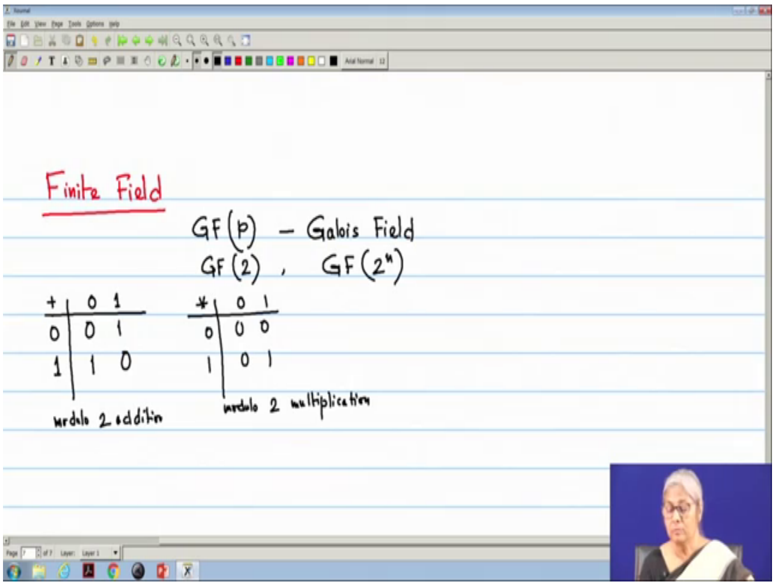
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 57
Finite Field and Applications (Contd.)

So we are discussing on the fields and in particular the finite fields.

(Refer Slide Time: 00:31)



Finite Field

GF(p) – Galois Field

GF(2) , GF(2^n)

+	0	1
0	0	1
1	1	0

modulo 2 addition

*	0	1
0	0	0
1	0	1

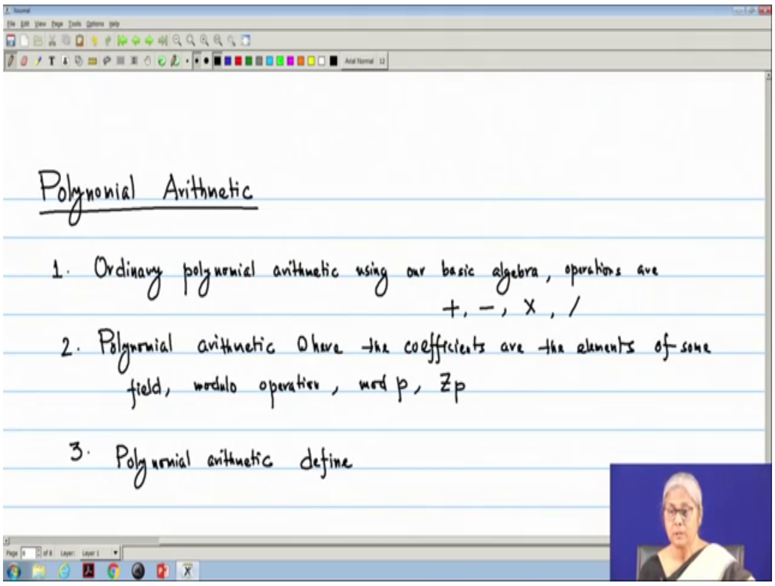
modulo 2 multiplication

So, we have read the how fields are formed; that means, over the commutative ring or the integral domain, how multiplicative inverse is that; if exist then it becomes a field. And we have seen the example that when we take the modulo p where p is a prime that modulo p addition and multiplication over Z p how it has formed a field.

Normally these if we consider that it is over p we call this is a Galois field we call that; it is called GF p that is Galois field and so, this is GF p that Galois field of p; if p equal to 2 then normally this becomes GF 2 and or what p to the power n mainly will be considering some field where GF 2 to the power n. So, for GF 2 this will be the; it will be of two elements only. So, it will be only two; 0 and 1; two elements and these are two elements. So, if I take modulo 2 addition it is 0 0 plus 0 0 1 , 0 plus 1 is 1 and then 1 plus 0 1 and 1 plus 1 this becomes 0.

So, it is nothing but our x or the modulo 2 addition; this is our modulo 2 addition. Now similarly I can write the modulo 2 multiplication 0 0 this is 1. So, this is my modulo 2 multiplication ok. Now before pursuing our discussion on fields and particular prime field; we must read something called the polynomial arithmetic. So, because our mainly will be seeing that how this polynomial operations or the over the field of polynomials this we can; this can become a field.

(Refer Slide Time: 03:22)



Polynomial Arithmetic

1. Ordinary polynomial arithmetic using our basic algebra, operations are
$+, -, \times, /$

2. Polynomial arithmetic 0 have the coefficients are the elements of some field, modulo operation, mod p, Zp

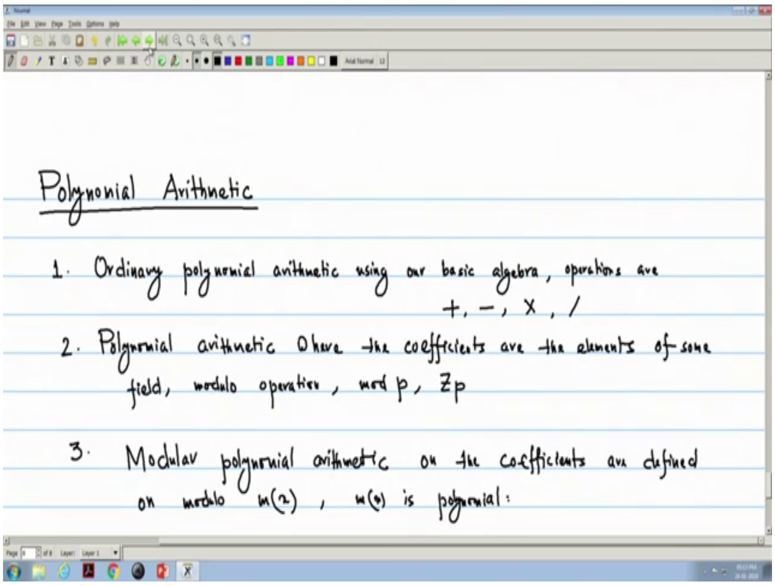
3. Polynomial arithmetic define

So, first we see the Polynomial Arithmetic. Now here actually this polynomial arithmetic; this any polynomial is taken as a variable. Now mainly here we will be reading the three things; one is normal polynomial arithmetic the or we call the ordinary arithmetic on polynomial; ordinary polynomial arithmetic using our basic algebra and the operations concerned are mainly operations are our ordinary addition, subtraction, multiplication and division, these are the operations will be seen.

Then we will see the polynomial arithmetic in which the coefficients are the elements of some field. So, now we will see the polynomial arithmetic where the coefficients are the elements of some field and just now the example or the last lecture we have read the modulo p; then the operations that will be taking that we will be the modulo operations; that means, modulo addition and multiplication. And we can see that the coefficients; if it is modulo operation on modulo p or modulo p then the coefficients can be Z p that will be seen.

Then another thing another will read the now polynomial again polynomial arithmetic and define polynomial arithmetic; it is defined that the operations are some modulo or modular polynomial arithmetic better I write because the operations are on modulo m x.

(Refer Slide Time: 07:27)



Polynomial Arithmetic

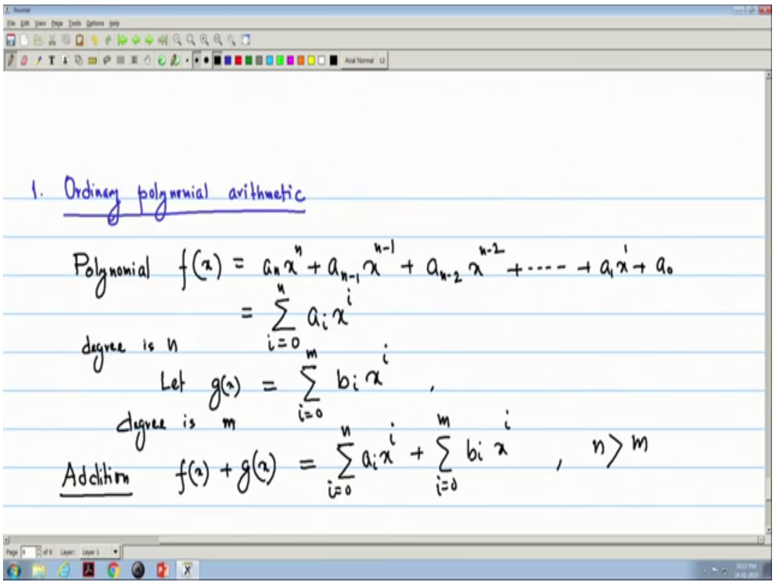
1. Ordinary polynomial arithmetic using our basic algebra, operations are $+, -, \times, /$

2. Polynomial arithmetic where the coefficients are the elements of some field, modulo operation, mod p, Zp

3. Modular polynomial arithmetic on the coefficients are defined on modulo m(x), m(x) is polynomial:

So, I write modular polynomial arithmetic; this is modular polynomial arithmetic on the coefficients are defined on modulo m x where m x is a polynomial ok. And finally, we will show that with this procedure that even some field which is not when we are taking that it is not a field if we consider that our normal modulo n operation, but using the polynomial arithmetic particularly modular polynomial arithmetic this becomes a field and that is of interest in real life applications.

(Refer Slide Time: 08:59)



1. Ordinary polynomial arithmetic

Polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x^1 + a_0$

$= \sum_{i=0}^{n} a_i x^i$

degree is n

Let $g(x) = \sum_{i=0}^{m} b_i x^i$,

degree is m

Addition $f(x) + g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i$, $n > m$

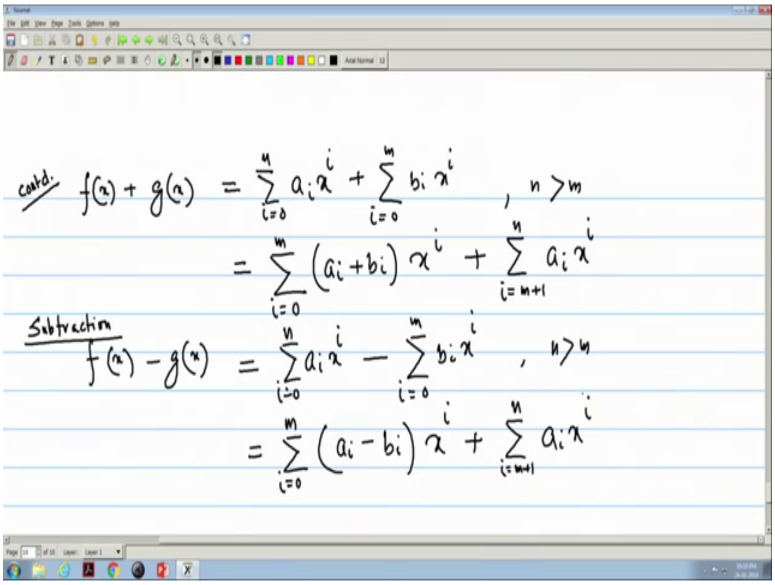
So, first we see the ordinary polynomial arithmetic; the number 1 is ordinary polynomial arithmetic as the arithmetic, here will be only on ordinary addition, subtraction, multiplication, division. So, first we consider the; our addition, subtraction and multiplication, division we will be seeing later.

So, first thing is first we define a polynomial so, a polynomial. So, we define a polynomial f x is a n x to the power n a n minus 1 x to the power n minus 1 a n minus 2 x to the power n minus 2 plus up to a 1 x x to the power 1 plus a 0; it is x to the power 0 is 1. So, I can write in this notation that n equal to 0 or sum i equal to 0 to n; i equal to 0 to n a i x to the power i and I call this is a n degree polynomial. So, this degree of the polynomial is degree is n.

Now, if I consider another polynomial g x so, let g x equal to another polynomial of degree m say i equal to 0 to m and b i x to the power i; that means, let g x; here degree is m. Now if I take the addition of f x and g x; that means, my addition will be f x plus g x and here i equal to 0 to n a i x to the power i i equal to 0 to m b i x to the power i and let we have considered n greater than m; that means, degree of f x is greater than the degree of g x.

So, there will be some more terms from because from m plus 1 to n that terms will be here.

(Refer Slide Time: 12:36)



contd.

$$f(x) + g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i \quad , \; n > m$$

$$= \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i$$

Subtraction

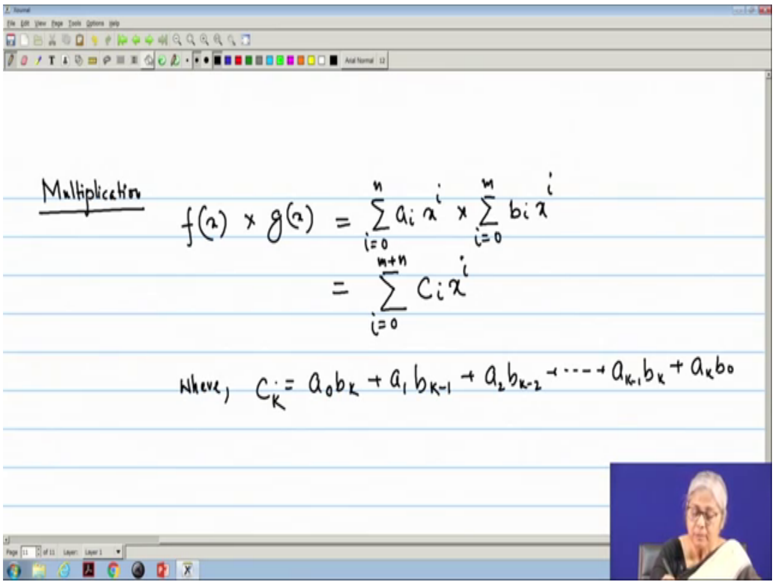
$$f(x) - g(x) = \sum_{i=0}^{n} a_i x^i - \sum_{i=0}^{m} b_i x^i \quad , \; n > m$$

$$= \sum_{i=0}^{m} (a_i - b_i) x^i + \sum_{i=m+1}^{n} a_i x^i$$

So, the sum will be the sum will be f x plus g x is i equal to 0 to n f a i; x to the power i and i equal to 0 to m b i x to the power i. So, what I can do that for i equal to 0 to m; since n less than; n greater than m. So, I can write that a i plus b i x to the power i ; that means, that degree wise the coefficients were added, I have some more terms in the first term that i equal to m plus 1 to n a i x to the power i. So, the addition is defined like that.

Similarly, I can defined it is same as that of my subtraction. So, if it is my subtraction it is f x minus g x and I can write this is i equal to 0 to n a i x to the power i minus i equal to 0 to m b i x to the power i; n greater than m and instead of plus only I have minus because i equal to 0 to m a i minus b i x to the power i plus as usual this m plus 1 to n this term will be a i x to the power i; now this is my subtraction.

(Refer Slide Time: 15:23)



Multiplication

$$f(x) \times g(x) = \sum_{i=0}^{n} a_i x^i \times \sum_{i=0}^{m} b_i x^i$$

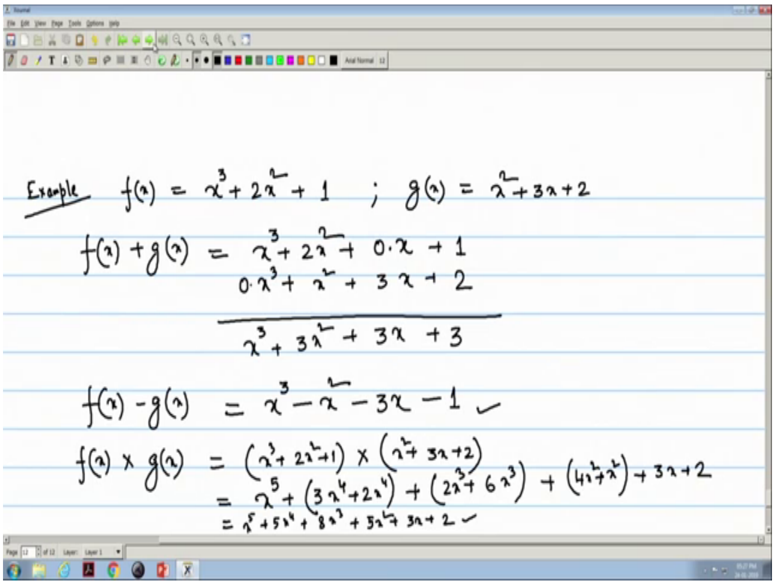
$$= \sum_{i=0}^{m+n} c_i x^i$$

Where, $c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_{k-1} b_k + a_k b_0$

Now, is multiplication; if I take the multiplication, the f x into g x and this will be simply the i equal to 0 to n a i x to the power i into i equal to 0 to m b i x to the power i and if I do that multiplication the result will be i equal to 0 to m plus n and this will be the a i of b j those terms all the terms will be there I write c i x to the power i where I can write where c i is a i or i all the terms if I write it will be a 0 b m plus n; I shall write a 0 b k a 1 b k minus 1 plus a 2 b k minus 2 plus a k minus 1 b k plus a k; a k b 0.

So, I can take all these terms and here actually k I have given. So, it should be k only; it should be k.

(Refer Slide Time: 17:33)



Example $f(x) = x^3 + 2x^2 + 1$; $g(x) = x^2 + 3x + 2$

$$
\begin{array}{rl}
f(x) + g(x) = & x^3 + 2x^2 + 0 \cdot x + 1 \\
 & 0 \cdot x^3 + x^2 + 3x + 2 \\
\hline
 & x^3 + 3x^2 + 3x + 3
\end{array}
$$

$f(x) - g(x) = x^3 - x^2 - 3x - 1$ ✓

$f(x) \times g(x) = (x^3 + 2x^2 + 1) \times (x^2 + 3x + 2)$

$= x^5 + (3x^4 + 2x^4) + (2x^3 + 6x^3) + (4x^2 + x^2) + 3x + 2$

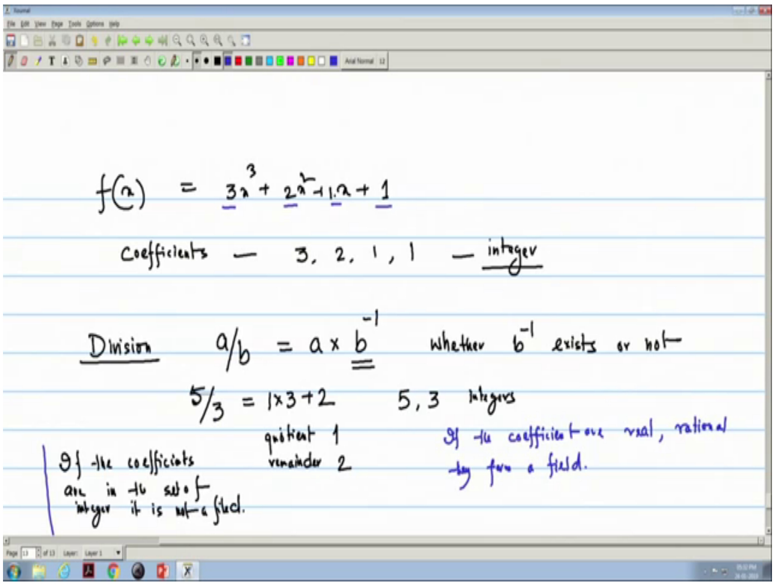
$= x^5 + 5x^4 + 8x^3 + 5x^2 + 3x + 2$ ✓

So, if I take some example; if I take one example say my f x is x cube plus 2 x square plus 1 and g x is x square plus 3 x plus 2 ok. Now what will be my f x plus g x, see f x plus g x; I can write if I consider all the terms that x to the power 3 plus 2 x square plus I can take since it does not have any x to the power 1 term so, I write 0 into x plus 1 and g x if I add so, g x does not have any x to the power 3 term so, I; coefficient should be 0 then x square, then 3 x then 2.

So, if I add I will be getting x cube then 3 x square plus 3 x plus 3. So, the way we have done that 0 to m so, it is up to 2; only the coefficients will be added. So, 2 x square it has 1 x square so, 3 x square it does not have any x term. So, 0 plus 3 3 1 plus 2 3 and the m plus 1 to n; that means, only 1 it is left is cube. Similarly I can do here now directly I can write f x minus g x; since there is no cube; degree 3 term say x cube minus x square because 2 minus 1. So, x square then minus 3 x because it does not have any 0 x minus 3 x plus 1 minus 2 so, it is minus 1. So, f x minus g x is that.

Now, if it is f x into g x that multiplied that ordinary multiplication we are doing and the coefficients are we are taking. So, this will be x cube plus 2 x square plus 1 and we take x square plus 3 x plus 2. So, it will be if I take m plus n; if we remember the way we have written so, it will be x to the power 5 plus 3 x cube the term will be the; a 0 b k. So, here x cube 3 x 4 and 2 x 4 so, I can write 3 x to the power 4 plus 2 x to the power 4 plus x cube term that 2 x cube; then 2 into 3 6 x cube plus that 2 x 4 2 x cube; then x square term 2 into 2 plus 4 x square plus 1 into x square plus now there is no other term here so, only 3 x plus 2. So, I have considered all the thing then it will be x to the power 5 plus 5 x to the power 4 plus 8 x cube plus 5 x square plus 3 x plus 2. So, we get the result here.

(Refer Slide Time: 22:39)



$f(x) = \underline{3}x^3 + \underline{2}x^2 + \underline{1}.x + \underline{1}$

Coefficients — 3, 2, 1, 1 — $\underline{\text{integer}}$

$\underline{\text{Division}}$ $a/b = a \times \underline{\underline{b}}^{-1}$ whether b^{-1} exists or not

$5/3 = 1 \times 3 + 2$ 5, 3 integers

quitient 1
remainder 2

If the coefficient are real, rational they form a field.

If the coefficients are in the set of integer it is not a field.

Now here the whenever we are considering a polynomial say f x say f x equal to I am taking 3 x square now 3 x cube plus 2 x square plus a x plus 1 like that. See here the coefficients are 3 2 1 1 here it is not there means it is actually it is 1 ok. So, now, my coefficients are here coefficients we are taking it is 3 2 1 1; that means, as if these are integer coefficients we are taking positive integers or integer coefficients we are taking.

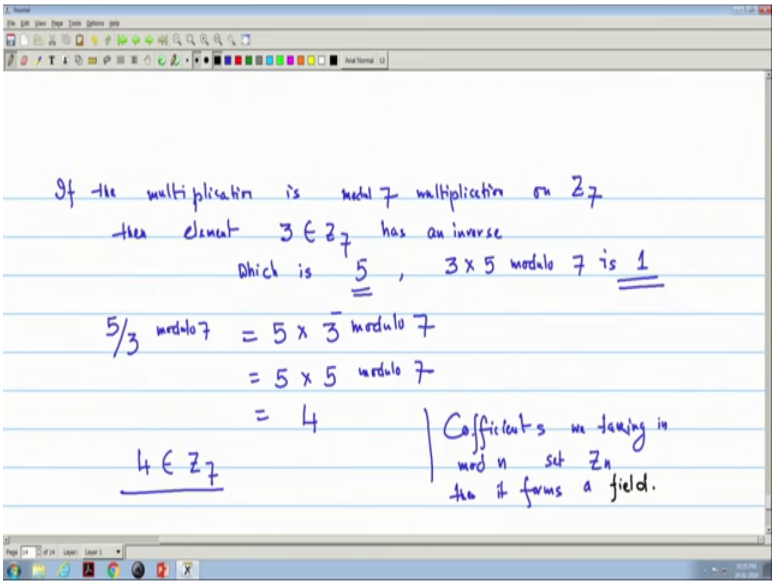
Now, so, we have defined multiplication; addition, subtraction, multiplication, now what about division? What about my division; because if we remember that our modulo 7 see if I; because if I want the division we consider division then I need some inverse. That means, I can write that a by b so, actually I can write this is a into b inverse if it is ordinary multiplication and division. Now the main point is or issue is here whether b inverse exist or not, because just now the; from the definition of field we have seen and we have seen some examples that this multiplicative inverse may not exist.

So, here that whether the main issue is whether b inverse exists or not. Say I consider 5 by 3; I consider 5 by 3. So, my 5 is 5 and 3 are integers so, if my set is the integer set then I know that I cannot get this integer as the 5 by 3 1, but because I know this 5 by 3 is 1 now the 1 into 3 plus 2 so that means, here I get that remainder; quotient 1 and remainder 2 ok, quotient 1 and remainder 2.

So, if my coefficient sets are integer then actually they are not forming a field they are not in field; they are forming a field; that means, coefficients, if the coefficients are in the set of integer because if it is a integer that multiplicative inverse does not exist. So, it is not a field , but if the coefficients are if the coefficients are real or complex number if the coefficients are real number or say rational number or complex number then they form a let me write here in this case I see the real numbers then they are form they form a field.

Now, if I take 5 by 3; now the operation we have seen say modulo 7.

(Refer Slide Time: 27:40)



If the multiplication is modul 7 multiplication on Z_7

then element $3 \in Z_7$ has an inverse

Which is $\underline{\underline{5}}$, 3×5 modulo 7 is $\underline{\underline{1}}$

$5/3$ modulo 7 $= 5 \times \bar{3}$ modulo 7

$= 5 \times 5$ modulo 7

$= 4$

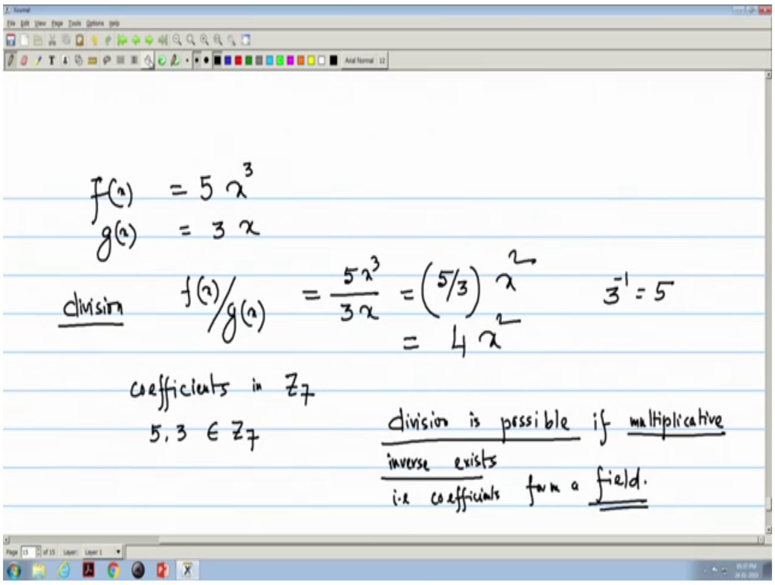
$\underline{4 \in Z_7}$

Cofficients we taking in mod n set Z_n then it forms a field.

If the multiplication is modulo 7; that is multiplication modulo 7 is modulo 7 multiplication on Z 7 then we know that 3 has some inverse, then the element 3 belongs to Z 7 has an inverse which is which is 5 because 3 into 5 modulo 7 is 1; multiplicative identity; this is multiplicative identity. So, this is I know that 3 has inverse so, now, if I do the 5 by 3 under modulo 7 operation then I can write this is 5 into 3 inverse modulo 7 and that is 5 into 5 modulo 7 and is 25 modulo 7 is 4. So, the result exist and since 4 is 4 belongs to Z 7 so, this forms a field.

So, if I take the coefficients and we take the instead of normal coefficients in Z p; so, now, what is the conclusion? the; if the coefficients we are taking; coefficients we are taking in some modulo n; that means, set is in coefficients set are in Z n; here the examples then it forms a field. Why you are doing that thing, because if inverse exist then we can take the we can do the division; then it forms a field and if it is field then inverse exist and then division is possible say field ok.

(Refer Slide Time: 30:35)



$f(x) = 5x^3$

$g(x) = 3x$

$\underline{\text{divisin}}$ $\quad f(x)/g(x) = \frac{5x^3}{3x} = (5/3)\,x^2 \qquad 3^{-1} = 5$

$= 4x^2$

coefficients in Z_7

$5, 3 \in Z_7$

division is possible if multiplicative inverse exists

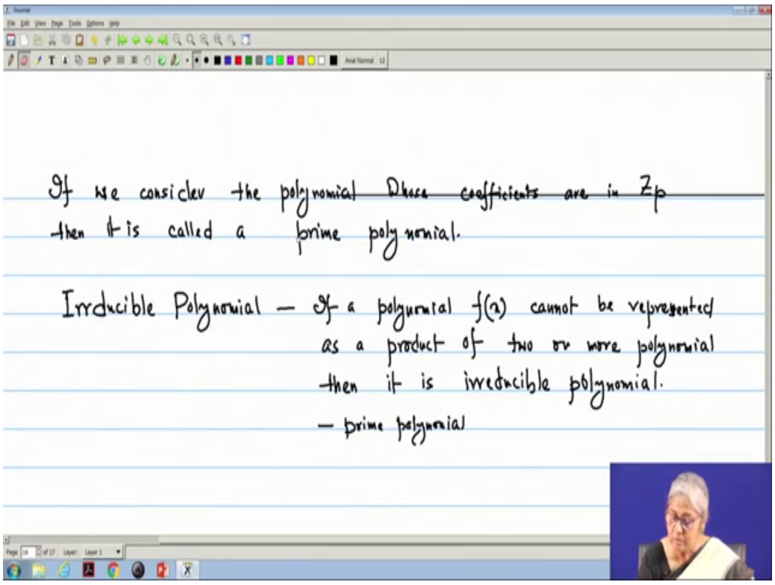
i.e coefficients form a field.

Now; that means what? If I; if it is a polynomial; that means, my f x say f x is I take a very simple example with 5 x cube and say my g x is g x is 3 x. So, division now if I consider division I can do f x by g x f x divided by g x and that is equal to 5 x cube divided by 3 x and this is 5 by 3 x cube by x is x square and ordinary division I cannot get, but if the coefficient is in modulo 7 then just now we have seen that it is 4 x square.

Because if the coefficients; because 3 inverse equal to 5. Just now we have seen coefficients in Z 7 because 5 and 3 or 5 3 all belongs to Z 7 because 0 to 6. So, then I can do the then division is possible so, conclusion is then division is possible; that means, multiplicative inverse exist and multiplicative inverse exist means the coefficient forms a field. Division is possible if multiplicative inverse exist multiplicative inverse exists and multiplicative inverse exist means and; that means, that is the coefficients form a field; that means, the coefficients form a field.

So, why field is very important because then only I can do the division also; I can do all the division etcetera. So, now, we will see that if I consider the polynomiality then it is actually.

(Refer Slide Time: 33:11)



If we consider the polynomial ~~whose coefficients are in Z_p~~
then it is called a prime polynomial.

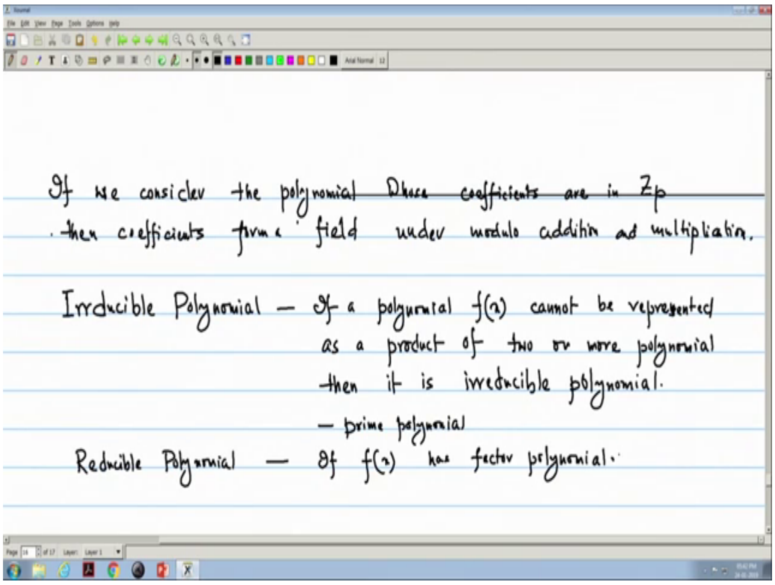
Irrducible Polynomial — If a polynomial $f(x)$ cannot be represented as a product of two or more polynomial then it is irreducible polynomial.
— prime polynomial

If the; if we consider polynomials we consider the polynomial because we are discussing on polynomial arithmetic, polynomial whose coefficients are in Z p then it is called a prime polynomial; then it is called a prime polynomial.

And some more definition on polynomial is very important and we will be discussing on that; one is that called the irreducible polynomial and reducible polynomial. So, irreducible polynomial that if the polynomial has no factor polynomial is has no factor then if a polynomial f x has no factor; that means, it cannot be represented as a product of two other polynomials; that means, it has no factor, product of two or more polynomials. So, it is similar or analogous to the prime number.

So, if your polynomial cannot be represented as product of two or more polynomial then it is irreducible polynomial and sometimes we analogy with irreducible is the prime; this is called the prime polynomial. So, this is different this is not prime here.

(Refer Slide Time: 36:44)



If we consider the polynomial whose coefficients are in Z_p

. then coefficients form a field under modulo addition and multiplication.

Irreducible Polynomial — If a polynomial $f(x)$ cannot be represented as a product of two or more polynomial then it is irreducible polynomial.

— prime polynomial

Reducible Polynomial — If $f(x)$ has factor polynomial.

Coefficients are in prime; consider polynomial whose coefficient are there; the; then the coefficients form a field under modulo addition and multiplication. And if the polynomial f x has factor then it is called reducible polynomial ok. If f x has factors; has factor polynomials; that means, factor means it has, it can be represented as a product of some other polynomials. So, what we see that if we; the, we started the discussion with three; one the ordinary polynomial arithmetic and then the so, mainly we have seen the ordinary polynomial arithmetic and the polynomial arithmetic where the coefficients are the elements of some field. So, we have seen that if the coefficients form a field then division is possible so, these two things we have done.

And now we will be in the; in our next lecture we will read this is the third one the when the modular polynomial arithmetic; that means, the divisor or the that can be treated as a itself treated as a variable and we can take the modulo m x type of thing. So and whether they form a field and what are the application areas of that. So, how finite fields mainly this polynomial arithmetic, why it is important that we will be discussing in our next lectures.