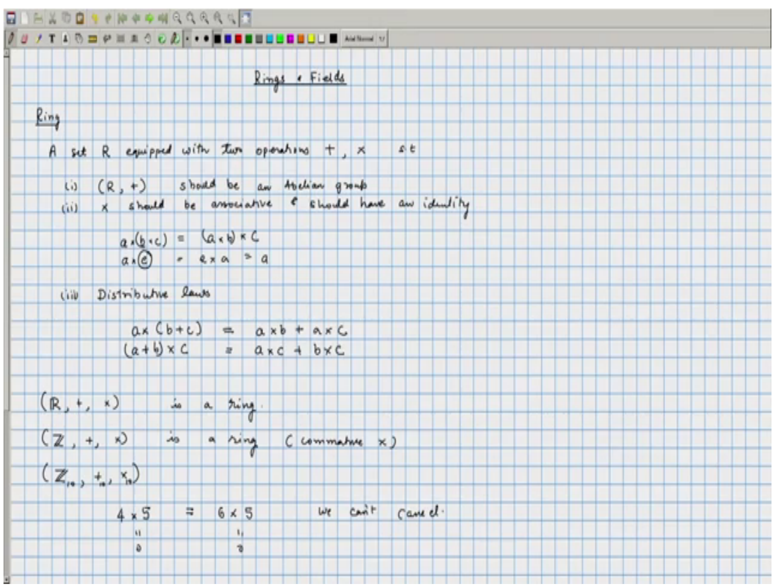
Discrete Mathematics

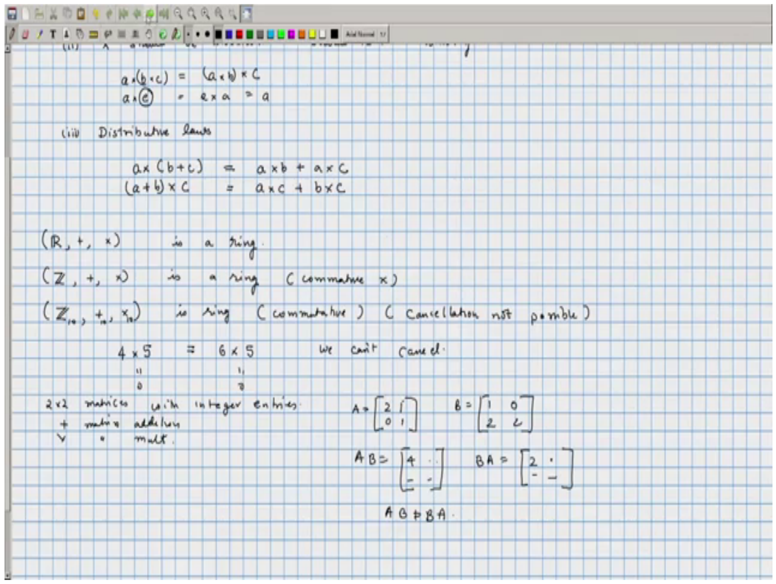
Professor Sajith Gopalan
Department of Computer Science and Engineering
Indian Institute of Technology, Guwahati

Lecture 42

In this lecture we will learn about 2 new algebraic structures namely rings and fields. We had learned about the groups, one way in which rings and fields are different from groups is, while we were talking about the groups there was only one operation but when we talk about rings and fields there are two operations and we will call these operations as addition and multiplication operations. So let us formally understand what is a ring.

(Refer Slide Time: 1:01)





So there is a set, so ring as a set R, equipped with 2 operations, let us call is as the addition and the multiplication operations. And these operations have to satisfy some properties. The first property is, if you just consider the set, with the addition operation, this should be an abelian group and if you look at the operation of multiplication then that should be associative and there should be a multiplicative identity.

So that should mean if you have elements a, b and c, a times b into c should be equal to a into b into c and there should exist an element e which can act as the multiplicative identity. So a times e should be equal to e times a should be equal to a. There should exists an element of this kind, okay.

The third property is how these, these operations interact with each other? So that is the distributive laws, namely if you multiply a with b plus c the product should be equal to a times b plus a time c for every a, b and c. And if you have a plus b into c, so no matter whether you multiply on left or whether you multiply on right, the distributive law holds. So this will be equal to a into c plus b into c. So if you have a set equipped with 2 operations which behaves in this manner, then that is called as a ring.

Let us look at some key differences or key some non-requirements, this multiplication need not be an invertible operation, when we are look into addition for every element of the group, there is an element which can act as the additive inverse, the multiplicative inverses need not be present. Not just that even cancellation laws need in hold, okay we will see examples of all those.

So that is the way in which this is the general ring is different from let us say if you consider the ring of real numbers.

So the ring of real numbers, is many additional properties that, that we do not insist for a general ring. So let us see some examples, if you just take the set of real numbers with usual addition and the usual multiplication then clearly under addition real numbers form an abelian group and the multiplication has the distributive properties and that is associative and one can serve as the identity, so this is the ring.

Now let us look at the set of integers under the usual addition and multiplication, this is also a ring. But here you can see that there is mean under multiplication inverses is not defined. For example, if you take the element 9, there is no multiplicative inverse there is no element which you can multiply with 9 to get a 1. But this is a commutative ring, in the sense the multiplication operation is commutative.

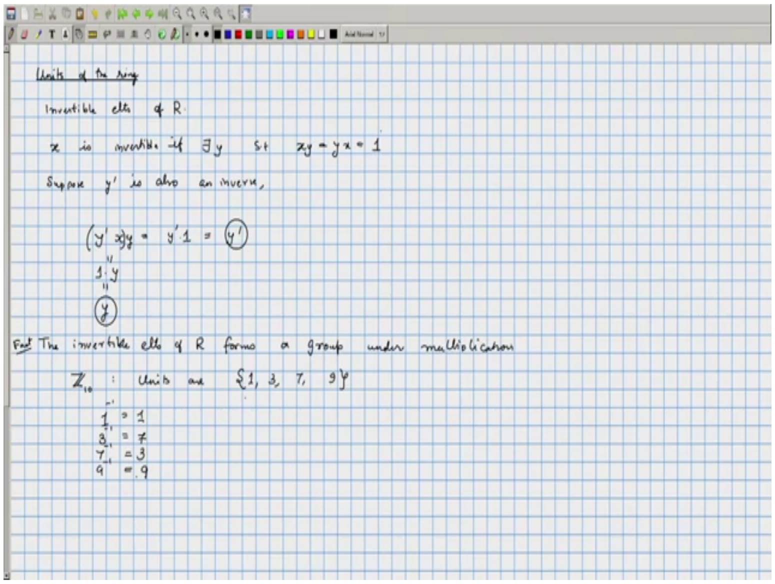
Okay same applies for R but Z is a commutative ring but it is the non-zero element, if you look at it, not all of them are invertible, only invertible elements in this ring are the plus 1 and the minus 1. Let us look at another ring, if you look at the set of numbers, modulo 10, so the operations are mod 10 operations. So now the (multipli) the addition is mod 10 (multiplication) addition and the multiplication is mod 10 multiplication.

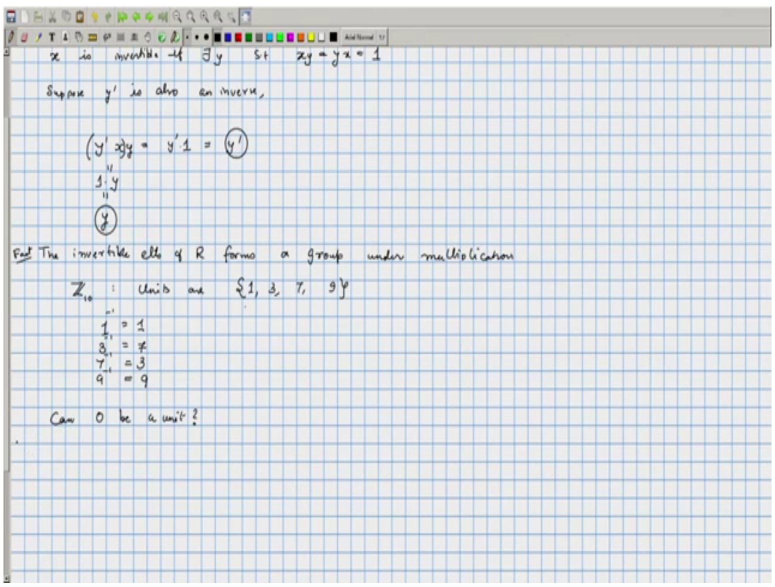
Now if you look at this ring, clearly this is a I mean you can verify that it will be a ring because addition is associative and the multiplication, there is a multiplicative identity and the multiplication is associative and the distributive laws holds. But now you can see that even cancellation laws does not really work. For example, if you have let us say 4 into 5, so that will be 20, that is equal to 0, is equal to let us say 6 into 5.

Both are 0 but we just cannot cancel off 5 and say that 4 equal 6 but this is again a commutative ring. But if you now take the set of matrices, if you look at matrices, so let say 2 cross 2 matrices where the entries are in are from the ring of integers and the addition is the usual addition and the multiplication is the matrix multiplication. Clearly this is not a commutative operation.

For example, if you take, say the matrix A is equal to 2 1 0 1 and B is equal to 1 0 2 2 okay, so AB if you compute the first element or the 1-1 element will be 2 into 1, 1 into 2, it will be 4 and the other elements would be something, whereas if you compute BA that is going to be 1 into 2 and 0 into 0, so this is going to start with 2. So clearly AB is not equal to BA. So matrix multiplication is not commutative and therefore V is matrices 2 cross 2 matrices with integers entries if you take those matrices they do form a ring but it does not have many other properties that we would have in other rings like it is not commutative and there is no cancellation may or may not be possible and okay so this is an example of a non-commutative ring.

(Refer Slide Time: 9:20)





Now let us further explore the rings, so we will first define what are called as a units of the ring. Since we have a multiplication operation and we have multiplicative identity, we could consider all the elements that are invertible. So units are nothing but invertible elements of the ring. Okay for example, the first that we should ask is, if an element is invertible, is the inverse unique? Okay so what do we mean by invertible elements?

So x is invertible, if there exist y such that xy is equal to yx is equal to 1 where 1 is the identity, we know that in the rings there is an identity. Okay now if there is one such x, will it be unique? It will be unique because suppose there is a y prime, suppose there is a y prime with similar properties, for an invertible element x, suppose there is a y prime. So if you consider xy equals 1 and multiply both side of this equation with y prime, okay so y prime into 1 this is equal to y prime and we can use associativity here and say that y prime times x that is going to be identity because y prime was an inverse.

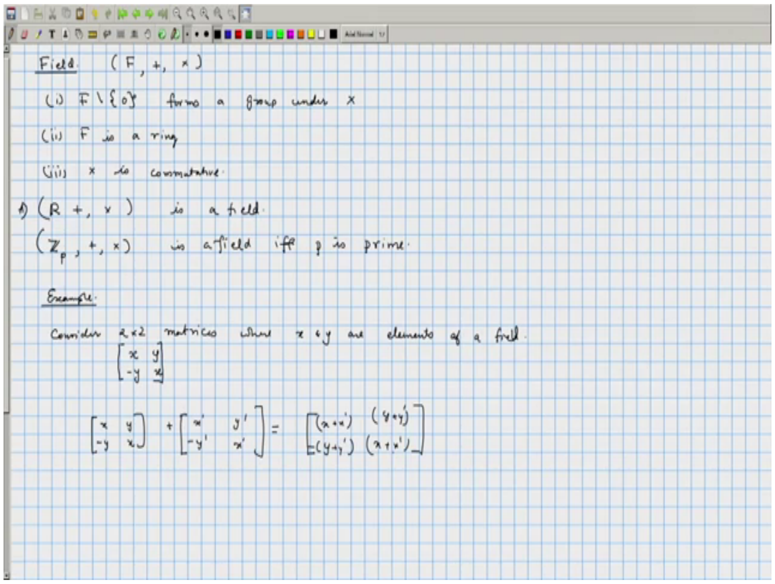
So this will be 1 into y and that is going to be equal to y because 1 is the identity, identity multiplied by any element you see 1. So this would imply that y is equal to y prime, so if an element is invertible, its inverse is unique. Now let us collect all the invertible elements together okay that is, they are going to be called as units and you can verify this, the invertible elements of R forms a group under multiplication.

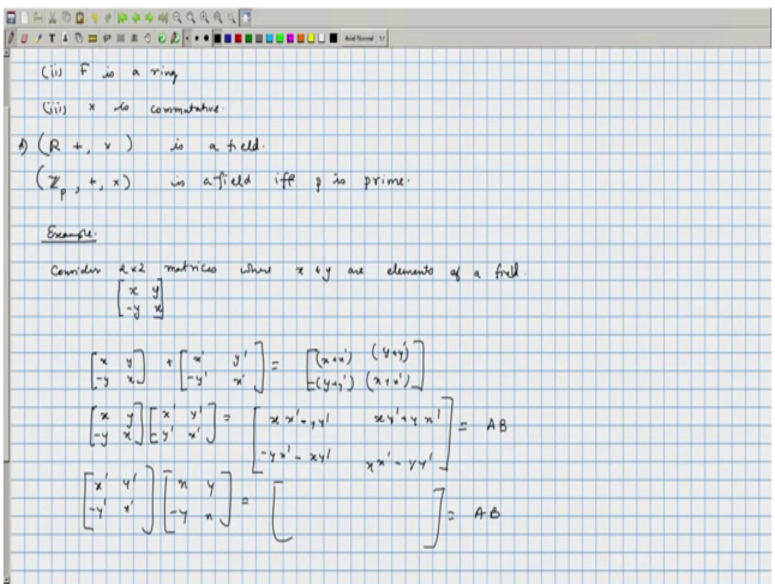
We have already seen this when we were looking at certain groups, if we were looking at Z10, that is a ring and invertible elements are namely 1, 3, 7 and 9. These were the numbers which are relatively prime to 10 and if take those elements, those alone are the invertible elements and you can check that the inverse of 1 is going to be itself, 3 inverse is 7 because 3 into 7 is 1 and 7 inverse is 3 and 9 inverse is 9 itself because 9 into 9 is 1.

Now we can define, what is a field? So we will rule out the trivial cases by saying that whenever we are thinking about rings or fields, the additive identity and the multiplicative identity they are going to be separate, they are going to be, they are going to be, they are 2 different distinct things. Okay soo there will be at least 2 elements in all the rings that we are looking at. So can 0 be a unit? Can 0 be inverted?

Okay so you can verify that this cannot be the case and therefore in any ring the best that we can hope for is the non-zero elements are invertible and such a ring with the additional property that it that the multiplication is commutative is called as a field.

(Refer Slide Time: 13:18)





Okay so let us defined what a field is, so again we will denote the set by F and there are 2 operations namely plus and multiplication. So this is a field if F minus this 0 element forms a group under multiplication and ofcourse F has to be a ring for these operations and then the third requirement is multiplication is commutative.

Okay so if these conditions are satisfied then that is called as a field. So we will see some examples of field, if you look at the real numbers under the usual addition and multiplication, this is a field. Because if you take a non-zero elements, each of them is invertible and they form a group under multiplication and ofcourse multiplication is commutative.

We will see far more interesting fields when we are looking at finite cases, if we look at let us say ZP under mod P addition and multiplication this is also a field if and only if P is prime. Okay now group is here we have checked that if you consider elements modulo, multiplication modulo P, the elements 1 to P minus 1 will form a group when P is a prime number and if it not a prime number, they will not form a group.

So this automatically means that we will have fields of size P for any prime. Can there be a field of size 6? Can there be a field of size 9 and so on? These are important questions and we will see the answers to some of these questions. So let us first look at some examples of fields, so let us look at matrices. Okay, so let us consider 2 cross 2 matrices which are skew symmetric, we have a very specific form for these, let us say they are of the form x y and then minus y x.

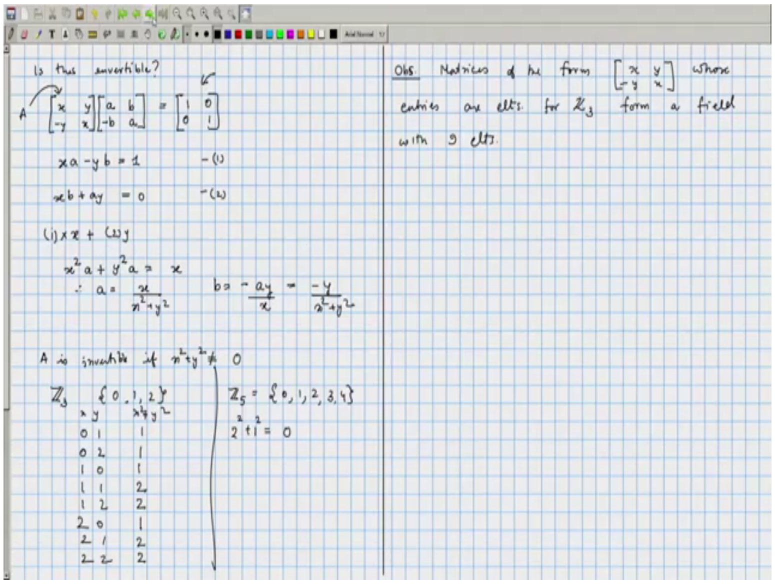
So look at 2 cross 2 matrices of this form, where x and y these are elements of a field, okay. Do these matrices, these collection of matrices form a field? Clearly they form a ring because if you have a matrix x y minus y x and if you add it to another matrix of that kind x prime, y prime minus y prime x prime, what is get is another 2 cross 2 matrix which is of the same form.

So x plus x prime will appear on the diagonal and y plus y prime and its negative will appear on the off diagonal. Okay so closure property is there and you can verify that under addition these do form a group. The multiplication is also well defined and you can see that the multiplication will in fact be commutative, if you just consider the matrices of this kind, okay so let just say its compute x y, let us take this matrix and find its product with another such matrix.

So the diagonal entries are going to be x-x prime plus y-y prime, so the product is going to be minus y x prime minus x y prime which is the negative of the 1, 2 and 3. And the diagonal elements are going to be x-x prime minus y-y prime. Then you can see that the result is symmetric in x and x prime or y and y prime because if you just change, I mean if you compute them product of x y prime minus y prime x prime with x y minus y x, that is going to be exactly same as, so if you call this as AB, this is also going to be equal to AB, okay.

So AB equal to BA and therefore these matrices when you multiply them out, they are I mean the multiplication is commutative.

(Refer Slide Time: 18:48)



But is invertible is the question. So that answer is going to depend on the particular field from which are choosing, okay so if you have a matrix x y minus y x, if it is invertible, let us first try and do the symbolic inversion of this matrix. So if you have another matrix which inverts then it should be other formed a, b minus b, a and this product should be equal to 1, 0, 0, 1 because this is going to be the multiplicative identity nothing else can act as the multiplicative identity.

So when will matrices be invertible? Okay so here the requirement is x a, the product would be xa minus yb that should be equal to 1, that is one of the requirements and the other requirement will be that xb plus ay should be equal to 0. We can solve these simultaneous equations for a and b and so if you call this as equation 1 and this is equation 2, we just multiply 1 into x plus 2 into y.

What we will get is x square a plus y square a is equal to x and therefore a is equal to x by x square plus y square and similarly you can show that b is equal to minus a y by x and that is going to be minus y by x square plus y square okay and therefore we can carry out this operation as long as x square plus y square is not equal to 0. Okay so these are going to be invertible if, so the matrix A, if we consider this as a matrix A, A is invertible if x square plus y square is not equal to 0 okay.

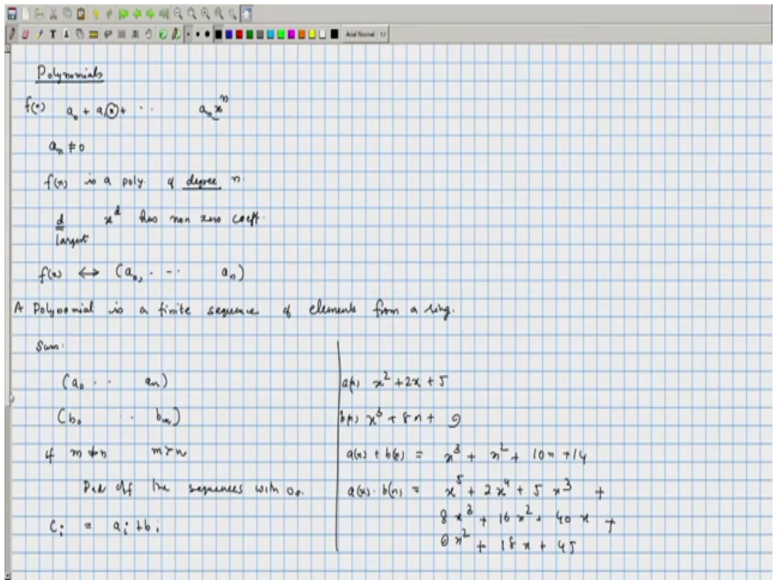
We had assumed that the elements come from a field, if they come from a field, all the non-zero entries will be invertible. So x square plus y square its inverse can be calculated, multiplied with x you will get the value of a and similarly you can find the value of b. So if you look at our field and if x square plus y square is not equal to 0 for any choice of x and y, ofcourse when x is, x and y are both 0 x square plus y square will be equal to 0 but in that case the matrix we are talking about is the all 0 matrix. So all 0 matrix we did not in mean that will not have to inverted, so all that we have to check is, are all the non-zero matrices invertible? Okay and that is the case if x square plus y square is equal 0.

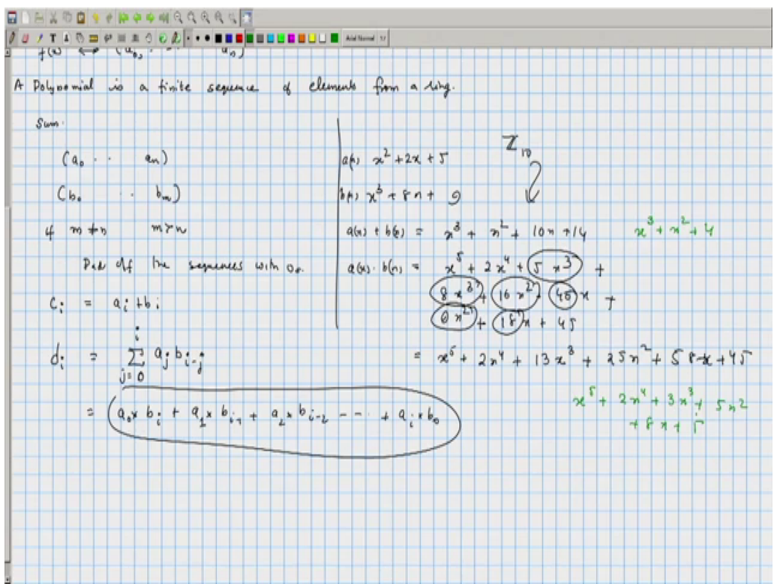
Now if you take Z3, this is 3 elements namely 0, 1 and 2. Okay so x has 3 possibilities, y has 3 possibilities, out of it 0-0 possibility we could discount and the other 8 possibilities you we manually check, so let us say 0 1 0 2, 0 0 we had skipped. So these are the x y values and then 10, 11, 12, 20, 21, 22 and x square plus y square, all those things computed mod 3, this is 1, this is 1, 1, 2, 1 square plus 2 square is 5 mod 3 that is again 2, this is 1, 2 square is 4 plus 1 5 so this is 2, 8 mod 3 that is again 2.

Okay so none of these are equal to 0, so if you choose elements from Z cube, they are going to form a field. So what we have proved is the following matrices of the form x y minus y x, whose entries are elements of Z3 form a field and this field has exactly 9 elements because x has 3 choices and y has 3 choices, once x and y has been fixed the matrix gets fixed. So and this is a matrix with, this is a field with 9 elements because we have constructed a field with 9 elements. We will see other methods for constructing fields.

But now maybe a similar thing would work, if we take Z5, we will get a field with 25 elements. If x and y, so let us try and choose Z from, x and y from Z5. Okay so that has these elements 1, 2, 3, 0, 1, 2, 3, 4 but here if we take x square plus y square, if you take 2 and 1, so 2 square plus 1 square that is equal to 0. So if we take elements from Z5, they do not form a field. Okay so we will probably have to explore other methods to come up with fields of size 25.

(Refer Slide Time: 25:00)





In order to do that, we will learn something about the polynomials. So what are polynomials? So they are familiar, we would write a polynomial in one variable x as a0 plus a1x plus anx raise to n. So this a polynomial of degree n if an is not equal to 0. So let us assume that an is not equal to 0 and then this becomes a polynomial of degree n, okay so if think of this as a function of x, we can say that f x is a polynomial of degree n. So the degree of a polynomial is a largest d such that if you consider x to the power d, its coefficient is non-zero.

So largest d is such that x to the d has non-zero coefficient, so this a0 a1 an is what we refer to as a coefficient. We are not really interested in evaluating these polynomials at particular points x, so we are just interested in the form of the polynomial. So x you can think of as a formal variable and therefore f x you can put it in one to one correspondence with a sequence of let us say n plus 1 terms. Okay so polynomial for us is now just a sequence, so a polynomial is a finite sequence of elements from a ring okay.

We will insist that these elements a0, a1 up to a n they are coming from a ring because we want is basically add and multiply polynomials. So let us look at these operations of sum and product, okay so you have one sequence a0, up to a n and another sequence b0 to bm, we can just look at terms and add them. So suppose m is not equal to n and let us say m is greater than n, then we can basically pad off the other polynomial with enough number of 0s okay and then we may assume that m is equal to n and therefore the new sequence, its Ci^{th} term will be equal to ai plus bi, okay so that is the sum.

So if you had this polynomial x square plus (x) plus, x square plus 2x plus 5 and another polynomial x cube plus 8x plus 9, so this is your 1^{st} polynomial, let us say this is ax and this is bx. So ax plus bx would basically be x cube plus x square plus 10 x plus 14. And here we were looking at these coefficients and the addition of these coefficients were happening in the ring, 8 plus 2 that gave us 10, 9 plus 5 we got 14, because we assumed that these numbers were from the ring of integers.

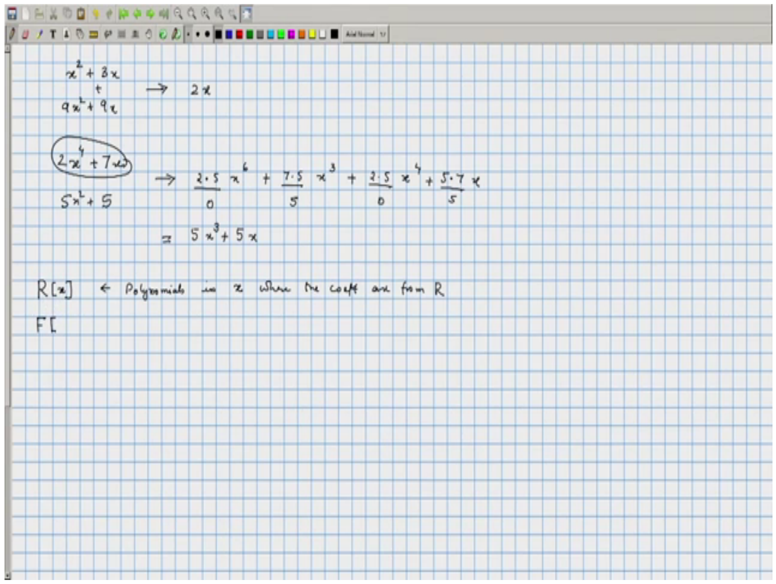
We could also define their product, so ax times bx would be equal to, so x cube into all these would give x raise to 5 plus 2 x raise to 4 plus 5x cube plus 8x when you multiply you will get 8x raise to 3 plus 16 x square plus 40x plus 9x square plus 18x plus 45. So that can be combined and written as x raise to 5 plus 2x raise to 4 plus these terms combined to give us 13x cube plus these two terms combined to give us 25x square plus 58x plus 45 okay.

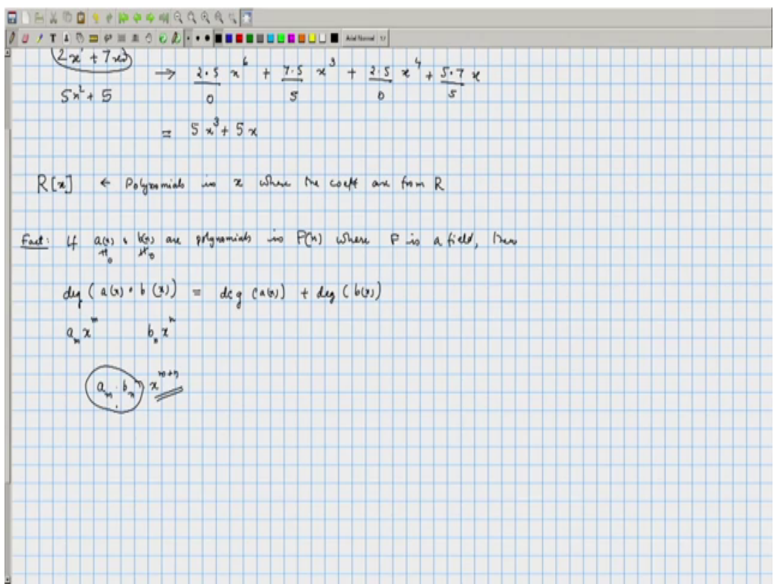
So multiplication is little more complex operation but we are essentially looking at the coefficients and adding and multiplying the coefficients in the ring of integers okay. So firmly, we could mean if you multiply this then the i^{th} term will be, if we just denote ci or let say di is a product, so di is equal to sum over let us say j varying from 1 to i, or 0 to i, aj b i minus j, so a0 multiplied by, that is equal to a0 into bj plus a1 into b, a1 into bi minus 1 plus a2 into b i minus 2 all the way up to ai times b0 okay.

So the i^{th} term coefficient will be basically this, sum of products. Okay again all those operations are carried out in the (integer) in the ring of integers when we have considered this particular example, okay so now if these elements, when instead of carrying out these operations in the ring of integers, if we had to carry out these operations mod 10 okay, so instead of integers if we were considering Z10, then this sum would be different, mean in that case the answer would be x cube plus x square plus 4, because 10x is 0 times x and that just 0 and 14 mod 10 is going to be 4.

And if we look at the product, that will be equal to x raise to 5 plus 2x raise to 4 plus 3x cube plus 5x square plus 8x plus 5. Okay so that is going to be a different polynomial than let us say what we do when we had considered the ring of integers. So when we are considering the arbitrary rings, the degrees I mean there some not means so the way the degree behaves is different from the usual behaviours. In the sense, if you add two polynomials, their degrees could come down.

(Refer Slide Time: 32:19)





For example, if you take x square plus 3x and 9x square plus which is plus 9x and if you add them, if you add them mod 10, if you are doing this mean if this is from the ring of integers mod 10 then when you sum the result would be 10x square which is 0 and plus 12x and that could be, that is just 2x. So suppose you had polynomials 2x raise to 4 plus 7x and 5x square plus 5, if you multiply them out, the usual, the answer would be 2 into 5 x raise to 6 plus 7 into 5 x cube plus 2 into 5 x raise to 4 plus 5 into 7 x, multiplication when carried out mod 10, this would give us 0, this would give us 5 and this would give us 0 and this would give us 5.

So mod 10 the answer is 5 x cube plus 5x okay, so we had taken a larger polynomial, mean the polynomial of larger degree and when you multiply it with some other non-zero polynomial, you are getting some result where the degree is reducing. Okay so the degree could behave in, in very funny manner. So we can take care of these kind of situations by just working in a field.

We insisted that these number, these coefficients of the polynomials were coming from a ring, (name) if you are taken these coefficients to come from a field then we can show that when you multiply two polynomials their degree cannot decrease. So let us have some notations, so if you have a ring R and if you look at polynomials whose coefficients comes from R, then we will write it as Rx. So this is the notation for polynomials in x where the coefficients are from R.

And if we have a field, we might usually write it as F of x to indicate the difference between a ring and a field. Okay so when we say Fx or Rx it means, we are considering polynomials in the variable x and the coefficients are coming from R or F. Okays so if we have a, if we have polynomials, if we consider the polynomials, where the coefficients are from a field then we will have the following observation.

If ax and bx are polynomials in Fx where F is a field then degree of ax times bx is equal to degree of ax plus degree of bx. Okay we should assume that ax is not equal to 0 and bx is not equal to 0 because if they were 0 and you take the product, we will get 0. So if they are non-zero polynomials then the degree is add up, easy to check. So if ax is a polynomial and if its degree is m and there is a term am x to the power m and in bx there is a term bn x to the power n and then you take the product is going to be this term am times bn into x raise to m plus n.

And since am and bn are coming from a field and they are non-zero elements of the field, they cannot multiply to give us 0 elements. So x raise to m plus n will have a non -zero coefficient and that is m plus n is going to be the largest term and therefore I mean it is the term of the highest degree and therefore the degree of the product would be equal to m plus n. Okay So we will stop here and continue in the next class.