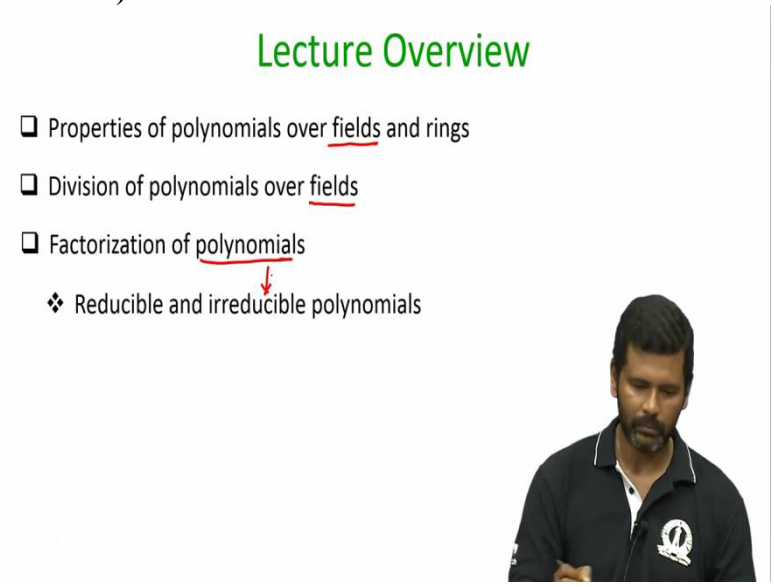
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology - Bangalore

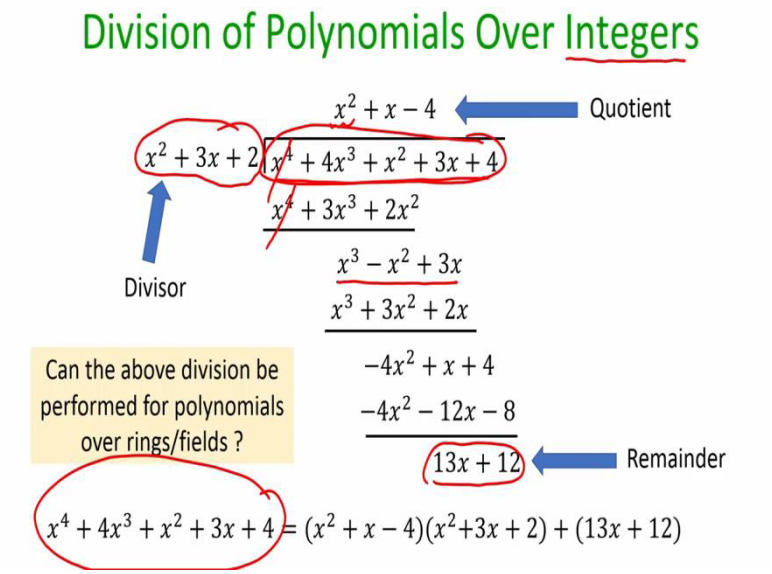
Lecture - 67
Polynomials Over Fields and Properties

(Refer Slide Time: 00:26)



Hello everyone, welcome to this lecture so, in this lecture we will continue our discussion on polynomials over rings. And we will see in this lecture, polynomials over fields and we will also discuss about how to divide polynomials over fields. And we will also discuss about factorization of polynomials using which we will define the notion of reducible and irreducible polynomials.

(Refer Slide Time: 00:52)



So, let us start with the usual division of polynomials that we are familiar with. So, if I consider 2 arbitrary polynomials where the coefficients are integers and we are my plus and

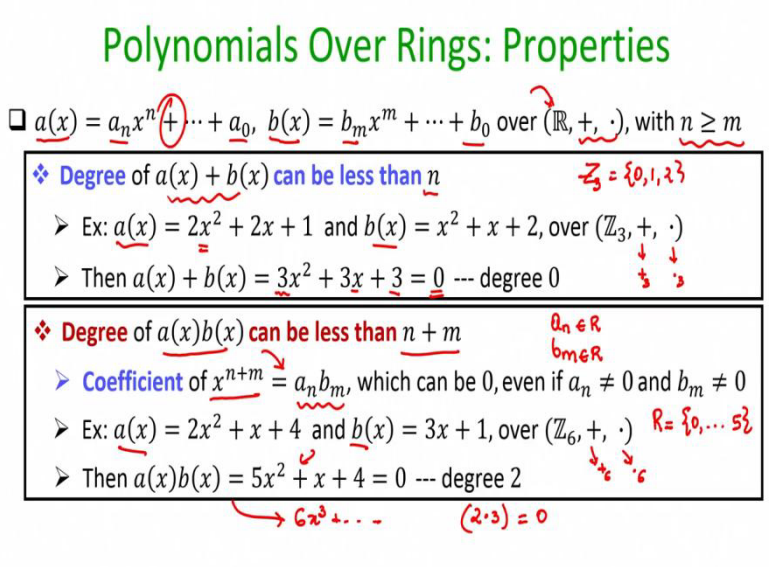
dot operations are the usual integer addition and integer multiplication then this is the way we perform the division. So, you will be given a divisor and you will be given a number which you want to divide.

And then what we do is basically say in this example my power is currently x^4 my divisor has x^2. So that is why I try to multiply my divisor with something so that I can get something of the form x^4 so that x^4 and x^4 cancels out and whatever is left that will be treated as my next value or the next thing which I want to divide. So, in each step basically we are slowly and slowly and slowly trying to reduce the power of the number which I want to divide.

And I keep on doing this till I cannot do anything further in the sense that the remainder that I obtain is a polynomial whose degree is less than the degree of my divisor. If I reach that stage then I cannot proceed further. And then I can say that safely that the number which I wanted to divide; that my original number is basically the product of divisor and quotient plus some remainder. That is the usual way of performing division of polynomials over the integers.

Now the interesting question here is the following in the last lecture we have defined or we have extended the notion of polynomials to rings and we have seen how to do addition of polynomials over rings which are more or less similar to the way we perform addition and multiplication of polynomials over the integers. What about the division operation? Can we do something similar for polynomials which are defined over rings or fields.

(Refer Slide Time: 03:04)



So, for that again let us recall the definition of polynomials over rings and further explore some more properties regarding the polynomials over rings. So, imagine you are given 2 arbitrary polynomials over an abstract ring $\mathbb{R}$. That means all your coefficients a_n, a_{n-1}, a_0, b_m, b_{m-1}, b_0 are elements of this set $\mathbb{R}$. And all this plus and dot operations are your ring plus and dot operations.

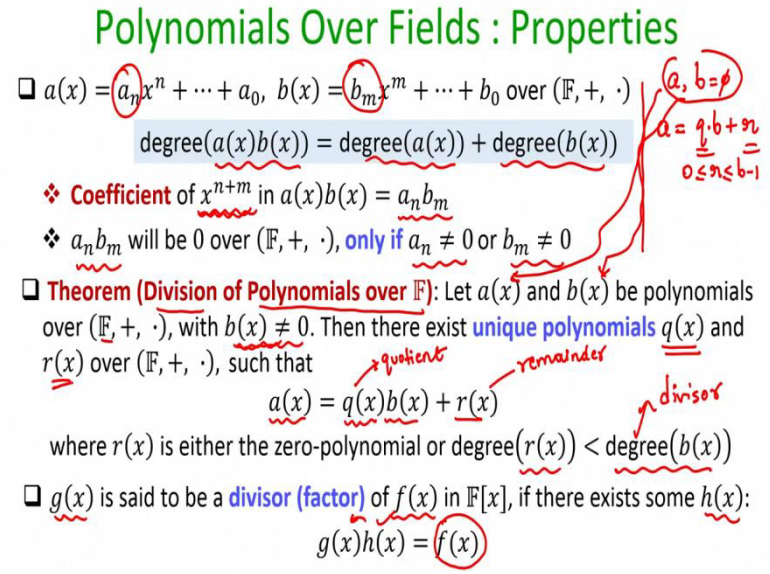
Now as we have demonstrated in our last lecture itself it might be possible that the summation of a(x) and b(x) has a degree which is less than n even if your n >= m it might be possible that when you take the summation of these 2 polynomials the resultant degree is less than n, that is quite possible. So, again to demonstrate my point let us take these 2 polynomials a(x) and b(x) over, where the coefficients are elements of the set 0, 1, 2.

And this plus operation is plus modulo 3 and this dot operation is multiplication modulo 3. And if these are my a(x) $(2x^2 + 2x + 1)$ and b(x) $(x^2 + x + 2)$ polynomial then the coefficient of x^2 will be 2 + 1 and 2 + 1 will be 3 and 3 modulo 3 will be 0; in the same way the coefficient of x will be 0 the constant coefficient will be 0. So, even though a(x) and b(x) none of them is numerical is 0, the 0 polynomial, in this case the summation of these 2 polynomials actually turns out to be a 0 polynomial. In the same way if I multiply 2 polynomials over rings then again it is not necessary that its degree will be exactly n + m which is the case if I multiply 2 integer polynomials but when I multiply 2 ring polynomials that may not be the case because the coefficient of x^{n+m} when I do multiplication of ring polynomials will be this value $a_n b_m$, and now since my a(n) is an element of the ring and my b(m) is also an element of the ring it might be possible that neither a(n) nor b(m) are 0 elements but still their product is a 0 element, this is quite possible if you are taking the coefficients over the ring remember this is not possible over a field. In a field if the product of 2 elements is a 0 element and definitely 1 of them has to be 0 but that may not be the case in a ring again let me demonstrate this.

So, my ring $\mathbb{R}$ here is set $\mathbb{Z}_6$ namely the elements 0 to 5 and of course my plus operation is plus modulo 6 and my dot operation is multiplication modulo 6 then what can I say about the product of these 2 polynomials $(2x^2 + x + 4)$ $(3x + 1)$. So, if I consider the coefficient of x^3 the coefficient of x^3 will be $6x^3$ but what will be 6? So the coefficient of x^3 will be basically 2 into 3 where this into is multiplication modulo 6 and 2 multiplied with 3 modular 6 is basically 0.

So, the coefficient of x^3 vanishes and now you can see that the degree of the product polynomial here is less than the summation of the degrees of a(x) and b(x) polynomial.

(Refer Slide Time: 07:11)



Now, what we can say about the addition of polynomials and multiplication of polynomials over fields? So, we can extend the definition of polynomial addition and multiplication that we have given for rings to fields as well because remember fields after all is a special type of ring. Now in a field we can definitely say that the degree of the product polynomial will be exactly equal to the sum of degree of the individual polynomials.

Which was not the case if I perform the multiplication of polynomials over rings we have already demonstrated that; this is because now the coefficient of x^{n+m} in the product polynomial will be the product of a_n and b_m. And remember in the last lecture we proved that the product of a_n and b_m can be 0 only if a_n was 0 or b_m was 0 that means you are at the first place your polynomial a(x) was not of degree n or your polynomial b(x) was not of degree m.

It can never happen that even though your a_n and b_m are both non 0 but still when you multiply a_n and b_m over a field you get a 0 element that is not possible that is why the coefficient a_n times b_m will survive. And that is why the x term with x^{n+m} will be present in your product polynomial. Now based on this observation we can give a theorem regarding the division of polynomials over a field.

And this is kind of generalization of your usual division property. What do we mean by the usual division property? We know that in the integer world if you are given 2 arbitrary integers a and b then I know; that of course where b is not 0. And I know that I can always express a in the form of some quotient times b plus some remainder r where the remainder r will be in the range 0 to b - 1. That is the usual divisibility theorem with respect to the integers.

We are now trying to extend that property that theorem in the context of polynomials over fields so you can interpret that now a is replaced by a polynomial. It is no longer just a single value but rather it is a polynomial where the quotients of the polynomial are from some field. In the same way your element b; the number b; is now generalized to a polynomial of some degree. And similar to the case of divisibility property that we have in the integer world where b is not allowed to be 0 because division by 0 is not well defined.

So that is why we are not allowing b(x) to be 0 here then this theorem basically says that you can express your a(x) as some quotient times divisor plus some remainder namely some quotient polynomial times your divisor polynomial plus some remainder polynomial where the degree of your remainder polynomial will be strictly less than the degree of your divisor polynomial.

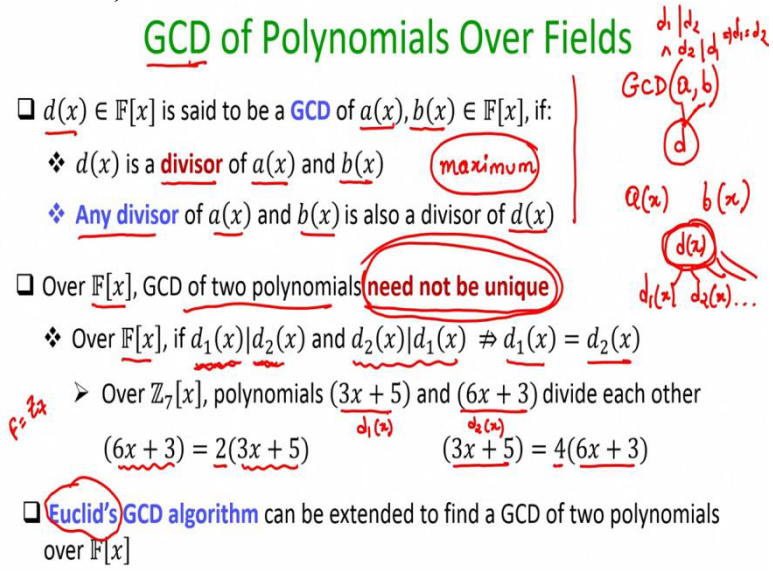
So, this is your divisor polynomial, q(x) is the quotient polynomial and r(x) is your remainder polynomial. Again we can prove this very easily but due to interest of time I am not going to prove that and the interesting part of the theorem here is that the quotient and the remainders will be unique here similar to the case of integer division. If you divide a by b you get a unique quotient and a unique remainder where the remainder is in the range 0 to b - 1.

Now if my remainder turns out to be 0 then I will say that a(x) is completely divisible by b(x) or in some sense b(x) is a divisor or factor of your a(x) so in other words consider a polynomial g(x) I will say that g(x) is a divisor of f(x) if f(x) is completely divisible by g(x) that means you get no remainder that means if you get a remainder but that remainder is actually a 0 polynomial.

In other words there exists some polynomial h(x) over the field which when multiplied with your g polynomial will give you the polynomial f(x) if that is the case then I will say g(x) is a

factor of your f(x) polynomial, of course if g(x) is a factor of f(x) polynomial then so is h(x) polynomial.

(Refer Slide Time: 12:39)



So, once we have given the definition of division of polynomials over field the next thing that we want to define is the GCD of polynomials over field. So, again this will be a generalization of the GCD of 2 numbers that we had discussed earlier in our module on number theory. So, d is said to be the GCD of a and b it if it is the greatest common divisor of both a and b; in the same way imagine you are given 2 arbitrary polynomials a(x) and b(x) over the field then another polynomial d(x) over the field will be considered as the GCD of these 2 polynomials and the following 2 properties are satisfied. Of course the d(x) polynomial has to divide both the a(x) polynomial as well as the b(x) polynomial because after all it is a common divisor and it is greatest in the sense that you take any divisor of a(x) and b(x) it is also a divisor of d(x) in that sense you can imagine that d(x) is actually kind of a maximal possible common divisor of both a(x) and b(x).

So, pictorially you can imagine that you are given a(x) polynomial b(x) polynomial and there can be multiple common divisors of both these 2 polynomials call them $d_1(x)$, $d_2(x)$ and so on. Among all those common divisors you can interpret that there is another divisor d(x) which is kind of sitting on top of the hierarchy in the sense that all these divisors $d_1(x)$, $d_2(x)$, $d_3(x)$, $d_n(x)$ they also divide d(x) in that sense d(x) is sitting at the top of the hierarchy among all the common divisors of a(x) and b(x).

And that sense it is the maximal possible common divisor of a(x) and b(x). The reason we are defining GCD in this sense is because we cannot define what we call as maximum when we are considering polynomials over the fields. So, again in the case of integer GCDs where we are given 2 integer values a and b, d was the GCD in the sense it has the maximum possible common divisor there is no other common divisor whose value is more than d.

There the notion of more is very well defined but when it comes to polynomials over field I cannot define that d(x) is the maximum possible common divisor of a(x) and b(x). I cannot define a notion like maximum common divisor polynomial; this is because it turns out that if I consider polynomials over fields then the GCD of 2 polynomials need not be unique at the first place. And that is why you can have multiple possible GCDs of 2 arbitrary polynomials.

This is because if I consider polynomials over fields and if you are having a situation where you have 2 divisor polynomial say $d_1(x)$ is a common divisor of both a(x), b(x) and so is the $d_2(x)$ polynomial that is also a common divisor of both a(x) and b(x) and say the divisor polynomial d_1 divides d_2 and say d_2 is a divisor of d_1 then I cannot conclude that the polynomials $d_1(x)$ and $d_2(x)$ are same.

And this is not the case in the usual integer world. In the usual integer world I know that if there is a number d_1 which divides d_2 and if it is the case that d_2 divides d_1 as well then I can conclude that d_1 and d_2 are the same numbers; but when I consider polynomials over fields and if I have 2 polynomials where the first polynomial divides the second polynomial and the second polynomial divides the first polynomial I cannot necessarily conclude that both polynomials are identical.

So, for instance if I consider the field $\mathbb{Z}_7$ namely my elements are 0 to 6 and my operations are addition modulo 7 and multiplication modulo 7 and suppose I take these 2 polynomials (3x + 5) and (6x + 3). It turns out that these 2 polynomials divide each other because if you divide 6x + 3 by 3x + 5 you will get the quotient polynomial 2 which is the constant polynomial and 0 remainder whereas if you divide 3x + 5 by 6x + 3 you will get the quotient polynomial 4 and 0 remainder, this is your $d_1(x)$ and this is your $d_2(x)$.

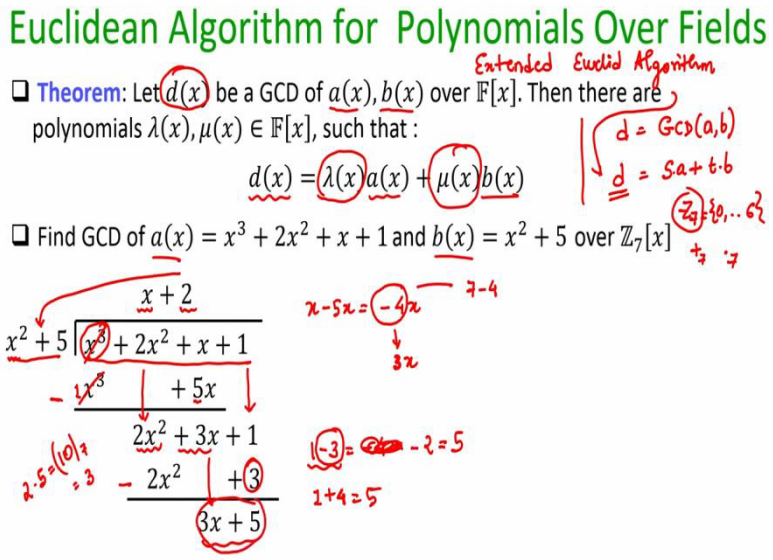
But you can see here that even though d_1 divides d_2, d_2 divides d_1 they are different polynomials and that means if say for instance both 3x + 5 as well as 6x + 3 are common

divisors of a(x) and b(x) then it can be very much possible that 3x + 5 as well as 6x + 3 are both GCD of a(x) and b(x), that is possible. That means I cannot say that when I consider polynomials over fields that I will have unique GCDs you can have multiple possible GCDs.

And this is unlike GCDs over integers so that is why I cannot define what I call as a maximum possible polynomial which is a common divisor polynomial of both a(x) and b(x). That is why I define what I call as maximal. You take any divisor of a(x) and b(x) it will be a divisor of your d(x). Now once we have defined GCD of polynomials of over field and next question is how do we find out?

And it turns out that the beautiful Euclid's GCD algorithm that we had discussed in our module on number theory it can be extended to even find GCD of 2 polynomials namely the GCD algorithm based on repeated division. The same algorithm if I extend to the case of polynomial, if I just extend it will work and it will give you GCD of 2 polynomials defined over the fields.

(Refer Slide Time: 20:03)



In fact we can get what we call as the extended Euclid GCD algorithm for polynomials over fields and find out what we call as Bezout coefficients which we had seen in our module on number theory. So, remember if d is the GCD of 2 integer values a and b then the Bezout's theorem says that I can always find out linear combiners s and t such that integer linear combiners such that s times a + t times b is actually your GCD d.

That means GCD is always; I can always express GCD as the linear combination of my 2 numbers a and b itself and we know how to find out this Bezout's coefficients using the extended Euclid algorithm. The same theorem holds even for the case of polynomials over fields. So, basically what the theorem says here the following: if you are taking 2 polynomials over the field and say d(x) is one of the GCDs, again remember there can be multiple GCDs possible.

So, if d(x) is one of the GCDs then I can always find out the corresponding Bezout's polynomials. So, you can find out this combiners $\lambda(x)$ and $\mu(x)$ which will be now polynomials because now everything is extended to polynomials such that your GCD can be expressed as a combination of your original polynomial say a(x) and b(x) where the combiners will be your $\lambda(x)$ polynomial and $\mu(x)$ polynomials.

So, I would not be going into the exact details of how to find out this Bezout's coefficients and how to find out the GCD's but I will work out an example here. So, say for instance I want to find out the GCD of this a(x) ($x^3 + 2x^2 + x + 1$) and b(x) ($x^2 + 5$) polynomials where all the operations are performed over $\mathbb{Z}_7$. So, $\mathbb{Z}_7$ has all the elements from 0 to 6 and my plus operation will be addition modulo 7, my multiplication operation will be multiplication modulo 7.

So, what we do in the GCD algorithm: we take the higher number and divide it by the smaller number but the numbers now here are the polynomials. So, we will take the polynomial with the higher degree and divide it by the polynomial with the lower degree. So, this is my a(x) this is my current a and this is my current b. And now you can see the way I am performing the division here, it is something similar to the way we perform division over the integers.

But instead of all the operations being performed over integers, the operations will be performed over $\mathbb{Z}_7$. So, for instance my current power here is x^3 and my divisor has the highest power x^2 so that is why I am putting an x here if I multiply x with $x^2 + 5$, I will get x^3. The coefficient here will be 1, 1 modulo 7 will be 1 and 5 into x. So, coefficient here will be 5, 5 modulo 7 will be 5.

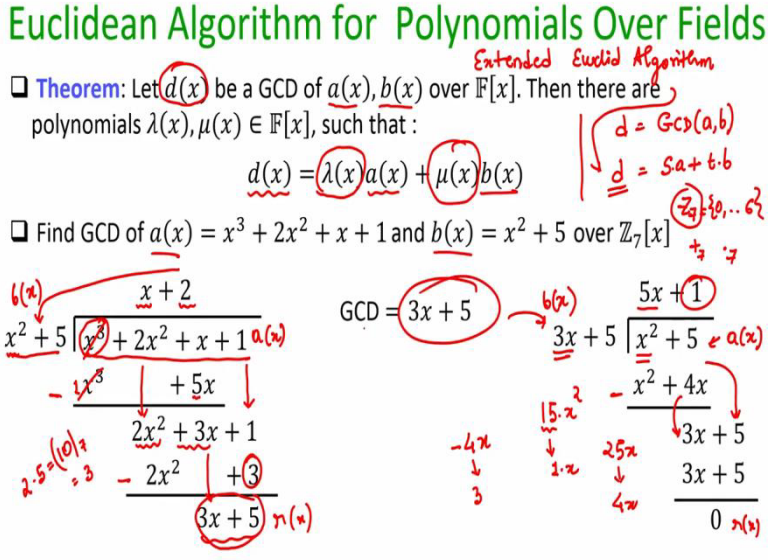
Now I have to take the difference here. I have to subtract so x^3 and x^3 cancels out $2x^2$ is taken as it is here. And now what will happen if I subtract 5x from x so x - 5x will be -4x.

But there is no -4. -4 in this field $\mathbb{Z}_7$ will be treated as +3 because by -4 I mean 7 - 4. Basically I am talking about because remember all the operations are plus mod 7, and all the multiplication operation are multiplication modulo 7. So that is why -4x will be treated as +3x so that is why will have +3x and this +1 will be retained as it is. Now I have to take care of this $2x^2$ so that is why I take my next term in the quotient as 2 so if I now multiply 2 with $x^2 + 5$, 2 times x^2 will be retained as it is whereas 2 into 5 will be 10 but 10 modulo 7 will be 3.

So that is why this is 3 this is not 10 and now I will be taking the difference here. So, 3 of x retains goes as it is now 1 - 3 will be -2 and -2 will be treated as 7 - 2 namely 5. If you are wondering how exactly we are getting this so -3 is basically +4. And 1 + 4 is 5, -3 in this field $\mathbb{Z}_7$ is +4 and +4 and +1 modulo 7 will be 5 so that is why I get 3x + 5.

And now you can see that the degree of 3x + 5 is less than the degree of my divisors. So, this will be treated as my remainder and I cannot proceed further. So, this will complete the first iteration of your Euclid GCD algorithm.

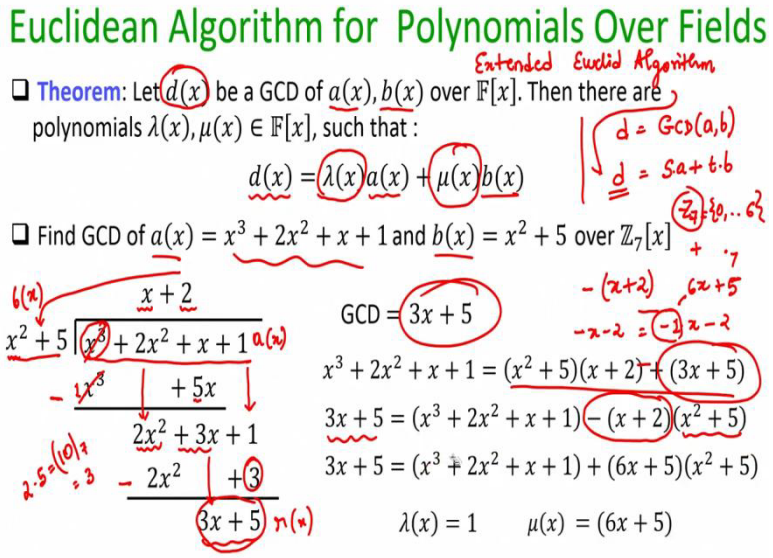
(Refer Slide Time: 26:15)



So, this was my b(x) this was my a(x) and this is my r(x). In the next iteration my b(x) becomes a(x). And my remainder becomes the next b(x) and now you can see that if I perform the division. Here my highest term is x^2 here it is 3x. So, if I multiply 3x with 5x I will get $15x^2$ but this coefficient 15 has to be reduced modulo 7, 15 modulo 7 will be 1 so $1x^2$ which is what I want to cancel out x^2.

So that is why I multiply with 5x and 5x with 5 will give you 25x. Now this 25 has to be reduced to modulo 7 so it becomes 4 so 4x so that is why I get 4x. Now if I subtract 5 goes as it is and I will get -4x. Now this coefficient -4 modulo 7 will be +3 so that is why -4x goes and becomes +3x. And now 3x + 5 is completely divisible by your divisor. If I put 1 as the next term in my quotient so, I get my remainder polynomial r(x) which is now a 0 polynomial. And that is why now I can say that my GCD is 3x + 5.

(Refer Slide Time: 27:54)

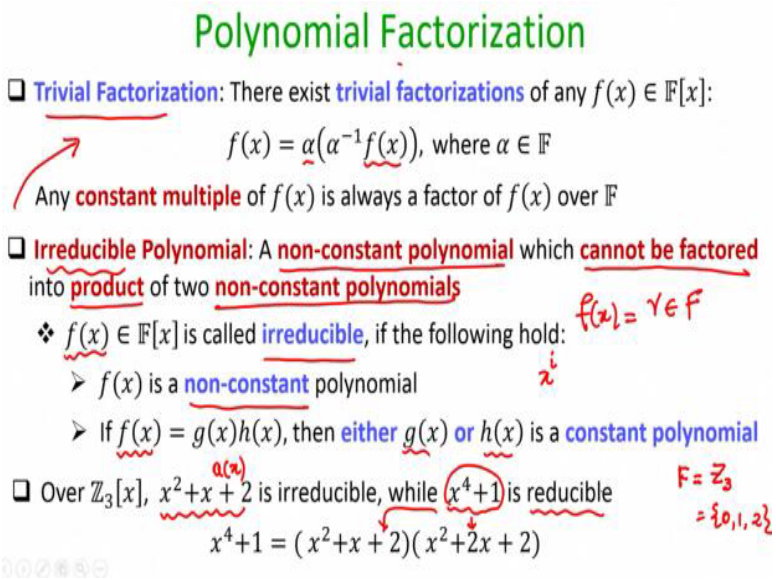


Now if I want to find out the corresponding Bezout polynomials for this GCD I can do the following. So, I can say that if I take my original a(x) in terms of divisors, quotients and remainder; I can write my a(x) in this form. And my goal is to express my GCD in terms of a(x) and b(x) polynomial. So, I can write down my GCD here and the remaining things I take to the left hand side I get this expression.

And now what I can do here is the following: I can say that this is my a(x) ($x^3 + 2x^2 + x + 1$) and this is my b(x) ($x^2 + 5$). So, I can treat my λ(x) to be the constant 1. And I can treat my μ(x) to this value, so I can say that my λ(x) is the polynomial 1 and my μ(x) is the polynomial –(x + 2) but wait –(x + 2) is -x -2 but -x means the coefficient is -1 times x and -2. So -1 is not there in $\mathbb{Z}_7$ I have to reduce it modulo 7.

So, -1 becomes 6 so it becomes 6x and in the same way -2 goes and becomes +5. So that is why my final Bezout polynomials will be this. That is the way I can find GCD and the corresponding Bezout combiners.

(Refer Slide Time: 29:57)



So, now the next thing that once we have seen polynomial division over the fields and GCD of polynomials we can define what we call as factorization. So, a trivial factorization that is possible for any polynomial is the following form. So, you are given the polynomial f(x), a trivial factorization will be the following: you take any constant from the field and you take that constant α multiplied with the multiplicative inverse of α of course α is not 0 here.

Otherwise the inverse is not well defined it does not exist. So, if I take any non 0 α from the field and multiply α and α^{-1} with that polynomial f(x) I will get back the original polynomial f(x) itself in that sense I can always say that there is a trivial factorization of f(x) namely α and α^{-1} are trivial factors for any f(x). So, now what we want to define is what we call as irreducible polynomial.

Namely polynomials which cannot be factored into products of lower degree polynomials. That is a rough idea of what we call as irreducible polynomial. So, let us now formally define, so intuitively it is a non constant polynomial which cannot be factored into product of two non constant polynomials. And why we are taking the case that it cannot be factored into product of two non constant polynomials.

Because of this trivial factorization, because if you give me any polynomial f(x) I can always factorize it, I can always say that α and α^{-1} are trivial factors of f(x) but when I am defining irreducible polynomials I am not interested in the trivial factorization so that is why to exclude the trivial factorization I am explicitly putting a condition that the polynomial f(x) should not be factored into the product of non constant polynomials.

So, more formally I take a polynomial over a field I will call it irreducible if the following holds. First that polynomial has to be a non constant polynomial that means it should have some term of the form x^i. It is not a constant polynomial that means it is not of the form say some γ where γ my f(x) is not of the form f(x) equal to some γ where γ is an element of the field that is not the form of f(x).

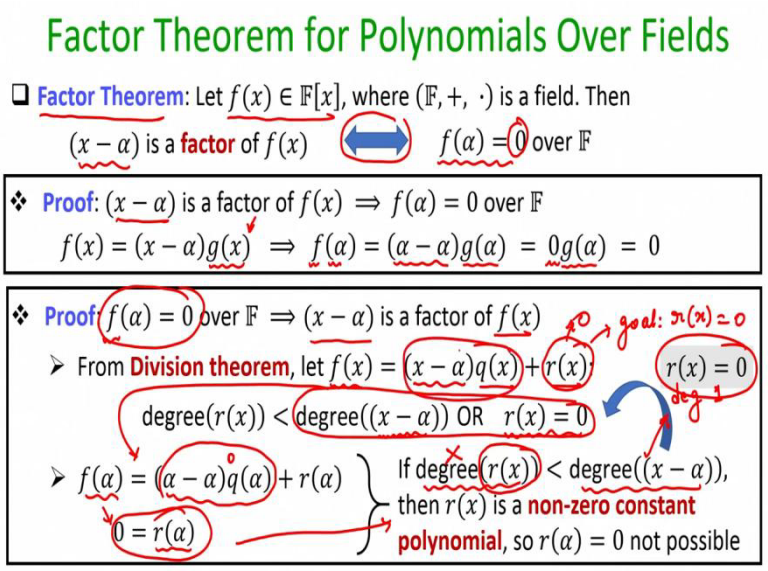
I am not interested in such polynomials when I am defining irreducible polynomials. And the second condition is that I can always decompose f(x) as per trivial factorization. But when I am defining irreducible polynomials my requirement is that I should not be able to write f(x) into the product of 2 other polynomials g(x) and h(x) where either g(x) or h(x) is a constant polynomial because I can always write f(x) in the form of f(x) α into α^{-1}.

And α into α^{-1} can be treated as an element 1. So, I can always say that f(x) = f(x) into 1. So, namely 1 is always a trivial factor of f(x) that is not considered as a violation of this definition. So, my irreducibility property demand here that my f(x) should not be factorized; it should not be possible to factorize f(x) into non trivial factors. If at all it can be factorized only when one of the factors is a constant polynomial that is allowed that would not be considered as a violation of the property of an irreducible polynomial.

So, to give you some examples here if I consider my field to be $\mathbb{Z}_3$ namely the set 0, 1, 2 where all the operations are addition modulo 3 and multiplication modulo 3 and if I consider polynomials over this field then this polynomial $(x^2 + x + 2)$ is irreducible, we can prove that. We will see later how do we show whether a polynomial is irreducible or not.

But you can see, you have to believe me that this is not reducible in the sense I cannot factorize it out into other than the trivial factorization; but this polynomial $x^4 + 1$ is reducible because I can write it in the form of this product of 2 polynomials $(x^2 + x + 2)$ $(x^2 + 2x + 2)$ where none of these 2 polynomials is a constant polynomial. So that is why it is reducible, reducible in the sense it is non trivially factorisable.

(Refer Slide Time: 33:52)



So, the next thing that we want to define is the factor theorem for polynomials over fields. So, the factor theorem states the following. If you take any polynomial over the field then the polynomial (x – α) will be considered as a factor of your polynomial f(x) if and only if the polynomial f(x) when evaluated at x = α gives you the element 0, where 0 is the additive identity.

And since this is an if and only if statement we have to give 2 proofs here we have to give proof both in the forward direction as well as in the reverse direction. So, let us see the proof in the direction where we assume that (x – α) is a factor of f(x), assuming that I have to show that the polynomial f evaluated at x = α will give you 0. So, we will give a direct proof a very simple proof here.

So, since (x – α) is a factor of f(x), that means I can express my f(x) as the product of two polynomials with one of them being (x – α) the remaining thing I can write it as some g(x) polynomial; that means what can I say about the value of the polynomial f evaluated at α that will be same as the product of α - α with the polynomial g(α) but α - α will give you the additive identity 0.

Because -α is the additive inverse of α and 0 multiplied with g(α) will give you 0 element, that is a simple proof. Let us see the proof in the reverse direction. So imagine your polynomial f is such that when evaluated at α gives you 0. If that is the case then I have to show that (x – α) is a factor of f(x). So, I utilize my division theorem and as per the division

theorem I can say that my f(x) when divided by (x – α) will give me some quotient and some remainder. This comes from your division theorem.

And my goal is to show that r(x) is 0 that is my goal. So, how do I show that r(x) is the 0 polynomial well I know that the degree of r(x) polynomial is strictly less than the degree of (x – α) because (x – α) is treated as a divisor here or I know that r(x) = 0. If r(x) is definitely 0 my proof is done because then I show that f(x) is equal to the product of q(x) and (x – α) and (x – α) is a factor of f(x).

But I cannot definitely claim that r(x) is always 0 I have to logically conclude that. So, again if this is the form of f(x) I can say that f(α) will be this. And now I use my premise my premise says that f(α) is 0. So, if f(α) is 0 I substitute this value and this term is anyhow 0. So, I get that r polynomial evaluated at α is 0. And now I can logically argue that indeed if r polynomial evaluated at α is 0 then I get a contradiction to this case.

So, remember my 2 possible cases for r(x) is that either its degree is less than the degree of (x – α) or r(x) is 0. Now if r(x) polynomial has a degree less than the degree of (x – α) polynomial then what can I say about r(x) polynomial. I can say that r(x) polynomial is a constant polynomial because the degree of (x – α) is 1 and if degree of r(x) is less than 1 the only possible degree which is less than 1 is 0.

That means I am actually considering the case when r(x) is a constant polynomial but if r(x) is a constant polynomial then it does not matter whether I evaluate it at α, β I should get the same value. But here I am getting that r polynomial evaluated at α is a 0 value. So these 2 things these 2 conditions goes against each other that means this case is not at all possible that means you cannot have degree of r(x) strictly less than the degree of (x – α).

Because if that is the case then that goes against this conclusion that r polynomial evaluated at α is 0. That means the only case that is left is that your r(x) polynomial is 0 polynomial which shows that this is 0 polynomial and hence f(x) is completely divisible by (x – α) showing that (x - α) is a factor of f(x).

(Refer Slide Time: 41:49)