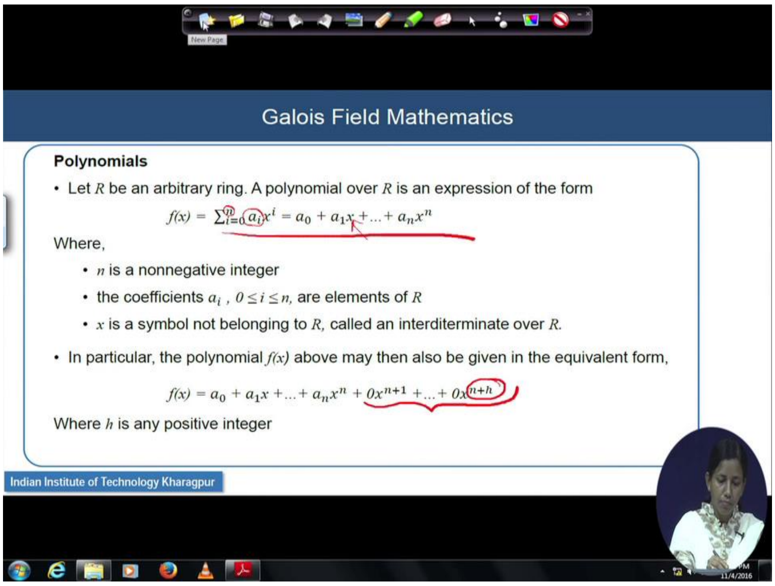
Spread Spectrum Communications and Jamming

Prof. Debarati Sen
G S Sanyal School of Telecommunications
Indian Institute of Technology, Kharagpur

Lecture - 26
Galois Field Mathematics (Contd.)

Hello students. In continuation of the Galois Field Mathematics; we will continue further the same thing in this module. We have learnt the definition and the properties of a set, a group, a ring and the field. Today our discussion will be mainly concentrating on the polynomials.

(Refer Slide Time: 00:45)



Galois Field Mathematics

Polynomials

- Let R be an arbitrary ring. A polynomial over R is an expression of the form

$$f(x) = \underline{\sum_{i=0}^{\boxed{n}} \boxed{a_i} x^i = a_0 + a_1 x + \ldots + a_n x^n}$$

Where,

- n is a nonnegative integer
- the coefficients a_i , $0 \leq i \leq n$, are elements of R
- x is a symbol not belonging to R, called an interditerminate over R.

- In particular, the polynomial $f(x)$ above may then also be given in the equivalent form,

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n + \underbrace{0x^{n+1} + \ldots + 0x^{\boxed{n+h}}}$$

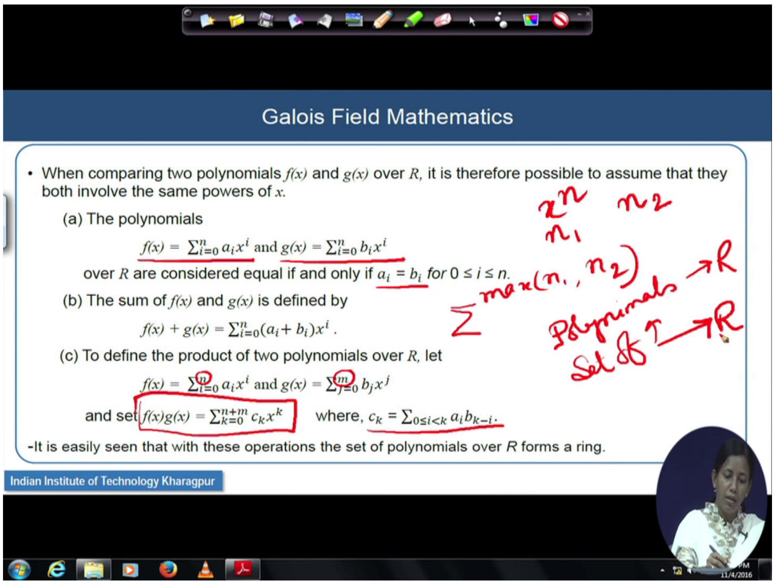
Where h is any positive integer

Indian Institute of Technology Kharagpur

Let R be an arbitrary ring. The polynomials over this ring will be given by the expression written here, f x equal to summation of the i is going from 0 to n a i into xi, where all the a is being the coefficients. And the coefficients based on the value of the i a i is moving from a 0 to a n. Remember this a n is a non-negative integer, and x is not a part of this ring, x is called the inter determinant. And it is introduced for the convenience in mathematics.

In particular, this expression of this polynomial can be specifically written like this, where the first equation is derived from the next by deleting all the zeroth co efficient elements. And with the 0th co efficient elements actually your higher order the maximum order of the x, actually is going up to n plus h, where h is another positive integer; however, as 0th co efficient terms can be discarded the polynomial expression that we will deal in this module will be given by this form.

(Refer Slide Time: 02:10)



Galois Field Mathematics

- When comparing two polynomials $f(x)$ and $g(x)$ over R, it is therefore possible to assume that they both involve the same powers of x.

(a) The polynomials

$$\underline{f(x) = \sum_{i=0}^{n} a_i x^i} \text{ and } \underline{g(x) = \sum_{i=0}^{n} b_i x^i}$$

over R are considered equal if and only if $\underline{a_i = b_i}$ for $0 \le i \le n$.

(b) The sum of $f(x)$ and $g(x)$ is defined by

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

(c) To define the product of two polynomials over R, let

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ and } g(x) = \sum_{j=0}^{m} b_j x^j$$

and set $\boxed{f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k}$ where, $\underline{c_k = \sum_{0 \le i < k} a_i b_{k-i}}$.

-It is easily seen that with these operations the set of polynomials over R forms a ring.

Indian Institute of Technology Kharagpur

x^n n_2
n_1

$\sum^{max(n_1, n_2)}$

Polynomials → R
Set of ↑ → R

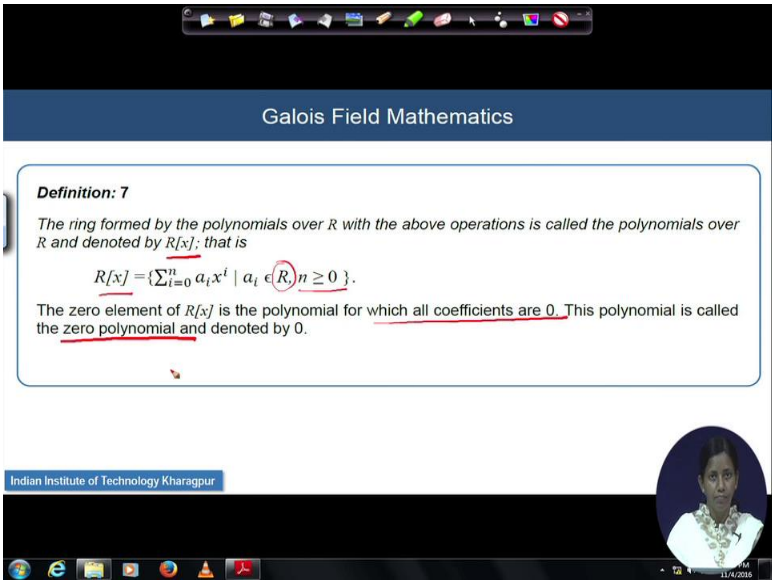
When comparing 2 polynomials suppose f x and gx are the 2 polynomials over this R and let us and let us also assume that both of the n are having the power of x equal to n. So, both of the n are having maximum power that is associated with both of the n is equal to n. So, the polynomials can be written like this f x is equal to a i x to the power i gx is also b i x to the power i. So, under what condition we can say both the polynomials are equal.

The condition is if and only if a i is equal to b i as the numbers are high order number is going up to n, hence this is the sufficient situation. And if it is not I mean f x is going sat up to the order of n 1, and gx is go going up to the n 2, and then for the polynomials to be equal definitely you also have to prove that n 1 is equal to n 2. The sum of the polynomials f x and gx were when both of them are having the same power of x equal to n, then it will be given simply by a i plus b i into x i.

Remember if they are having different values of n, then it will be the summation will go up to maximum of n 1 comma n 2, anybody maximum of n 1 comma n 2 means that whoever is having the higher value, the summation will run up to that. To define the product of 2 polynomials, we will start with the same having considering that both are having the same structure. And if they are having the same structure it will be n plus m and it is having the up to the value of m gx is running, then it will be given by n plus m. So, if it is n 1 n 2, then it will go up to the n 1 plus n 2, where actually this a i and b j they will be combined in the form of c k, where c k can be expressed like this. So, there is a relation of a i b i and c k given by this expression, and the product is given by this final expression f x gx is equal to like this, so it easily seen that with this operation the set of the polynomials.

So, R over R they also form a ring. So, polynomials R a part of a ring, and the same and the set of the polynomials, who are having such kind of the properties they can form another ring which we will call the polynomial ring over the ring R.

(Refer Slide Time: 05:06)



Galois Field Mathematics

Definition: 7

The ring formed by the polynomials over R with the above operations is called the polynomials over R and denoted by $R[x]$; that is

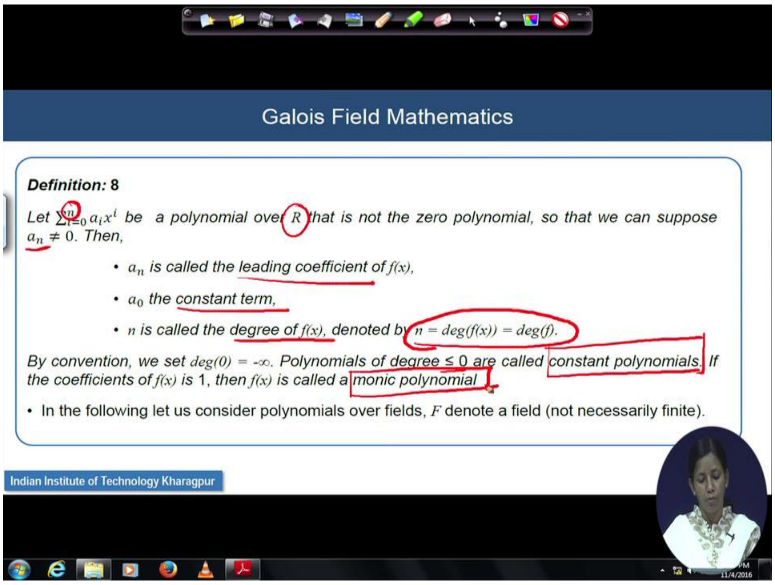
$$R[x] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in R, n \geq 0\}.$$

The zero element of $R[x]$ is the polynomial for which all coefficients are 0. This polynomial is called the zero polynomial and denoted by 0.

Indian Institute of Technology Kharagpur

So, the ring that is formed over the polynomial by the polynomials over R, with this above property will be explained like we will have expressed by R x. Whereas the R x will be given as i going from 0 to n a i x i, where a i is drawn from ring R and n should be a positive and positive integer greater than equal to 0. If a with the 0 element of this ring is a polynomial for which all the coefficients are 0.

(Refer Slide Time: 05:56)



Galois Field Mathematics

Definition: 8

Let $\sum_{i=0}^{n} a_i x^i$ *be a polynomial over* R *that is not the zero polynomial, so that we can suppose* $a_n \neq 0$. *Then,*

- a_n *is called the leading coefficient of* $f(x)$,
- a_0 *the constant term,*
- n *is called the degree of* $f(x)$, *denoted by* $n = deg(f(x)) = deg(f)$.

By convention, we set $deg(0) = -\infty$. *Polynomials of degree ≤ 0 are called constant polynomials. If the coefficients of* $f(x)$ *is* 1, *then* $f(x)$ *is called a monic polynomial*

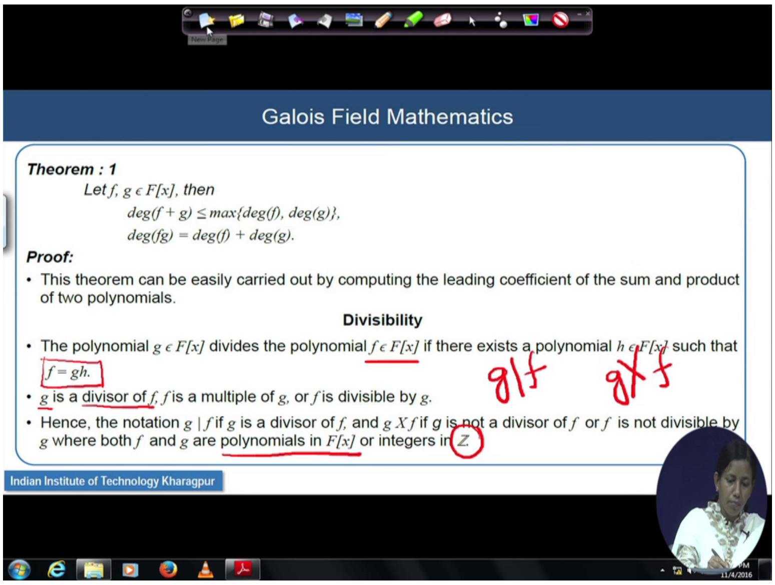
- In the following let us consider polynomials over fields, F denote a field (not necessarily finite).

Indian Institute of Technology Kharagpur

So, the all coefficients equal to 0 polynomials we will call the 0 element. And polynomial will be called also the 0 polynomial. Now definition next definition; suppose this is a polynomial a i x i summation going from i equal to 0 to n, over the ring R is a polynomial. And we also consider that it is not a 0 polynomial. So, we can think that if it is not a 0 polynomials. So, none of the coefficients are 0. And hence an is not equal to 0. Then this a n will be called the leading coefficient. And a 0 will be called the constant term. The n will be call up to which the summation is running, this n is called the degree of the polynomial, and hence we can write it like this. By convention we set that degree 0 is equal to minus infinity. And all the polynomials so, we will have the degree less than equal to 0 which we will call them the constant polynomials.

If the coefficient of f x of the all the polynomial coefficients are equal to 1, we will have called them the monic polynomial. So, see there were last slide we have learnt about the 0 polynomial, where all the coefficients at 0. All the coefficients are equal to 1 means a monic polynomial and if the degree is less than equal to 0, polynomial will be called as a constant polynomial. And let us consider from next round was let us consider the polynomials over a field capital F, F may not be doing not to be a consider as a finite field it may be an infinite.

(Refer Slide Time: 07:37)



Galois Field Mathematics

Theorem : 1

Let $f, g \epsilon F[x]$, then

$deg(f + g) \leq max\{deg(f), deg(g)\}$,

$deg(fg) = deg(f) + deg(g)$.

Proof:

- This theorem can be easily carried out by computing the leading coefficient of the sum and product of two polynomials.

Divisibility

- The polynomial $g \epsilon F[x]$ divides the polynomial $f \epsilon F[x]$ if there exists a polynomial $h \epsilon F[x]$ such that $\boxed{f = gh.}$
- g is a divisor of f, f is a multiple of g, or f is divisible by g.
- Hence, the notation $g \mid f$ if g is a divisor of f, and $g \not\mid f$ if g is not a divisor of f or f is not divisible by g where both f and g are polynomials in $F[x]$ or integers in Z.

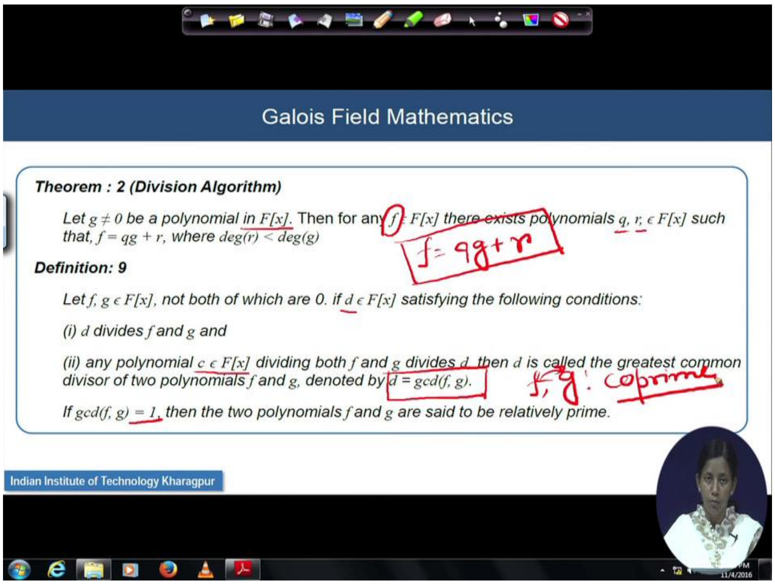
$g|f$ $g \not| f$

Indian Institute of Technology Kharagpur

The theorem says that if f and g they are the 2 polynomials that belong to the field f x. So, then the degree of the so, after summation of the 2 polynomials will be always less than equal to the maximum degree of f comma degree of g. Degree of f into g will be always the summation of the degree f plus degree of g, and it can be easily proved by that sum and product of the 2 polynomials. So, we have not included the proof here.

The next important property of the polynomials is a divisibility. So, a polynomial g that belongs to f x, which we will divide any other polynomial f, which also belongs to the f x the of the field f x, if and only if there exist third polynomial called hx who belongs to the same field f x, in such a way that f is equal g into h. So, in that situation, we can call that g is the divisor of f, f is of definitely the multiplier of g, and we will sometimes we that f is also divisible by g. So, if g is divisor of a, then we will write the term as g is a divisor of f like this. And if it is not then we will write the g is not a divisor of f. Provided that f and g both are belongs to the both polynomials belong to the field effects and they are they are the integers in the natural the set Z.

(Refer Slide Time: 09:21)



Galois Field Mathematics

Theorem : 2 (Division Algorithm)

Let $g \neq 0$ be a polynomial in $F[x]$. Then for any $f \in F[x]$ there exists polynomials $q, r, \epsilon F[x]$ such that, $f = qg + r$, where $deg(r) < deg(g)$

$\boxed{f = qg + r}$

Definition: 9

Let $f, g \epsilon F[x]$, not both of which are 0. if $d \epsilon F[x]$ satisfying the following conditions:

(i) d divides f and g and

(ii) any polynomial $c \epsilon F[x]$ dividing both f and g divides d, then d is called the greatest common divisor of two polynomials f and g, denoted by $\boxed{d = gcd(f, g)}$.

f, g : coprime

If $gcd(f, g) = 1$, then the two polynomials f and g are said to be relatively prime.

Indian Institute of Technology Kharagpur

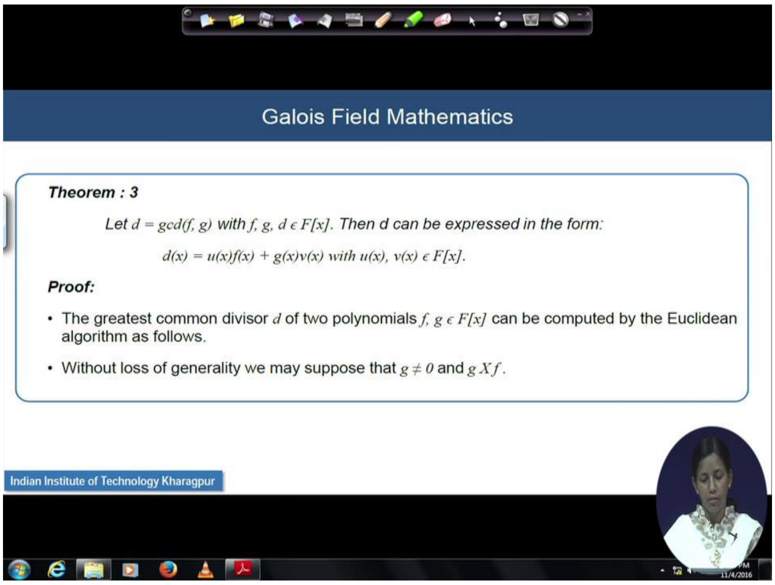
Then comes the theorem of the division algorithm. Let us assume that g which is not equal to 0 it is a polynomial over the field. Then for any other polynomial f which belongs to the same fields, that exists and has some polynomials q and r which are also part of this f x, such a way that f is equal to my q into g plus r where this degree of the r is always the less than the degree of the g.

So, earlier we were not talking about this r. We were thinking about the relation of 3 polynomials, f is divisible and gk is a divisor of f, if that exist the third polynomial q. Or earlier slide we have shown it as h, over all are belong to the same field. Now we are saying that actually they are may be a third fourth polynomial are, such a way that they can be related in this way. I have provided the degree of r is less that degree of g. Then we this is the total division algorithm of the polynomials over the field f.

And next definition let us proceed. Suppose f g these are the polynomials, which belong to the field f x, and now not both them are 0. Then they are will be existing and another polynomial d say if it also belongs to the field f x, and if d satisfies the following situation, that d divides both f and g. So, what I said is, suppose we starting with 2 polynomials f and g which belongs to f x, not both of them are equal to 0. And there is existence of another polynomial d, which is also in the field effects and d divides both g and f. And also there is an existence of the fourth polynomial c, in the same field who divides both f g, as well as d. If this is the situation, then we will say d is the greatest common devisor of f and g, and we write it as this.

If we find that the greatest common divisor of f and g or any 2 polynomials is equal to 1, then we will say that those 2 polynomials are relatively prime to each other. We call it coprime. We have seen actually this term coefficient prime when we were discussing the formation of a group. So, inside a group we have seen that if the group consists of a residual modulo p, with the prime numbers modulo the numbers which are generated from the prime number set, with the modulo p operation. Then we will see that we saw that actually any element within 0 to that p that 2 elements will be always coprime. And another coprime fundamental we have already discuss that time, that this is the greatest common divisor it comes from the fundamentals of the greatest finding outer the greatest common divisor to be equal 1 for both the polynomials. Here we have revisited it

(Refer Slide Time: 12:55)



Galois Field Mathematics

Theorem : 3

Let $d = gcd(f, g)$ with $f, g, d \epsilon F[x]$. Then d can be expressed in the form:

$$d(x) = u(x)f(x) + g(x)v(x) \text{ with } u(x), v(x) \epsilon F[x].$$

Proof:

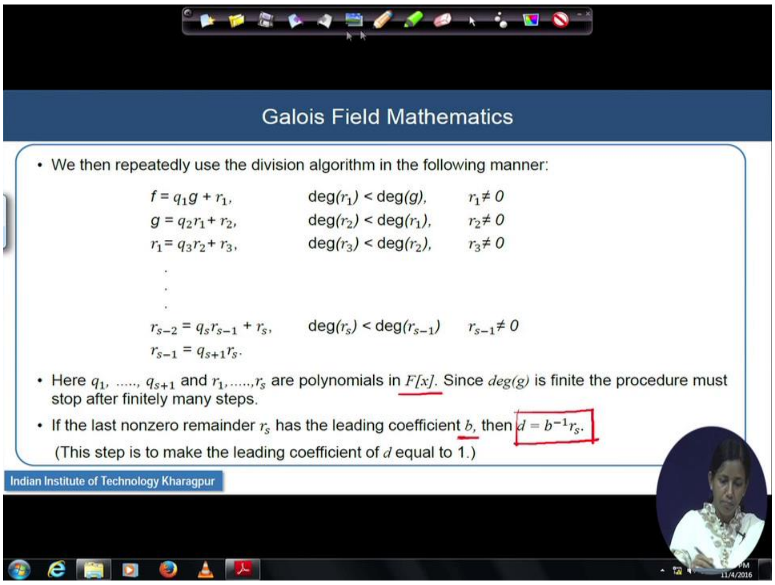
- The greatest common divisor d of two polynomials $f, g \epsilon F[x]$ can be computed by the Euclidean algorithm as follows.
- Without loss of generality we may suppose that $g \neq 0$ and $g X f$.

Indian Institute of Technology Kharagpur

Next theorem is supposing d is a greatest common divisor of 2 polynomials where all this 3 belong to the same field. Then this d the polynomial d, should be we should be able to express it in terms of x is equal to ux into f x plus gx into vx, where this ux and vx are other 2 polynomials which also both of them belongs f x. This proof is very easy and actually the greatest common divisor of the d of 2 polynomials can be computed by the Euclidean algorithm. And those Euclidean algorithms we will see in the next slide.

We think that g is not equal to 0 for the next example. And g is in the output divisor of f, d is a divisor for both of them, but g is not divisor of f.

(Refer Slide Time: 13:53)



Galois Field Mathematics

- We then repeatedly use the division algorithm in the following manner:

$$\begin{array}{lll} f = q_1 g + r_1, & \deg(r_1) < \deg(g), & r_1 \neq 0 \\ g = q_2 r_1 + r_2, & \deg(r_2) < \deg(r_1), & r_2 \neq 0 \\ r_1 = q_3 r_2 + r_3, & \deg(r_3) < \deg(r_2), & r_3 \neq 0 \\ \cdot & & \\ \cdot & & \\ \cdot & & \\ r_{s-2} = q_s r_{s-1} + r_s, & \deg(r_s) < \deg(r_{s-1}) & r_{s-1} \neq 0 \\ r_{s-1} = q_{s+1} r_s. & & \end{array}$$

- Here q_1, ..., q_{s+1} and $r_1, \ldots.., r_s$ are polynomials in $F[x]$. Since $deg(g)$ is finite the procedure must stop after finitely many steps.
- If the last nonzero remainder r_s has the leading coefficient b, then $\boxed{d = b^{-1} r_s.}$

(This step is to make the leading coefficient of d equal to 1.)

Indian Institute of Technology Kharagpur

Let us start with that example. We find that f can written as q into g plus r, here we will write it as q 1 plus r 1. Where the degree of r 1 is always less than the degree of g, if this is the situation then we can form another recurring equation, g is equal to the q 1 plus r 1 plus r 2 remember you are in the first equation f q g 1 r 1 all are the polynomials and all of them belong to the same field. If we can construct now g by a q 1 r 1 plus r 2, where q 2 r 1 q 2 and r 2 are also belong to the same field.

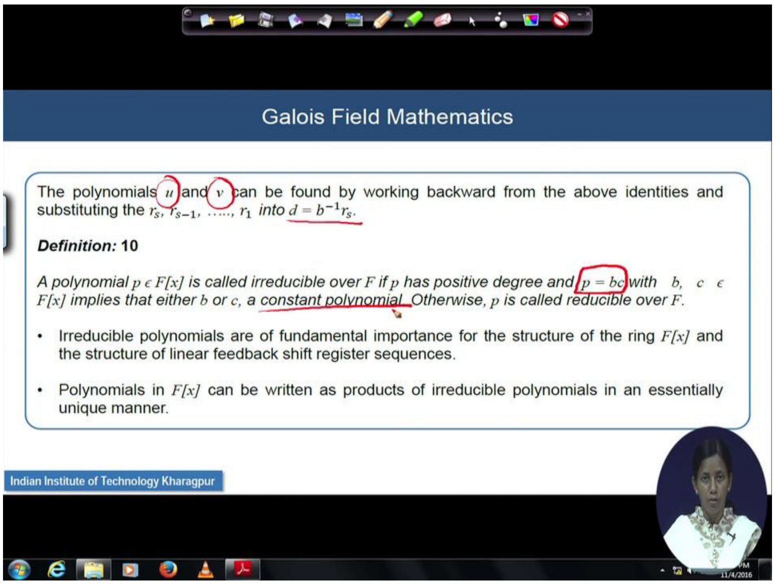
There are the other polynomials and they belong to the same field f x and again going by the same way, if now r 1 can be written as q 3 r 2 plus r 3. Where actually your q 3 and your r 3 both of them belong to the same field and degree of r 3 will is it is less than the degree of r 2. So, whenever you are finding the new polynomial to form the equation division rule, divisional got the one division equation, please remember that the degree of the newly find polynomial should be less than the degree of the immediately of the polynomial immediately found immediately earlier.

So, like that if I go ahead and we will end up with the coefficients called rs minus 1 expression. All these expressions q 1 to qs plus 1 and the r 1 to rs we have told that they are all the polynomials they should be all the polynomials and belong to the same field f

x. And sees this degree of the g is a finite number. So, with finite number of the steps, this algorithm should division algorithm should stop also.

And if the last non 0 remainder this rs that you are getting it has the leading coefficient say b then we can write that the divisor greatest common divisor the d will be given to b to the power minus 1 into rs. This step is to make this leading coefficient of d equal to 1, also because this relation is universally true because if you cannot prove that the division algorithm holds good and you can read it and you reach to feasible stoke point. And you are able to find all the other polynomial. So, were the field effects?

(Refer Slide Time: 16:33)



Galois Field Mathematics

The polynomials u and v can be found by working backward from the above identities and substituting the $r_s, r_{s-1}, \ldots, r_1$ into $\underline{d = b^{-1} r_s}$.

***Definition:* 10**

A polynomial $p \in F[x]$ is called irreducible over F if p has positive degree and $\boxed{p = bc}$ with $b, c \in F[x]$ implies that either b or c, a constant polynomial. Otherwise, p is called reducible over F.

- Irreducible polynomials are of fundamental importance for the structure of the ring $F[x]$ and the structure of linear feedback shift register sequences.
- Polynomials in $F[x]$ can be written as products of irreducible polynomials in an essentially unique manner.

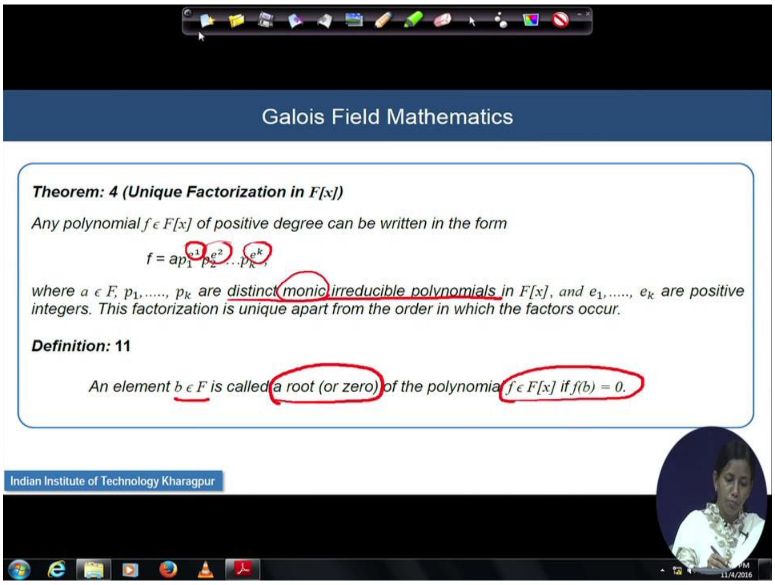
Indian Institute of Technology Kharagpur

So, now the polynomials u and v that v could which was in a equivalent to the last algorithm with the substitutions of rs and R rs up to r 1 into with this expression that we have right now, find out you we can find out actually this you and this v. Next definition it says that polynomial p it will be irreducible under what situation. And that degree p can be written in terms of b and c, where b and c both are the constant polynomial. We remember that the constant polynomial means the degree of those polynomials are less than equal to 0. And we will go back and revisit and check. So, the constant polynomials were defined where the degree will be less than equal to 0 and so, with that understanding, if that is the situation that p is equal to b into c, where all the b and c both polynomials are the constant polynomial, then it is it will be true that p cannot be divided it is reducible over that field capital F and otherwise you could reduce it.

This irreducible polynomial is of the very fundament importance when we will discuss about the code generation in l through lfsr linear feedback shift register architecture. There are they actually very fundamental importance of the ring, and they can be also very fundamental concept when you will be going ahead with the discussion of the correlation and analysis of the correlation analysis of the period maximum length sequence frequency generation even pn sequence generations, long non-linear sequence generation. We will see actually this expression of it is important in the generation of linear feedback shift register, and also the long non-linear sequence generation later on.

The polynomials in f x; it can be written in the as products of this irreducible polynomials as in essentially unique manner. We will see it you can verify it by some example. Now let us come some unique factorization in f x; suppose the polynomial f is existing over the field f x. And it is having a positive degree.

(Refer Slide Time: 19:15)



Galois Field Mathematics

Theorem: 4 (Unique Factorization in $F[x]$)

Any polynomial $f \epsilon F[x]$ of positive degree can be written in the form

$$f = ap_1^{e1} p_2^{e2} \dots p_k^{ek},$$

where $a \epsilon F$, $p_1, \dots.., p_k$ are distinct monic irreducible polynomials in $F[x]$, and $e_1, \dots.., e_k$ are positive integers. This factorization is unique apart from the order in which the factors occur.

Definition: 11

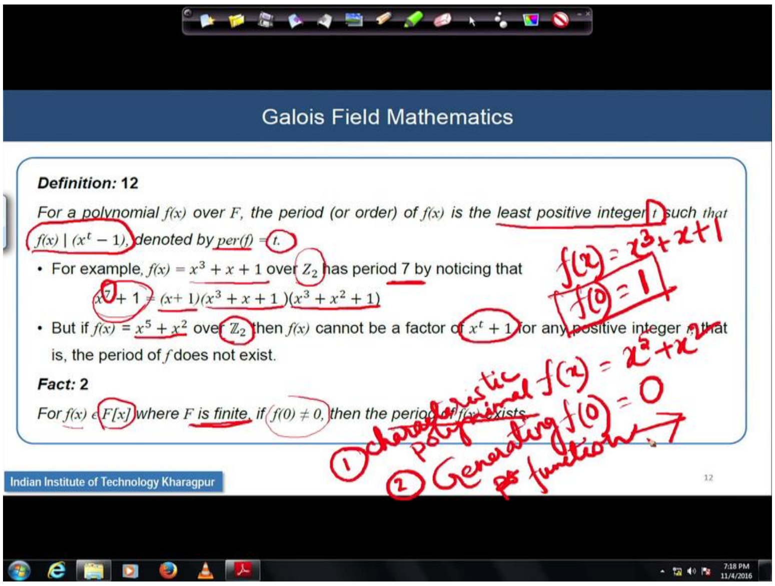
An element $b \epsilon F$ is called a root (or zero) of the polynomial $f \epsilon F[x]$ if $f(b) = 0$.

Indian Institute of Technology Kharagpur

So, if it is having the positive degree I can express it in this form. What is this a? A is a polynomial which belongs to capital a and a belongs to capital F and p 1 to pk these are the distinct monic irreducible polynomials. Monic irreducible poly polynomials mean monic means all the coefficients of those polynomials are equal to 1, and each of these polynomials are irreducible further. And these are all the positive integer values, and if this is the situation then this factorization unique apart from the order in which the factors occur.

So, this is the called the unique factorization. The rule of unique factorization and remember any element b now that belongs to the f, we will call that a root or 0 of the polynomial, if and only if the f of b gives you equal to 0.

(Refer Slide Time: 20:44)



Galois Field Mathematics

Definition: 12

For a polynomial $f(x)$ over F, the period (or order) of $f(x)$ is the least positive integer t such that $f(x) \mid (x^t - 1)$, denoted by $per(f) = t$.

- For example, $f(x) = x^3 + x + 1$ over Z_2 has period 7 by noticing that

  $x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$

- But if $f(x) = x^5 + x^2$ over $\mathbb{Z}_2$ then $f(x)$ cannot be a factor of $x^t + 1$ for any positive integer t, that is, the period of f does not exist.

Fact: 2

For $f(x) \in F[x]$ where F is finite, if $f(0) \neq 0$, then the period of $f(x)$ exists.

$f(x) = x^3 + x + 1$

$\boxed{f(0) = 1}$

$f(x) = x^5 + x^2$

$f(0) = 0$

① characteristic polynomial

② Generating function

Indian Institute of Technology Kharagpur

12

7:18 PM
11/4/2016

So, to define a root of a polynomial we have to find out actually the function that polynomial with that value typically should raise the value equal to 0. So, now, we are actually in a situation to define a polynomial f x over a field F and define it is periodicity. Suppose we are having a polynomial f x and we are really interested to find the period of it. Period means it is order of f x with the at some least positive integer. Suppose they have least positive integer here the point of our consideration is the least positive integer here is denoted as t, such that this polynomial f x given by my x to the power t minus 1, will be denoted and we will denote this period of f which is equal to t.

So, what is the meaning of that. The period is something that if t is such a number a positive integer, such a p such a number that so, that this polynomial will be divisible by x to the power t minus 1. Then we can say that the period of that polynomial is equal to t we will test it. Suppose we have a polynomial given by x 3 plus x plus 1, and it is it belongs to the it belongs to Z 2. It is the group Z 2 and it has a period 7.

How will you define that it has a period 7? Because if I take up the period, if I take polynomial as x to the power 7 plus 1, and this x to the power 7 plus 1 can be expressed n form of x plus 1, x cube plus x, plus 1 and x cube x square plus 1. You please continue the multiplication of the right hand side and check whether you can come back to the polynomial x to the power 7 plus 1 or not at home. And once this is the case then we can really think that the target polynomial x to the power cube plus x plus 1, definitely it is divisible by this x to the power 7 plus 1, generally these 2 other polynomials. So, definitely then 7 is a period of this polynomial x to the power cube plus x plus 1. And, but remember we if we take another polynomial who is having x to the power 5 plus x square, who is also actually having the existence over Z 2 the group z 2 and the ring Z 2 also.

And then f x cannot be factor of this x t plus 1 for any positive integer of t. So, if you cannot find any positive integer of say t, for which actually the polynomial it can be divisible it can divide it with some constituting some polynomial with that integer value t, then we cannot find that actually that target polynomial is having any period over that. It does not have any period and there is no period hence we declare that no period exists for that typical polynomial. For my any polynomial f x to that belongs to the field f, where f is if it is a finite field and, then f 0 which is not equal to 0 if there is the situation then definitely there will be a period of for x. So, immediately to check if we are getting a f 0 equal to 0 or not. Will give you the answer whether the period exist. And then the second task is to find out our typical integer value t for that typical polynomial so that you can find out the period of it.

So, for example, if we can apply this formula apply this logic on the expression of this f x that we have seen earlier. Which actually equal to x to the power 5 plus x square, putting the value of f equal to 0 there we will find that the right hand side will be completely 0 which proves that actually for this polynomial we will be never be able to find any period of it. So, before searching for any period searching for such integers which can be a period of a given polynomial; please do this check. For another one like this f x which is equal to my x cube plus x plus 1, then in such situation we will be able to see that if I put f equal to x equal to 0 there we are ending up with the value equal to 1.

So, it proves that definitely you should search for some positive integer for which this polynomial will be periodic polynomial which will have a period of it. And hence such will have to some searching you will be able to get this. So, with these we will be we are ending with the Galois field mathematics and it is fundamentals understanding which gives us a complete journey to understand financial either set then the binary operation of on a set.

What is the meaning of the algebraic structure of group, and then from group we learnt what exactly is the ring to field and finally, what does the meaning of polynomial over that field? Fundamentally we will use mostly this concept of polynomial and the polynomials over the field for the generation of the code architecture, and for the generation of the code and the code architecture we will try to understand what does the characteristic polynomial and what is the generating function for all our linear feedback shift register based codes in the next few lectures. And remember actually with respect to the Galois field mathematics these are the most 2 important terms that we will be introducing in in context of the code generation. One is actually our characteristic polynomial and second one will be my generating function.

Remember the characteristic polynomial is a very critical one, who will be generating function. This characteristic polynomial should be able to develop the generating function where we will see later on that the characteristic polynomial actually is a divisor of some other polynomial, if it can be structured like that. If we can find out the characteristic polynomial and it if it is finding out it is a divisor of some other polynomial of the lsfr structure. Then the generating function can be generated which can give.

Finally, give rise to a would say particular code, from the random sequence code generated from the form that lsfr structure. So, let us wait for the next 2 modules to come up and where we will go in detail of this characteristic polynomial we will see in detail.