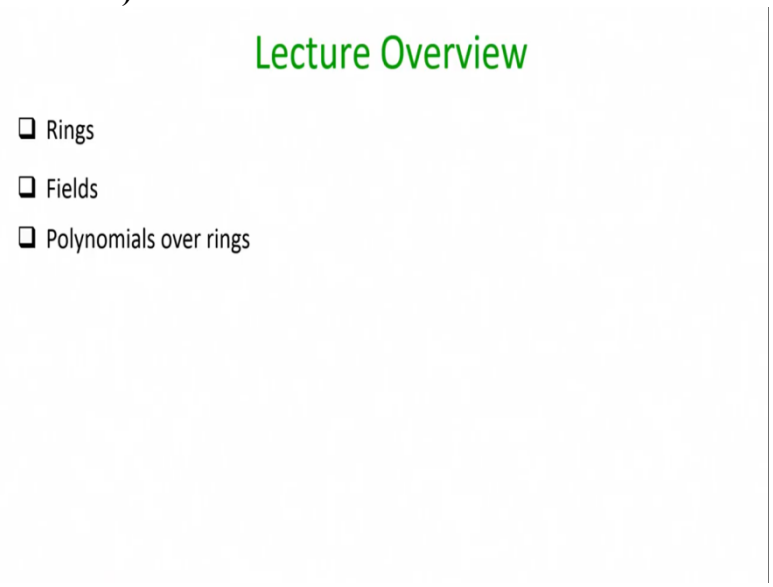
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology, Bangalore

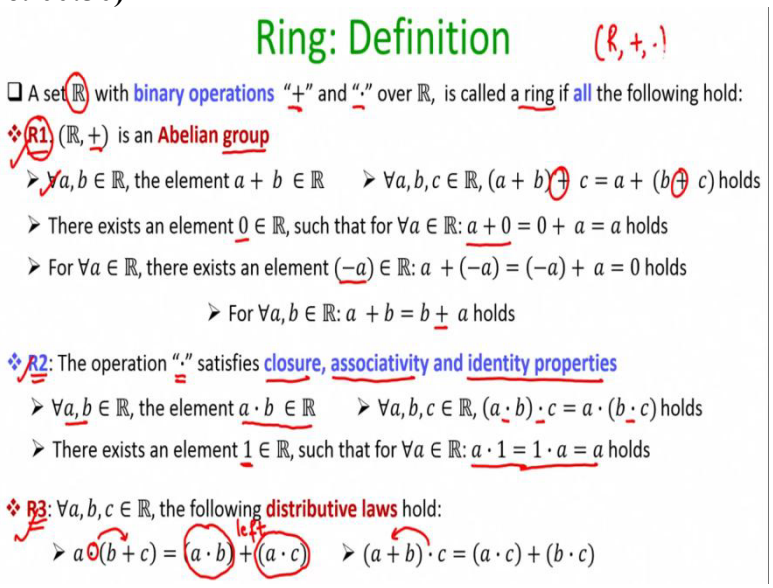
Lecture - 66
Rings, Fields and Polynomials

(Refer Slide Time: 00:24)



Welcome to this lecture. So, the plan for this lecture is as follows. In this lecture we will discuss about rings, fields and polynomials over rings.

(Refer Slide Time: 00:30)



So, let us begin with the definition of a ring. So, we denote our ring by this notation $\mathbb{R}$ and it is an algebraic structure. So, namely a set, set of values, it could be a finite set, it could be infinite set, so, it is a set and there are 2 operators plus (+) and dot (·) which are defined over the elements of this set. I stress that these are not integer plus and integer dot they are just some abstract operations.

But for the sake of notation we are using this plus notation and dot notation. So, we will say that this set $\mathbb{R}$ along with these 2 operations plus and dot will be called a ring if all the following ring axioms are satisfied. Axiom number 1: we need the set $\mathbb{R}$ to satisfy the properties of an abelian group with respect to your + operation and what are the properties that we require from an abelian group.

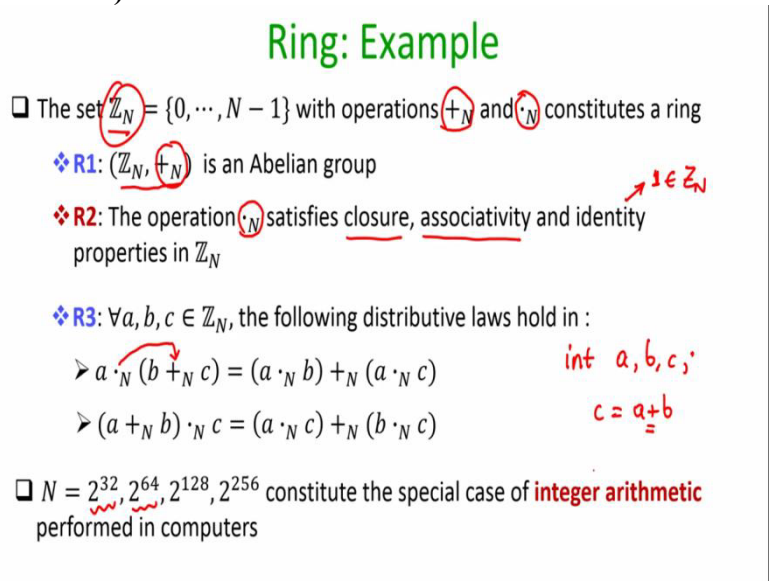
We need closure property, we need plus operation to be associative, we require the presence of some special identity element which we denote by this '0' such that if you perform the plus operation with element a you should get back the element a for every element a from the set $\mathbb{R}$. We need the presence of additive inverse and we need the operation plus to be commutative. So, this is the first requirement from the set $\mathbb{R}$ and operation + namely it has to satisfy the properties of an abelian group.

The second axiom that set $\mathbb{R}$ should satisfy is the following: we require that the dot operation should satisfy the closure property namely, you take any pair of elements (a, b) from your set $\mathbb{R}$ and you perform the dot operation you should get back again an element from the same set $\mathbb{R}$. We require the dot operation to be associative. That means, it does not matter in what order you perform the dot operation on 3 elements, you should get back the same answer.

And we demand the presence of an identity element with respect to the dot operation. So, I denote the identity element if at all it exists by this element 1. I again stress that in abstract algebra, this is just a notation this does not mean numeric 1 or integer 1. So, this element 1 should satisfy the property that if you perform the dot operation with 1 and any group element; any element from the set $\mathbb{R}$ you should get back the same element a. So, this is the second ring axiom and the third property or the so called third ring axiom that needs to be satisfied is that your dot operation should be distributive over the plus. Namely, if you take any triplet of elements from the set $\mathbb{R}$ called them as a b c, then it does not matter whether you first perform the plus operation on b and c. So, you will get one element from the set $\mathbb{R}$ because the set operation plus will satisfy the closure property and if you now perform the dot operation on the result and a then the result should be the same as if, if you perform the dot operation involving a and b, you perform the dot operation involving a and c and then if you perform the final plus operation and we need the distributive property to hold both in the left sense as well as right sense.

And namely, we need to satisfy both the left distributive property as well as the right distributive property. So, the distributive property that I had just discussed is called as the left distributive property. We need the dot to be distributed over plus even if dot is after the plus. So, if all these 3 properties R1 R2 R3 are satisfied, then we will say that the set $\mathbb{R}$ along with the abstract operations plus and dot constitutes a Ring $(\mathbb{R}, +, \cdot)$.

(Refer Slide Time: 05:08)



So, let us see some examples for ring. So, recall our set $\mathbb{Z}_N$ is the set of integers 0 to N - 1 and suppose I take 2 operations here: plus operation is the addition modulo N $(+_N)$ and my multiplication operation is multiplication modulo N $(\cdot_N)$ and my claim is that with respect to these 2 operations, my set $\mathbb{Z}_N$ satisfies all the ring axioms. So, it is easy to verify that indeed the collection 0 to N - 1 along with the operation addition modulo N constitutes an abelian group we had already proved in our earlier discussion.

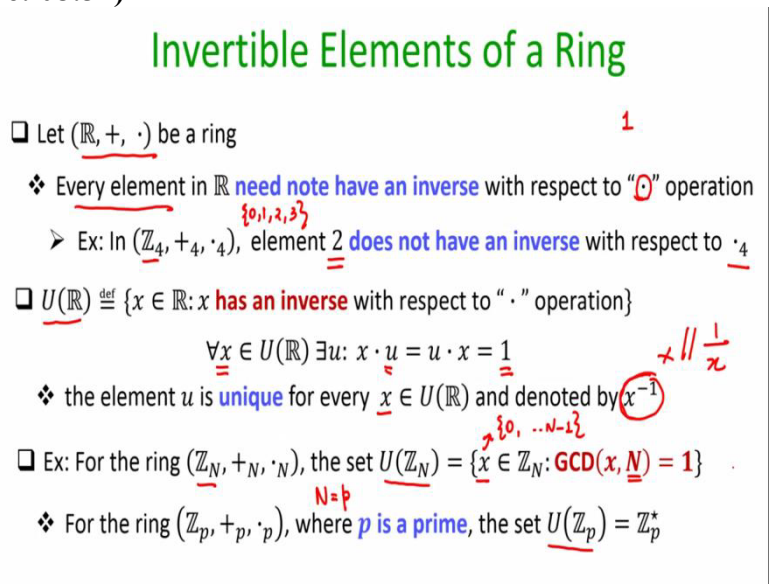
And it is also easy to verify that if we consider the multiplication modulo N operation then it satisfies the closure property, the operation is associative and identity element is actually the numeric 1, integer 1 which is actually present in your set $\mathbb{Z}_N$. If you multiply 1 with any element from the set $\mathbb{Z}_N$ and then take modulo N you will get back the same element and it is easy to that the distributive property is indeed satisfied.

That means you can distribute this multiplication module N over plus modulo N both in the left sense as well as in the right sense. So, that is why all my ring axioms are satisfied and this ring $\mathbb{Z}_N$ with respect to the operation plus modulo N and multiplication modulo N is a very

special ring. Because typically in our computers in our programming in our computers we have registers we have either 32 bit registers, 64 bit registers or even if you have powerful processor then you have 128 bit registers, 256 bit registers, where you can save values using either 32 bit or 64 bits or 128 bits or 256 bits and so on and if you add any two 32 bit number, then again you get back a 32 bit answer and so on. So, if you consider say for instance your C programming language; in older version the integers used to have 32 bit representation and you add any 2 integer values; again you used to get back an integer value which can be represented by 32 bits.

So, implicitly there the operation that we are performing are addition module N and multiplication module N; namely if I say int a, b, c and if I perform c = a + b then internally I am actually performing a + b modulo N where N is 2^{32} if the integers a b c are represented by 32 bits whereas my N will be 2^{64} if my a b c are represented by 64 bits and so on. So, this is a very useful ring used because our internal processors in computers perform operation with respect to addition modulo N and multiplication modulo N.

(Refer Slide Time: 08:31)



So, the next thing that we want to discuss is the invertible elements of a ring. So, imagine you are given a ring and if you see closely the ring axioms, it turns out that it is not the case that every element should have a multiplicative inverse. Again, without loss of generality, I am considering this dot operation in the multiplicative sense. But again and again I stress that this is not the usual integer multiplication.

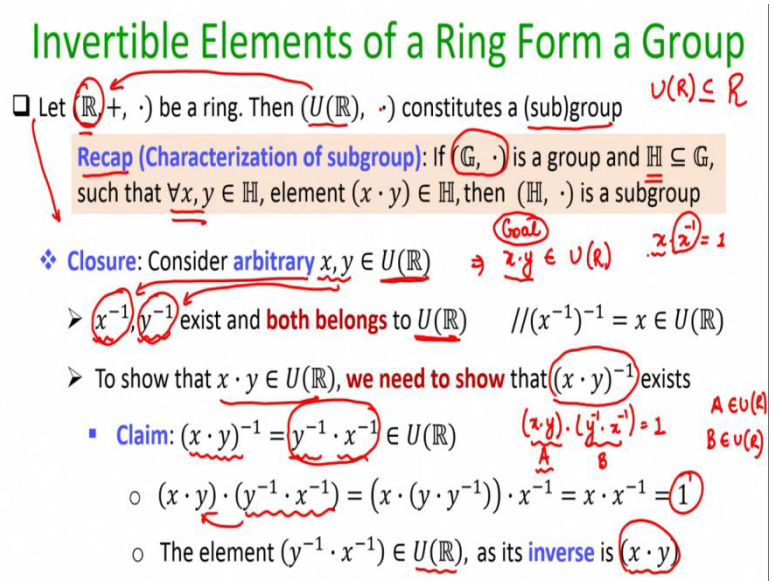
So, if you see the ring axioms it is not necessary that every element have a multiplicative inverse, you need the presence of identity element 1, but it is not necessary that every element has a multiplicative inverse. So, for instance, if I take this ring, $\mathbb{Z}_4$, where my $\mathbb{Z}_4$ is the collection 0, 1, 2 and 3, then there are several elements which do not have any inverse with respect to the multiplication modulo 4 operation.

So, for instance the element 2 does not have any inverse. You multiply 2 with 0, you get 0. You multiply 2 with 1 and then take mod 4 you get 2, you multiply 2 with 2 and take mod 4 you get 0 and so on, you never get a result which is 1. So, the element 2 does not have multiplicative inverse here. So, now what we are going to do is we are going to define a special set which I call as $U(\mathbb{R})$ and $U(\mathbb{R})$ is basically the collection of all invertible elements with respect to the multiplication operation.

So, it is the collection of all elements x from your set $\mathbb{R}$ for which you have the guarantee of presence of some element u such that if you perform the dot operation with x involving x and u, you get back the multiplicative identity element and if you have an element x present in the set $U(\mathbb{R})$ then the corresponding multiplicative inverse we denote by this notation (x^{-1}) again I stress that this does not mean, that I am talking about 1/x this is just a representation; representation of the unique value u which when multiplied with x gives you the identity element 1. So, let us see some examples of the set $U(\mathbb{R})$; if I again consider the same ring $\mathbb{Z}_N$ then we know that the invertible elements of the set $\mathbb{Z}_N$ are those elements x in the range 0 to N - 1 which are co-prime to N.

Because we have proved that multiplicative inverse with respect to multiplication modulo N of a number x exists if and only if x is co-prime to N, that means, if I consider my N to be a prime number p then this set you $U(\mathbb{Z}_p)$ will be nothing but all the elements except 0 in the range 0 to p - 1 because 0 would not be co-prime to p.

(Refer Slide Time: 12:06)



So, now we can prove some interesting properties for this set $U(\mathbb{R})$. We can prove that if you are given a parent ring and parent ring in the sense that my set U is defined with respect to this ring $\mathbb{R}$ then if I consider the set of all invertible elements from this ring with respect to the multiplication operation then that collection constitutes a group and we are going to prove this.

So it constitutes a group in the sense that it will be actually a subgroup of your set $\mathbb{R}$. Because your set $U(\mathbb{R})$ will be a subset of your bigger set $\mathbb{R}$. So, basically what we want to prove here is that the collection of invertible elements with respect to the dot operation constitutes a subgroup of your original ring $\mathbb{R}$ and for this what we have to do is we have to recap the characterization for a subgroup which we had seen in our earlier discussion.

So, recall we proved that if you are considering a group, parent group and dot operation and if you take any subset H of that parent group then it will constitute a subgroup with respect to the dot operation if the closure property is satisfied, if you just prove that the closure property is satisfied that automatically ensures that all other properties are also satisfied. So, what we have to prove is the following. To prove this theorem that the collection of all invertible elements of an abstract ring constitutes a subgroup with respect to the dot operation, we just have to prove that your closure property is satisfied in this collection $U(\mathbb{R})$. So, for proving the closure property we have to show the following : you take any 2 elements x and y from this set $U(\mathbb{R})$, the element $x \cdot y$ is also a member of $U(\mathbb{R})$ that is what we have to prove this is our goal.

And recall our definition of $U(\mathbb{R})$ is that an element is considered to be present in $U(\mathbb{R})$ if it is invertible. So, basically we have to show that x ·y is also invertible. So, the first thing to observe is that since I am considering that element x as well as element y are invertible let me denote the multiplicative inverse by x inverse and y inverse : x^{-1} and y^{-1} respectively.

Now, my claim here is that the elements x^{-1} and y^{-1} they also individually belong to this set $U(\mathbb{R})$ that means, I can say that element x^{-1} itself is invertible and I can say that element y^{-1} itself is invertible this is because, the definition of inverse says that if x multiplied with x^{-1} gives you 1 I can interpret it as if that x inverse. So, here this x^{-1} is considered as the inverse of x.

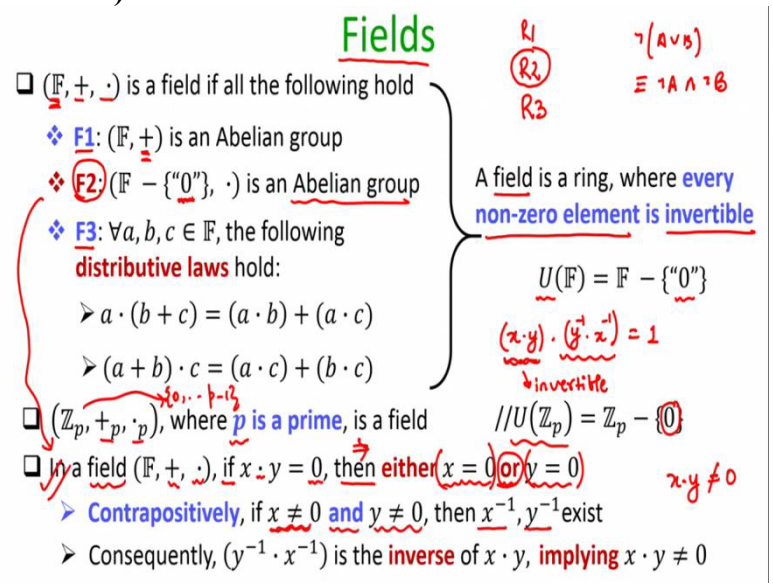
I can also consider that x is the inverse of x^{-1}. This is because if b is the inverse of a then I can consider a as the inverse of b and vice versa. So, that is why I can say that since x is invertible and I have the guarantee of presence of x^{-1}; similarly if y is invertible I have the guarantee that y^{-1} is present, I can say that both these elements are themselves individually invertible.

And hence they also belong to the set $U(\mathbb{R})$. Now, what we have to show remember our goal is to show that x ·y is also invertible because we have to show that it belongs to the set $U(\mathbb{R})$ that means, I have to show that there exists some element x $\cdot y^{-1}$ which when multiplied with x ·y will give you the identity element and my claim is that the inverse of x ·y is nothing but y^{-1} $\cdot x^{-1}$.

This is because if you multiply y^{-1} $\cdot x^{-1}$ with x ·y and then if you use the associative law and then rearrange the terms you get the identity element. So, that shows that this element is the inverse of this element and the second thing that we have to prove is that this element y^{-1} $\cdot x^{-1}$ is also an element of $U(\mathbb{R})$ and that simply comes from the fact that we have proved that it is the inverse of x ·y.

So, since we have so what we are basically saying here is that since I have shown that; call this element (x ·y) as A and call this element (y^{-1} $\cdot x^{-1}$) as B. So, what we have shown here is that A is the inverse of B and B is the inverse of A that means, I can say that both A is an element of $U(\mathbb{R})$ because it is invertible and I can say that B is also an element of $U(\mathbb{R})$ because it is invertible and that is what we wanted to show here.

(Refer Slide Time: 18:29)



So now what we are going to do is we are going to extend our definition of ring to another interesting algebraic structure which we called as a field. So a field is an algebraic structure it is a set of values and there are 2 operations; 2 abstract operations plus and dot, which are defined over the elements of this set $\mathbb{F}$ and we will say that all together this collection $\mathbb{F}$ along with the operation $+$ and $\cdot$ is a field if the field axioms are satisfied.

So, what are the field axioms: the axiom number 1 is that the set $\mathbb{F}$ along with the plus operation should constitute an abelian group. The second property that we demand here is the following if I exclude the additive inverse and see I have written down here 0 in quote and unquote - it is not integer 0 it is just a representation for denoting the identity element with respect to the plus operation.

So, what I am saying here is that if I exclude the additive identity element, then all the remaining elements of the set $\mathbb{F}$, together with the dot operation satisfies the properties of an abelian group and the third property the third field axiom that needs to be satisfied is that your dot should be distributive over plus. So if you see; closely these axioms F1 F2 F3 and compare it with your ring axioms R1 R2 R3.

You can easily identify that your field is a special type of a ring, where every non-zero element is invertible with respect to the multiplication operation. So remember recall in axiom number R2 is when we considered a ring axioms, we never demanded that with respect to dot operation, all the elements should be invertible and so on, no such demand was there,

but now, I am putting a demand that, I am giving you the liberty, I am giving you the freedom to exclude the 0 element 0 element in the sense the additive identity element; all other remaining elements should have multiplicative inverse and if that is the case then I can say that my ring is a field. So in other words, with respect to the set U that we have defined just now, so remember U is a collection of all elements which are invertible with respect to your dot operation. So I will say that my set $\mathbb{F}$ is a field if all the elements except the 0 elements are invertible, namely, the set $U(\mathbb{F})$ is entire set $\mathbb{F}$ excluding the elements 0. So now it is easy to verify that if I consider a prime modulus then the set of integers, 0 to p - 1, which is nothing but the set $\mathbb{Z}_p$ along with the operation addition modulo p and multiplication modulo p satisfies the field axioms.

Because the set of all invertible elements in this collection is the entire collection excluding the numerical 0 because here the numerical 0 is actually your additive identity. Now an interesting property in the field is the following. If I am given a field with an abstract plus operation and an abstract dot operation and if it is given that the result of $x \cdot y$ is 0 again I stress this is the abstract dot and this is the abstract 0.

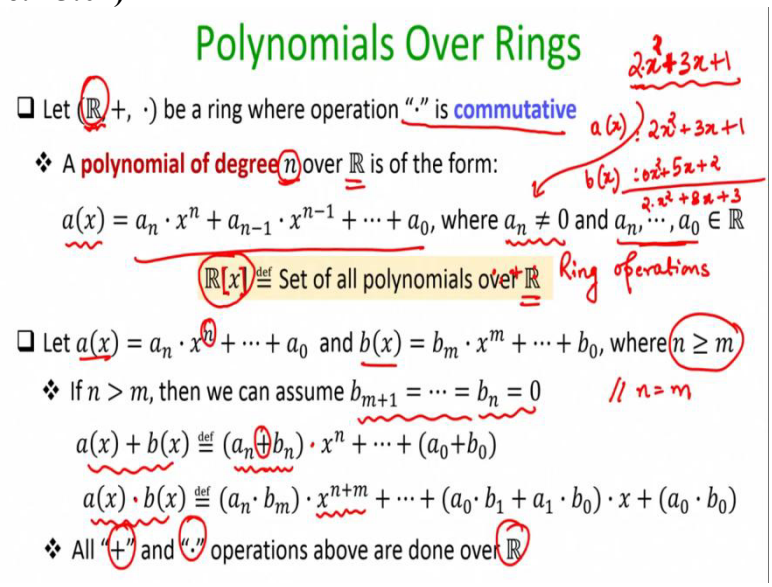
Do not consider it as to be the usual multiplication and numerical 0. So, if $x \cdot y$ is 0, then we can safely conclude that it is either the case that your element x is 0 or the element y is 0 that means it will never happen that you take 2 non-zero elements and if you perform the dot operation you get a 0 element that would not happen in a field I stress this is true for a field you can verify this may not be the case for a ring.

So, how do we prove this. So this is an if-then statement, your if condition is this and this is if-then part. So, I will give up proof by contrapositive. So contrapositively; what will be the contrapositive here since an OR is involved here and you have $x = 0$ OR $y = 0$, if I put negation in the in front of this $x = 0$ OR $y = 0$, I get $x \neq 0$ and OR gets converted into AND because remember logically if you take negation of a OR b, then that is logically equivalent to negation of a AND negation of b. So contrapositively I want to show here that if $x \neq 0$ and if $y \neq 0$, then $x \cdot y \neq 0$. That is what I want to show here. So, let us prove that so since $x \neq 0$ and as per the field axioms, every non-zero element has a multiplicative inverse. So let me denote that multiplicative inverse by x^{-1}. Similarly, y is non-zero. So, it will have a multiplicative inverse let me denote it by y^{-1}. Now, as we had proved earlier, that, if you

multiply $x \cdot y$ with $y^{-1} \cdot x^{-1}$ you will get back the identity element. That means, I can consider the product of y^{-1} and x^{-1} to be the inverse of the element $x \cdot y$.

That means, I can say that the element $x \cdot y$ is invertible and if the element $x \cdot y$ is invertible, then from the field axiom F2 we can conclude that element $x \cdot y$ was not a 0 element and that shows that whatever we claimed here is correct.

(Refer Slide Time: 25:07)



Now, the next thing that we want to discuss here is the polynomials over rings, which is a very important concept used in computer science. So, imagine you are given a ring with some abstract plus an abstract dot operation and imagine that your dot operation is commutative. Now, if I want to define a polynomial of degree n over this ring $\mathbb{R}$ it will be of this form $a(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_0$ and this is very much similar to the notion of polynomials that we are familiar with.

We are very much familiar with polynomial over integers or real numbers and so on; if I consider a polynomial of the form $2x^2 + 3x + 1$ then I say that this is a polynomial of degree 2 because the highest power is x^2 with coefficient 2 we are more or less trying to define the same concept where in the case of usual polynomials the plus operation is the integer plus operation and 2 times x^2 should be treated as 2 multiplied with x^2.

So, we are just extending those plus and dot operation with respect to an abstract ring, that is what is the generalisation here. So, we are basically generalising the existing definition of polynomials that we are aware of with over integers to any abstract ring. So, here we have

saying that the polynomial will have the form $a_n \cdot x^n$, $a_{n-1} \cdot x^{n-1}$ and so on and everything added together.

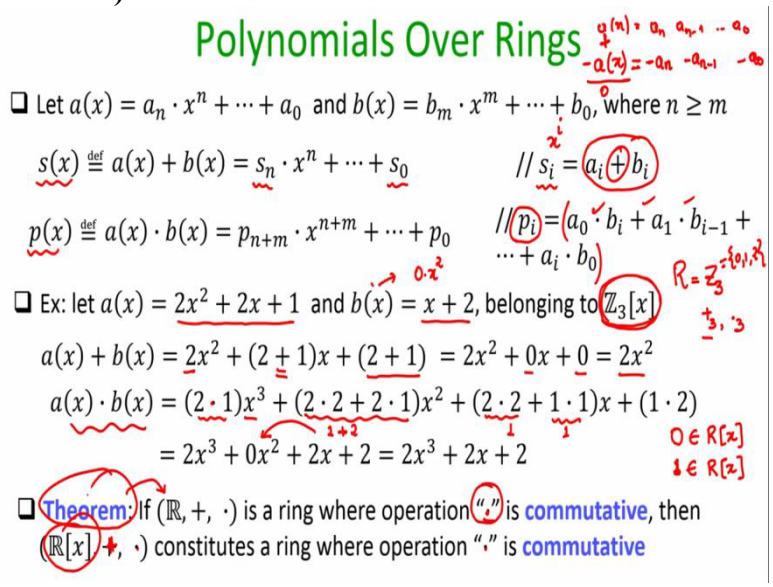
Since my degree is n my restriction will be that the coefficient a_n will be non-zero all other coefficients are allowed to be 0 and each of these coefficients are from your set $\mathbb{R}$ and your plus operation and your dot operation are the ring operations; they are not integer plus or integer dot operations. So, now, if I consider the set of all polynomials of various degrees that are possible over this ring $\mathbb{R}$, I denote that infinite set by this notation $\mathbb{R}[x]$. So, now, my x is no longer in regular parenthesis they are now within square parenthesis. So, this is just a notation that you are taking polynomials of degree n = 0 followed by all polynomials of degree n = 1 followed by all polynomials of degree n = 2 and so on. So, it is easy to see that this is an infinite set because I am taking all possible polynomials of various degrees which is a never ending process.

Now, let us see how we define the operations of polynomials over ring. So, we know how to add 2 integer polynomials. So, if I am given 2 polynomials, say a polynomial $2x^2 + 3x + 1$ and say another polynomial $5x + 2$ say this is my a(x) polynomial this is my b(x) polynomial the usual way to add these 2 polynomials is the following since there is no term is involving x^2 in b(x), I can imagine that it has some 0 times x^2 present implicitly, so, that I can now safely assume that both a(x) and b(x) are of the same degrees and then I can say that you position wise add the various coefficients, so, 2 + 0 will give you 2, 2 x^2 then the coefficient of x will be 5 + 3 and the constant coefficient will be 2 + 1 = 3, that is the usual way of performing addition of integer polynomials, we are now extending the same definition to polynomials over abstract rings.

So, imagine you are given 2 abstract polynomials arbitrary polynomials over a ring and for simplicity and without loss of generality assume that the degree n is greater than equal to m. Now, if n is not equal to m, then as I have done for the case of integer polynomials, I can substitute higher order coefficients in the b polynomial with 0 and then I can safely assume that n = m then the way I perform the addition of these two ring polynomials is that, I component wise take the coefficients of various powers of x from the a polynomial b polynomial and I add them where my addition will be now, the addition operation over the ring and of course, these dot operations are the dot operation over the ring in the same way, I extend my notion of multiplication of 2 integer polynomials to multiplication of 2 ring

polynomials. So, again what I do here is if I take the product of 2 polynomials of degree n and m respectively, the polynomial will be now of degree n + m and these will be the various coefficients and again and again I stress that all this plus and dot operations are the dot and plus operations over my ring R, they are not the usual or traditional plus and dot operations.

(Refer Slide Time: 30:54)



So, if I denote s(x) to be some polynomial then let us denote the coefficients of this sum polynomial to be s_n, s_{n-1} up to s_0 and it turns out that the coefficient of x^i which is denoted by s_i will be nothing but summation of the coefficient of x^i in the a polynomial and coefficient of x^i in the b polynomial where the plus operation is over the ring.

And in the same way, if I denote p(x) as the product polynomial and if I denote the coefficients of the product polynomial as p_{n+m}, p_{n+m-1} up to p_0 and it turns out that the coefficient of x^i will be this expression $(a_0 \cdot b_i + a_1 \cdot b_{i-1} + \cdots + a_i \cdot b_0)$ where all the dot and plus operations are over the ring. So, let me demonstrate for you, whatever we have discussed with some example here.

So, imagine I consider my ring to be $\mathbb{Z}_3$ and my plus operation is addition modulo 3 and my multiplication operation is multiplication modulo 3 and $\mathbb{Z}_3$ means the elements 0, 1 and 2. Now, I am taking 2 arbitrary polynomials. One polynomial is of degree 2 ($2x^2 + 2x + 1$) and another polynomial of degree 1 (x + 2) belonging to this set $\mathbb{Z}_3[x]$. Remember $\mathbb{Z}_3[x]$ denotes the set of all possible polynomials of various degrees, where the coefficients are from the set 0, 1, 2 and where my plus and dot operations are addition modulo 3 and multiplication modulo 3. So, now let us see the result ofsummation of these 2 polynomials. So if I sum these

2 polynomials so you can imagine that in b(x) there is no term with x^2, so, you can implicitly assume that you have 0 times x^2 present. So, the coefficient of x^2 and the sum polynomial will be 2 + 0 modulo 3.

Because the; plus operation is plus modulo 3. So, 2 + 0 modulo 3 will give you 2. Now, the coefficient of x will be 2 + 1 but now this is not the usual plus this is now the plus modulo 3. So, that is why the coefficient of x will now vanish and in the same way, the constant coefficient will be 2 + 1 but now this is 2 + 1 modulo 3 which will become 0. So, you can now see that the summation of these 2 polynomials will be $2x^2$.

Whereas if I multiply these 2 polynomials then the coefficient of x^3 will be this 2, why x^3? So, this polynomial is a(x) is of degree 2 and b(x) is a polynomial of degree 1, so, the resultant product polynomial will have degree 3 at most. So, the coefficients of various powers will be this; now 2 times 1 and multiplication here is multiplication modulo 3, so 2 times 1 modulo 3 will be 2.

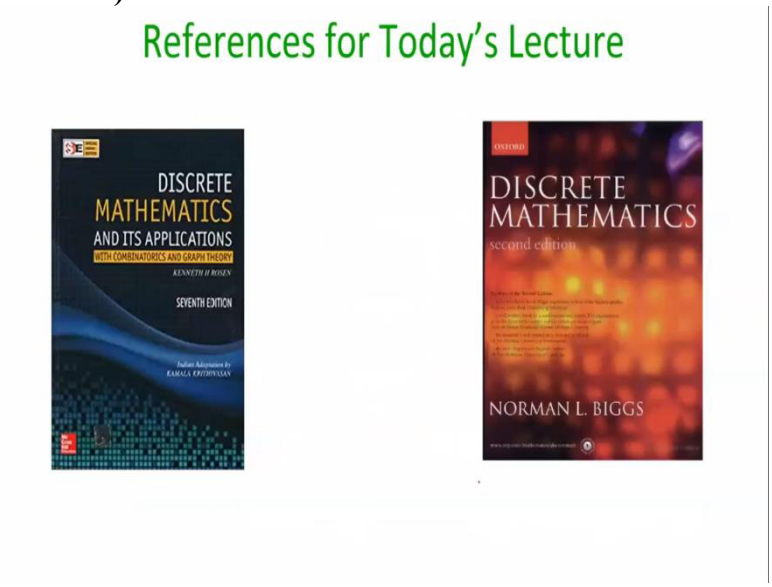
But now if you see this term, this is 2 into 2 = 4 and 4 modulo 3 will be 1 plus 2 into 1 will be 2 and 2 + 1 modulo 3 will become 0 so that is why the coefficient of x^2 will become 0. In the same way this 2 into 2 will be treated as 1, 1 into 1 will be treated as 1 and 1 + 1 will be 2 and so on. So now we can prove here that if my dot operation over the ring is commutative, then if I consider the set of all polynomials of various degrees where the coefficients of the polynomial are from this ring $\mathbb{R}$ then even with the dot operation, namely, the product of the polynomials, if I consider this operation, then it will satisfy the; and of course, the summation of 2 polynomials the way I have defined here. So, basically what I am saying here is that if I consider the set of all possible polynomials over the ring. Then along with the addition of the polynomials and multiplication of the polynomials the overall algebraic structure will satisfy your ring axioms provided the dot operation in your ring $\mathbb{R}$ is commutative.

And this can be proved very easily, you can at least see that we have already seen an example here, but it is not very difficult to prove it. We can of course prove the closure property, associative property with respect to the polynomial addition. we can prove the closure property, associative property with respect to the multiplication of the polynomials the constant polynomial 0, which belongs to $\mathbb{R}[x]$ will be treated as an additive identity because you add the 0 polynomial to any polynomial you again get back the same polynomial;

whereas the polynomial 1 the constant polynomial 1; will be treated as the multiplicative identity. And if you have a polynomial a(x) say with coefficients a_n, a_{n-1} up to a_0 then it is easy to see that, I can find out a corresponding –a(x) polynomial and –a(x) polynomial will be nothing but will have coefficients $-a_n$ and $-a_{n-1}$ and up to $-a_0$ where the minus elements are the additive inverse elements with respect to my ring then if I perform the addition of these 2 polynomials, I will get a constant polynomial namely the 0 polynomial. Similarly, I can show that my plus operation is distributive over the dot operation.

Namely the addition of the polynomial is distributive over the multiplication of the polynomials and so on, I am leaving the proof of this theorem as an exercise for you, but it is very easy to prove.

(Refer Slide Time: 37:41)



So, that brings me to the end of today's lecture these are the references used. Just to conclude, in today's lecture we saw the definition of fields. rings and we also discussed about polynomials over rings. Thank you.