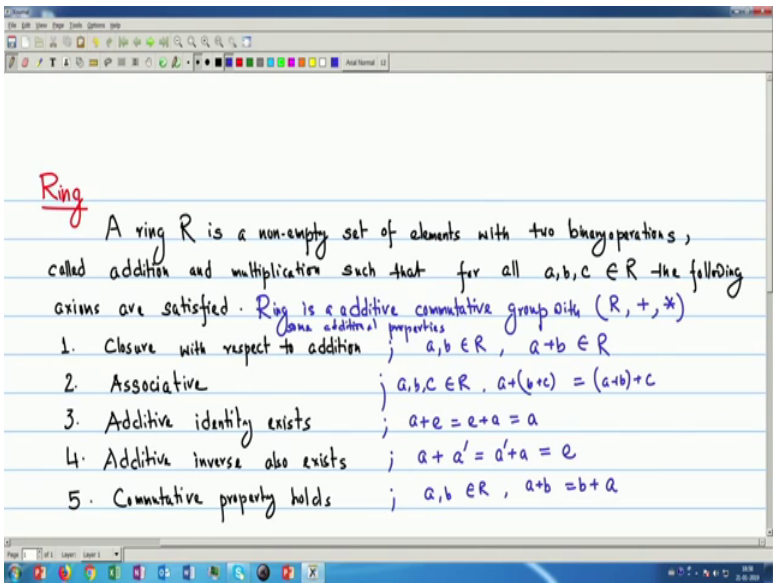
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 51
Ring and Modular Arithmetic

So, we are discussing about the algebraic structures and some general properties of the algebraic systems we have read. And, now based on the properties that the one set with some binary operators, they are satisfying, we are defining the different algebraic systems. We have read the semi group, monoid and group. And, today we will read the another algebraic structures Ring.

(Refer Slide Time: 01:00)



Now, this algebraic structure ring is slightly different from the other three that we have read. Normally, the algebraic systems we have defined, that one set or non-empty set with finite or infinite number of elements and, a binary operator one single binary operator defined on the set.

Now, for this ring that instead of one operator, that two operators will consider and the general properties that the commutativity, associativity, closure, that multiplicate, the identity inverse, etcetera, that we have read. And, we will see that for the two operations defined on this ring and what are the properties that must satisfy. So, that this algebraic system we can call a ring.

So, ring R is; if I give the definition is a non-empty set of elements with two binary operations. Normally, we called addition these two operations are addition and multiplication, but these addition and multiplication may not be our ordinary addition and multiplication. There are there can be two different operations, but normally we call them addition and multiplication; such that for call all elements a, b, c belongs to R the following properties are satisfied.

Now, since there are two operations. So, what are the properties based on these two operations that we identify. So, first thing is that this is a additive commutative group. Ring is a additive commutative group. So, it can write the ring; so, obviously, since it is a group so, the property of the group that group satisfied; that must be satisfied.

So, we write the group properties we remember, that it must satisfies the closure. So, since now we have two operations. So, closure with respect to addition. If, we remember that when we have define the group, then consider only one operation. So, with respect to one operation say the addition first we are considering.

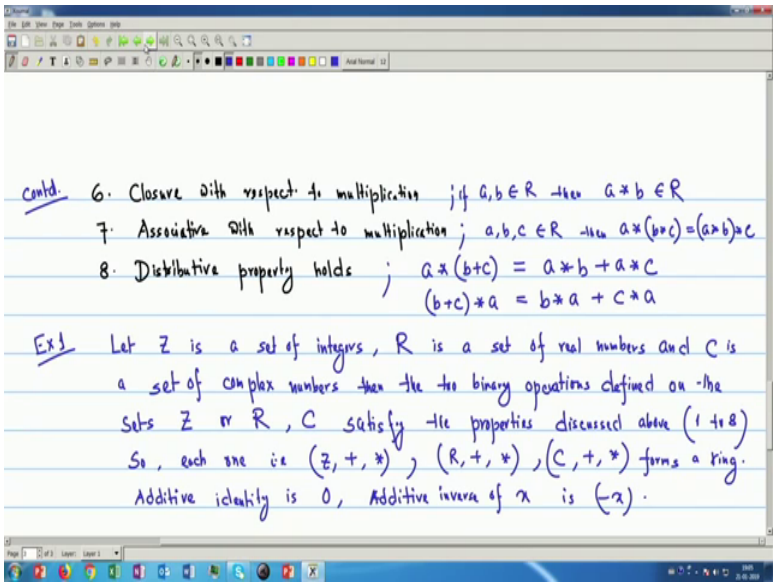
Then, the, it should be the associative; it must hold the associativity. So, it is associative then the additive identity exists and if it is a group, then there must be additive inverse also. So, additive inverse also exist. Now, it is a commutative group; so; though it must hold the commutative property. So, now, commutative property holds.

So, if we quickly write that closure we remember that if a b belongs to R, then a plus b belongs to R.

So, the notation we are taking that plus and star. So, the ring we are defining R plus star. As it plus is addition and star is multiplication. Now, if it is associative then a, b, c belongs to R with respect to addition. So, we write a plus b plus c is a plus b plus c. Now, additive identity exists. So, if e is the additive identity, then a e is e plus a equal to a only. Additive inverse exist; so, we know that a plus if a dash is the inverse of a is a dash plus a equal to the identity.

Now, if it is commutative property holds, then a b belongs to R, a plus b equal to b plus a. So, this is only the a. Ring is a additive commutative group in addition the sum of the properties so, with some additional properties some additional properties. Now, what are those properties? So, these are only with respect to addition.

(Refer Slide Time: 09:18)



So, in addition we write it is continue the properties. Now, we remember there are two binary operators when we are discussing the ring. So, now, we considered the multiplication operation.

So, again this 6 property will be the it is closure property, closure with respect to multiplication, than it is associative with respect to multiplication. Now, it is distributive in nature. Since, we have two operations. So, now, this is distributive property holds. Now, these are the three additional properties. So, since we have taken the star notation for multiplication. So, if a b belongs to R, then a star b also belongs to R. Now, associative so, a b c belongs to R then a star b star c is equal to a star b star c.

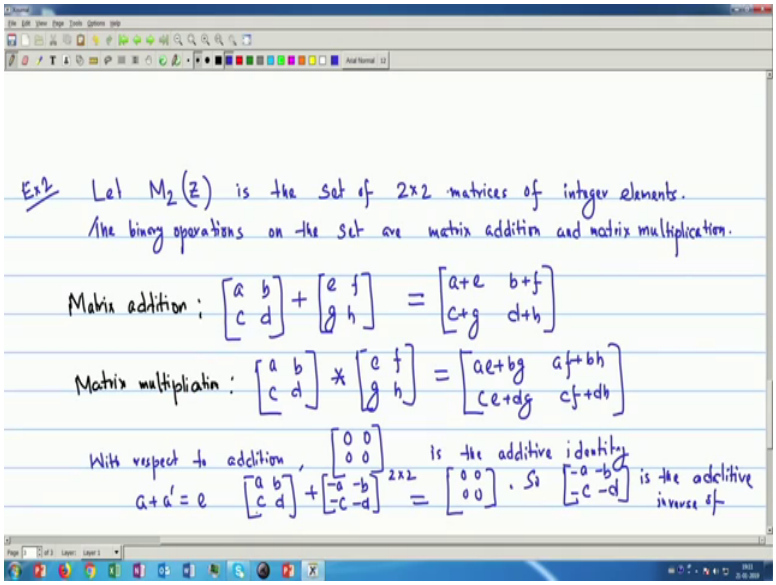
Distributive property holds; so, we take that multiplication is distributive over addition. So, a star b plus c equal to a star b plus a star c or I can write that b plus c star a since it is ok, we write the two operations that I can write b star a plus c star a. So, these are the three additional properties over additive commutative group that makes a algebraic system ring; this is my ring. So, give simple example that where this property holds.

So, let Z is a set of integers, R is a set of real numbers and C is a set of complex numbers, then the two binary operators or operations defined on this sets say Z, or R real numbers or complex numbers will satisfy all the properties, this satisfy the properties. Just now we discussed that the commutative group, additive commutative group and the though with respect to multiplication the closure associative and distributive. Now, I can

write that 1 to 8 that we have discussed. And, so, each one; that means, Z, plus, star, R, plus, star, C the complex number, plus, star forms a ring.

And obviously, when we are considering the complex number; the multiplication is the multiplication of between multiplication two complex numbers, or addition of two complex numbers. Now, here the addition or the additive identity is 0 and additive inverse is of additive inverse of x inverse of x is minus x. Normally, we will take like that.

(Refer Slide Time: 16:36)



Now, we consider another example of different type. Say we consider a set of matrices; 2 by 2 matrices. So, let M 2 Z is the set of 2 by 2 matrices or integer matrices; that means, matrices of interior elements. The two binary operations on the set are matrix addition and matrix multiplication.

So, quickly we see that what is matrix addition; 2 by 2 Matrix; so, we consider the say a b c d plus e f g h. And, this is equal to; it is; we know the matrix addition is defined as the sum of element wise addition or the sum of elements; that means, a plus e b plus f c plus g and d plus h.

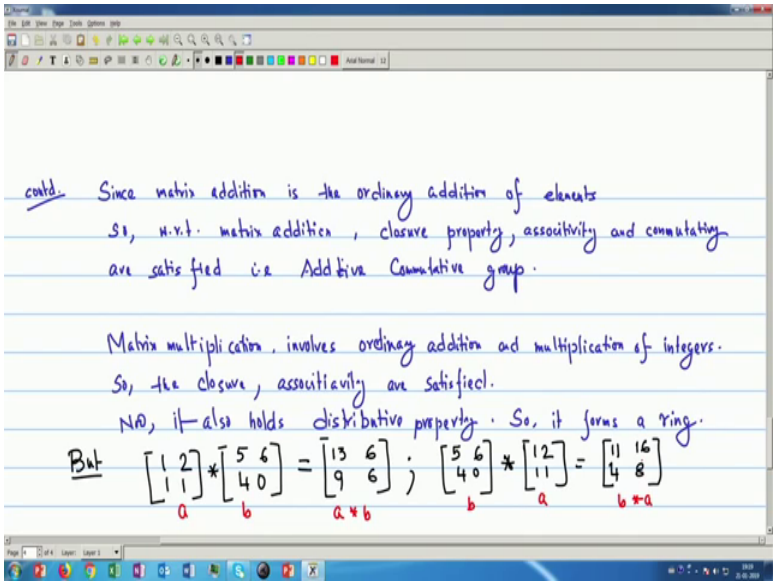
Now, how we define the matrix multiplication? If, I take the same matrix a b c d, now I take multiplication; then e f g h equal to we know that a e plus b g, then a f plus b h, c e plus d g, c f plus g h, this is my matrix multiplication. Now, if we see that then I can

write my matrix or additive identity; matrix addition if we consider, then with respect to the operation addition; that 0 0 0 0, this 2 by 2 matrix is the additive identity. Since, if we add element wise 0 then I will be getting the same matrix, now this is additive identity.

Then, what is additive inverse? That; we know that a plus; a plus a dash equal to e; that means, if I take the 2 by 2 matrix is a b c d, then my minus a minus b minus c minus d is equal to give me 0 0 0 0. So, minus a minus b is my additive inverse, minus a minus b minus c minus d is the additive inverse of a b c d.

So, if I now seems the element wise it is the addition and our normal addition is closure property holds. So, obviously, for addition also matrix addition also the closure property holds.

(Refer Slide Time: 22:29)



So, if I continued; so, since matrix addition is the ordinary addition of elements matrix elements. So, we can see that; so it with respect to addition, I should tell that matrix addition, The closure property the associativity, and commutativity are satisfied.

So, already we have seen that it is additive; that is it is matrix addition is or the set of 2 by 2 matrices with respect to matrix addition is the additive, commutative group. That we have seen when we have studied this example as a example of a group.

Now, what about the matrix multiplication? So, matrix multiplication if we see, then multiplication is defined as a multiplication, ordinary multiplication and addition. So,

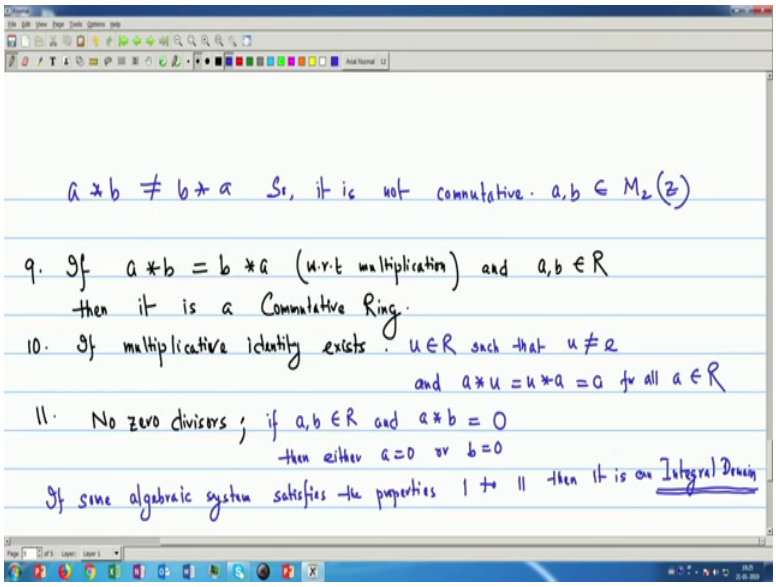
closure property holds. So, if we consider the matrix multiplication, matrix multiplication, inverse ordinary addition, and multiplication of elements integer, because we have considered the integer matrices; multiplication of integers.

So, the closure property, the associativity are satisfied. Now, since it is multiplication. So, the multiplicative identity, multiplicative identity is sorry we have not yet read that the distributive properties, we have to with respect to multiplicative operations of the multiplication matrix multiplication, the distributive property also holds. So, it forms a ring.

But, one thing we observe or we notice, that if we take say one example that 2 matrix; 2 by 2 matrix of like say 1 2 1 1 and 5 6 4 0. If, I do the matrix multiplication we get 1 into 5 plus 2 into 4 that is 13, then 1 2 6 0 that is 6, 1 1 this is 9 and again this is 6. Now, if we take the 5 6 4 0 same matrix in different order; that means, a b and b a. So, 1 2 1 1 then we get that 5 plus 6, this is 11, then this is 10 plus 6 it is 16, 4 0. So, this becomes 4 and this becomes 8.

So, what we see that this a b, if I consider that a is a 2 by 2 matrix and b is a 2 by 2 matrix, this is a star b and this is we take b and a. So, this is my b star a and these two are not equal.

(Refer Slide Time: 30:02)



So, what we can conclude that though if a b or bit error rate with respect to my matrix multiplication, this is not equal to b star a. So, it is not commutative. So, that means, if the if we want a commutative rings, then we have in addition we have to make that this property should hold. So, here actually here a, b belongs to M 2 Z ok. So, if I add then that the ring also holds; that means, if earlier we have seen that the ring holds the 8 properties. Now, if we give as if this is a ninth properties that if a star b equal to b star a ; that means, with respect to; with respect to the operations multiplication, may or may not be the original multiplication ok. And a b a b belongs to R, then it is a commutative group; commutative ring, then it is a commutative ring.

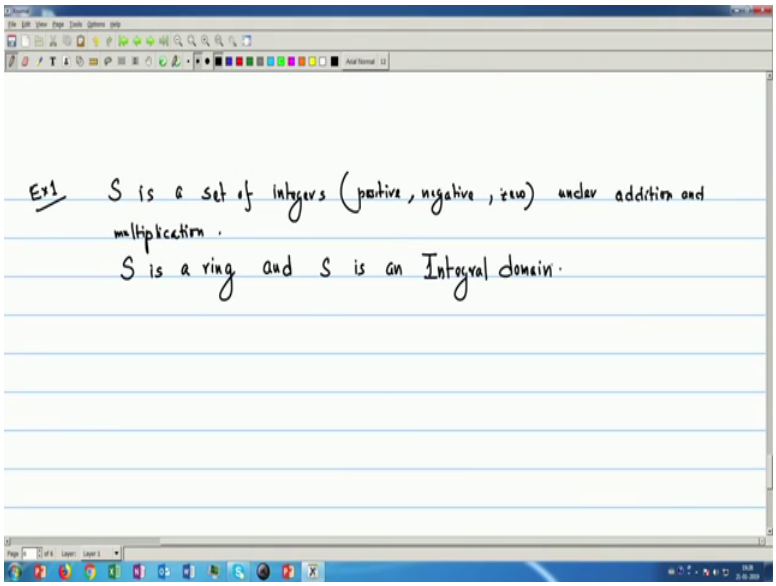
Now, if we add some more properties with respect to multiplication. So, I see that; see with respect to multiplication we are considered closure, we are considered associative and with respect to both addition and multiplication, we have considered the distributive properties, but if I consider say the; if multiplicative identity exists ok. So, if multiplicative identity exists that is I can write that say some element u belongs to R such that u not equal to the additive identity say e.

And, a u or it should write a star u since multiplicative multiplication sign we have taken star, a star u equal to u star a equal to a for all a belongs to R; that means, one multiplicative identity exists.

Another property we take that say no 0 devices. This is my property that no 0 devices; that means, if a b belongs to R and a star b equal to b star a equal to 0. Then, either a equal to 0 or b equal to 0. Then if these all 3 all 1 to 11 this property holds. So, if some algebraic systems or I can tell the ring in the algebraic system satisfy. So, the properties1 to 11, then it is an integral domain it called an integral domain.

That means over the properties of over the properties of ring, we can add the properties of that commutativity with respect to multiplication, then multiplicative identity exist and no 0 devices, then this becomes a this is called that Integral Domain.

(Refer Slide Time: 37:01)



Now, if I just take the example that S is a set of integers say positive, negative, and zero, under addition and multiplication, ordinary addition and multiplication, then S is a ring first and S is the additional 3 properties also hold. So, S is an integral domain; that means, it is a commutative ring with multiplicative identity and with no zero devices.

So, we have read the mainly the definition of ring how one algebraic systems, becomes a R and what are the properties over the group the other algebraic systems that we have read earlier so that it becomes 18. And, then again the properties over ring, we have considered some other additional properties with respect to the another binary operations, that commutativity, multiplicative identity and no zero devices, then this is making an another algebraic systems or the variant of ring sometimes we called this is the integral domain.

And, we will read some examples and some more properties of ring in the next lecture. Because, in real life or in ring has different type of application particularly in computer science and in mathematics as usual that ring has a number of applications area. So, we will see some of the properties.