positive integers.

Then, also it holds set of positive integers. Here, you can write set of integers. So, there are many such properties of subring and we can write.

(Refer Slide Time: 44:39)



And, some of these 1 very important property, I can tell that or if we if we consider that examples, that earlier we have taken with respect to that, if we remember that one ring that example we have taken earlier R the class dot that ring.

We have considered and if we see that whether this becomes a sub ring or not, say we have considering that now it is instead of R that R is actually my Z, Z say R equal to we consider R equal to the Z. And, the subset S is set of odd integers, set of odd integers. Then, what about the addition, that say a addition b is a plus b minus 1. So, if a b belongs to S odd integers, then this becomes odd. So, this is; that means, a b belongs to so, this because a plus b is even so, this is odd.

So, a b belongs to R sorry S a b belongs to S, then a x plus b belongs to S, then what about the multiplication that a b is a plus b minus a b. So, if a b are odd. So, this becomes even and this becomes odd. So, this becomes odd. So, I can write that a b belongs to S, a dot b belongs to S. So, we can see that with these two these are actually holds the closure property. So, I can write that S is a s is a actually sub ring is a sub ring of Z, here R equal to Z ok.

So, we have read the algebraic systems ring and with two binary operations which is different from the others I repeatedly we are mentioning and then some examples. Mainly to show that the addition and multiplication the two binary operations that we are defining with ring, that I am not ordinary, that may or may not ordinary addition and

multiplication. And, we have read some of the properties and how actually one algebraic systems, whether it forms a ring or not that we have studied with some examples. So, with this we finish the discussion on the ring.

Next day, we will see the other properties and how they are related there are some operations and how they are related with ring.