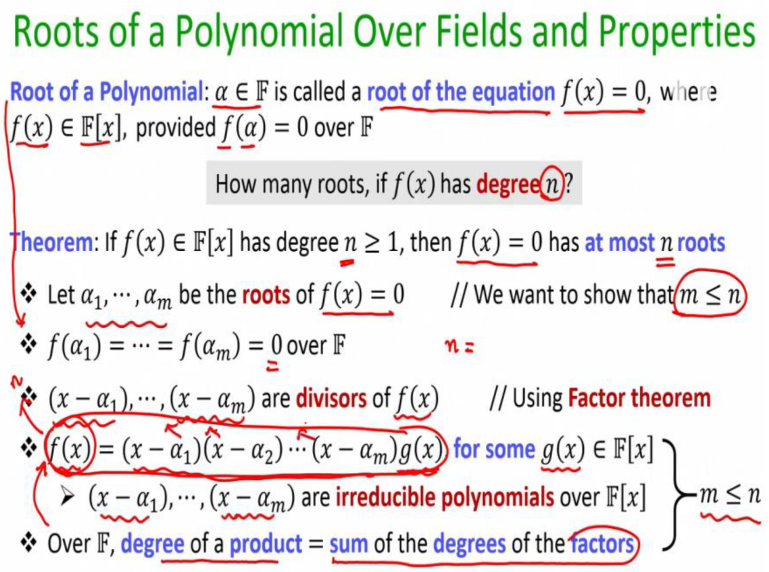


Roots of a Polynomial Over Fields and Properties

Root of a Polynomial: $\alpha \in \mathbb{F}$ is called a **root of the equation** $f(x) = 0$, where $f(x) \in \mathbb{F}[x]$, provided $f(\alpha) = 0$ over $\mathbb{F}$

How many roots, if $f(x)$ has **degree** n?

Theorem: If $f(x) \in \mathbb{F}[x]$ has degree $n \geq 1$, then $f(x) = 0$ has **at most n roots**

❖ Let $\alpha_1, \cdots, \alpha_m$ be the **roots** of $f(x) = 0$ // We want to show that $m \leq n$

❖ $f(\alpha_1) = \cdots = f(\alpha_m) = 0$ over $\mathbb{F}$ $n =$

❖ $(x - \alpha_1), \cdots, (x - \alpha_m)$ are **divisors** of $f(x)$ // Using **Factor theorem**

❖ $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) g(x)$ **for some** $g(x) \in \mathbb{F}[x]$

➢ $(x - \alpha_1), \cdots, (x - \alpha_m)$ are **irreducible polynomials** over $\mathbb{F}[x]$

❖ Over $\mathbb{F}$, **degree** of a **product** = **sum** of the **degrees** of the **factors**

$m \leq n$

Now based on this factor theorem what we define is the root of a polynomial. So, a value α from the field will be considered as the root of this equation f(x) = 0 where f(x) is a polynomial over the field provided the polynomial evaluated at α gives you the value 0 over the field. So, again this is kind of a generalization of the notion of roots that we are familiar with.

Now the next question is that how many roots I can have if my polynomial has degree n, so I can prove a familiar result. So, we know that for the regular polynomials if we have degree n then it can have at most n roots in the same way I can show that if my polynomial is over a field then this equation f(x) = 0 can have at most n roots how do we prove this? So, imagine that α_1 to α_m are the roots of your equation f(x) = 0.

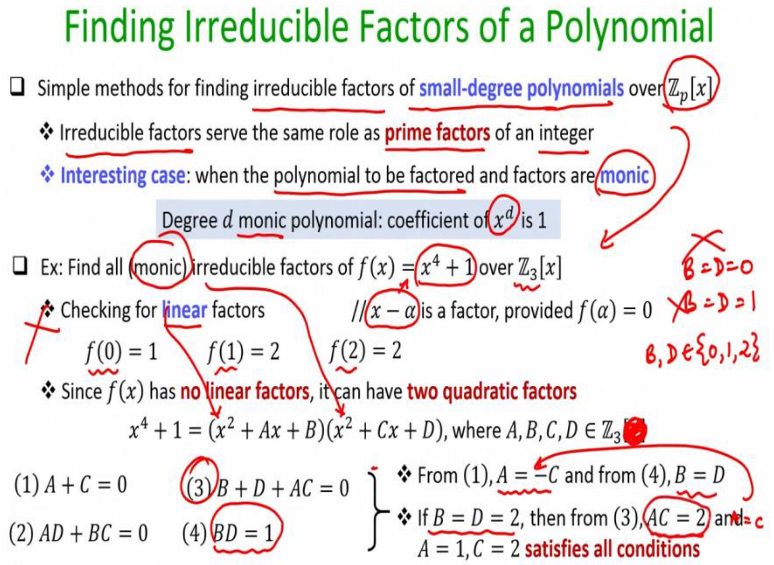
And we want to show that m is less than equal to n upper bounded by n that is my goal. Now as per the definition of a root since α_1 α_2 each of them is a root I know that the f polynomial evaluated at α_1, f polynomial evaluated at α_2, f polynomial evaluated at α_m all of them will give you the value 0 over the field. And if they give the value 0 over the field that means I can say that each of these polynomials as per the factor theorem are divisors of my polynomial f(x).

That means I can say that I can write down my f(x) polynomial as the product of these m individual degree 1 polynomials followed by some leftover polynomial g(x) where g(x) could be some polynomial over the field. And an important thing to notice here is that each of these polynomials (x - α1), (x – α2), (x – αm) they are irreducible polynomials because they are already any how polynomials of degree 1.

And they are non constant polynomials and I also know that over a field if I multiply several polynomials then the resultant polynomial will have a degree which is actually the sum of the degrees of the individual factors. This is possible over a field but this is not true over a ring we already proved that. So, now if I apply this fact over this statement.

I know that the degree of f(x) is n. And I know that this f(x) is definitely at least a product of m factors plus there is something else as well g(x) is another additional factor. So, the degree of f(x) is n that is given to me and since it is the product of at least m factors, I can say that definitely n is greater than equal to m which is what I wanted to show because each of these factors contribute 1 to the overall degree of f(x) which is n.

(Refer Slide Time: 45:59)



Finding Irreducible Factors of a Polynomial

- ❑ Simple methods for finding irreducible factors of small-degree polynomials over $\mathbb{Z}_p[x]$
  - ❖ Irreducible factors serve the same role as prime factors of an integer
  - ❖ Interesting case: when the polynomial to be factored and factors are monic

Degree d monic polynomial: coefficient of x^d is 1

- ❑ Ex: Find all (monic) irreducible factors of $f(x) = x^4 + 1$ over $\mathbb{Z}_3[x]$
  - ❖ Checking for linear factors // $(x - \alpha)$ is a factor, provided $f(\alpha) = 0$

$f(0) = 1$ $f(1) = 2$ $f(2) = 2$

  - ❖ Since $f(x)$ has no linear factors, it can have two quadratic factors

$$x^4 + 1 = (x^2 + Ax + B)(x^2 + Cx + D), \text{ where } A, B, C, D \in \mathbb{Z}_3$$

(1) $A + C = 0$ (3) $B + D + AC = 0$

(2) $AD + BC = 0$ (4) $BD = 1$

- ❖ From (1), $A = -C$ and from (4), $B = D$
- ❖ If $B = D = 2$, then from (3), $AC = 2$ and $A = 1, C = 2$ satisfies all conditions

$B = D = 0$

$B = D = 1$

$B, D \in \{0, 1, 2\}$

$= c$

So, now the next thing is; next question is how exactly we find irreducible factors of a polynomial how exactly we do the factorization. So, it turns out that we do have some simple methods for finding irreducible factors for the special case where my polynomials are over $\mathbb{Z}_p[x]$ and where my polynomials are of small degrees. And if you are wondering what exactly is the whole purpose of finding out the irreducible factors basically the problem is something similar to finding the prime factorization of an integer.

So, you are given an integer you want to factorize it in the same way you are given polynomial and say if it reducible I want to find out its irreducible factors. So, there are some well known methods for that we will discuss one of the methods for a special case when the polynomial that we want to factor is a monic polynomial as well as the factors which we want to find out they are also monic.

By the way what is a monic polynomial? A polynomial is called as a monic polynomial and degree d if the coefficient of x^d is 1. So, now let us see this method, by the way this method is mechanical and it will work only when your polynomial is of small degrees. So, suppose this polynomial (x^4+1) is given to me and I already showed you the factors of this polynomial but now let us try to find it out.

So, if at all this polynomial has a factor it will have either linear factors; it will have several linear factors possible or it can have 2 possible quadratic factors or it can have 1 linear factor and 1 cubic factor and so on these are the various possibilities because the degree of f(x) is 4. So, now let us check for linear factors that means can I write f(x) as product of some $(x – \alpha)$ and another polynomial where α is some element from $\mathbb{Z}_3$.

So, remember that if at all $(x – \alpha)$ is a factor of this f(x) then this f(x) polynomial evaluated at α should give me the value 0. So, let us check whether α can be 0 or not or α can be 1 or not or α can be 2 or not why only these 3 values? Because everything is allowed to be from $\mathbb{Z}_3$. Now it turns out that neither f(0) nor f(1), nor f(2), is 0 by the way all the operations are performed over $\mathbb{Z}_3$ namely all the addition and multiplications are modulo 3.

That means I can rule out the possibility of linear factors. Now since linear factors are not possible the next thing that we I want to check is whether it can have 2 quadratic factors possible. Now if at all it has quadratic factors it can have 2 quadratic factors. So, let me write down it in the form of 2 quadratic factors and remember I am interested to find out the monic factors so that is why one of the monic quadratic factors I am writing like this $(x^2 + Ax + B)$.

And another unknown monic quadratic factor I am writing like this $(x^2 + Cx + D)$; my goal is to find out whether I can find out A, B, C, and D or not. Where A, B, C, D are allowed to be from $\mathbb{Z}_3$ not $\mathbb{Z}_3[x]$. So, now if at all this f(x) polynomial can be expressed as the product of 2 quadratic factors these 4 conditions should be satisfied : (1) $A + C = 0$ (2) $AD + BC = 0$ (3) B

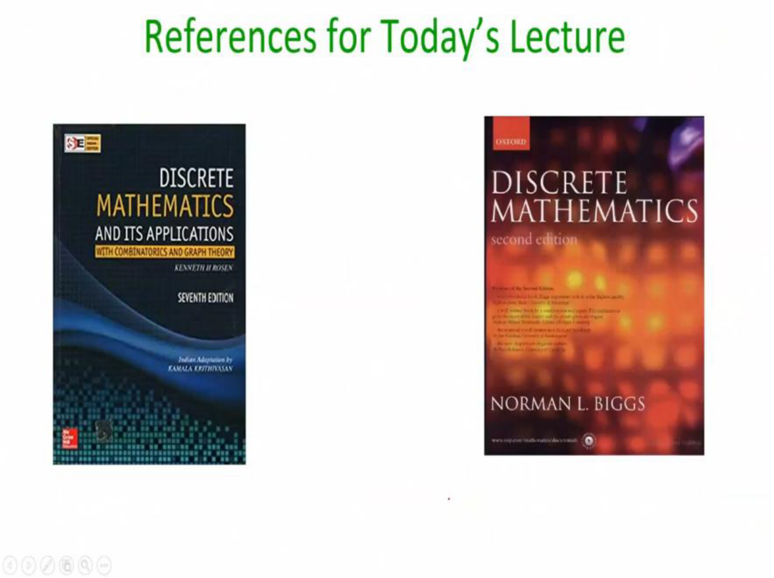
+ D + AC = 0 (4) BD = 1. Why so? Because you see what will be the coefficient of x^3 as per my right hand side? It will be (A + C) x^3.

Because Ax into x^2 will give me A times x^3 and Cx multiplied with x^2 will give me Cx^3. So, the coefficient of x^3 will be A + C and I want that A + C should be 0 because in my left hand side there is no coefficient of x^3 in the same way I am basically just comparing the various powers of x in the LHS and RHS and arriving at these 4 equations. Now I have to check whether I can satisfy all these 4 equations simultaneously given that my A, B, C, D can take values from the set $\mathbb{Z}_3$.

Now from the first equation I can conclude that A should be minus C. And from my fourth equation I can conclude that B should be equal to D why B should be equal to D? Because my B and D are allowed to be only from the set 0, 1, 2. So, B and D are both allowed to be from the set 0, 1, 2. So, I cannot have different values of B and D from this set 0, 1, 2. But when multiplied together and then taken modulo 3 gives me the value 1. So, the only possibility that B, D gives me 1 is when both B and D are 1 or both B and D are 2. Now I can simply rule down the possibility of B = D = 0 that is not allowed because if that is the case B into D cannot be 1. But I cannot have B and D both equal to 1 because a both B and D are equal to 1 then my third equation gives me that product of A and C should be 1.

And then as per the same logic A should be equal to C but that goes against the conclusion that I get from the first equation A = - C. So, I can rule down B and D equal to 1 as well. So, the only option left is check whether B and D can be 2 and if B and D and are 2 then as per the equation 3 I get AC should be equal to 2. And if AC = 2, I can satisfy it by saying that A = 1 and C = 2 and that does not violate this condition that A = - C.

(Refer Slide Time: 52:51)



References for Today's Lecture

DISCRETE MATHEMATICS AND ITS APPLICATIONS
WITH COMBINATORICS AND GRAPH THEORY
KENNETH H ROSEN
SEVENTH EDITION
Indian Adaptation by KAMALA KRITHIVASAN
OXFORD
DISCRETE MATHEMATICS
second edition
NORMAN L. BIGGS

That means I can now safely say that A = 1, B = 2, C = 2, D = 2 satisfies these condition and hence I can factorize my $x^4 + 1$ as product of 2 quadratic monic factors with that I conclude today's lecture. Thank you.