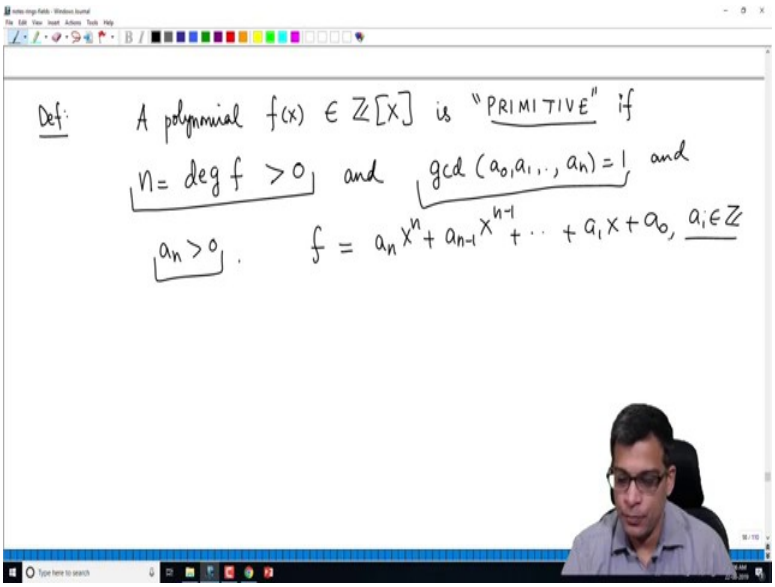
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture – 28
Gauss Lemma

In the last video, I talked about a characterization of UFDs which said that if R is an integral domain in which factorization terminates then it is a UFD if and only if every reducible element is prime. Using that we showed that PIDs are UFDs and our next order of business, in the study of UFDs is to show that Z X is a UFD. And I started the discussion in the, at the end of the last video, in which I said that goal really is to consider Q X, Q is the quotient field of Z. In Q X we know that UFD property holds because Q is a field, Q X is a polynomial ring in one variable over Q which is a PID hence it is a UFD.

So, in particular in that ring every irreducible element is prime. Every element in Z X can be thought of as an element of Q X. So, we are going to use that and somehow conclude that in Z X also every irreducible element is prime. And I ended the last video by the remark that, this analysis and the proof that we are going to present today works exactly in the same way for any UFD R, not just Z and at the end when we conclude Z X is a UFD that analysis also shows that R X is a UFD as soon as R is a UFD. So, let us begin today by considering the following definition.

(Refer Slide Time: 01:35)

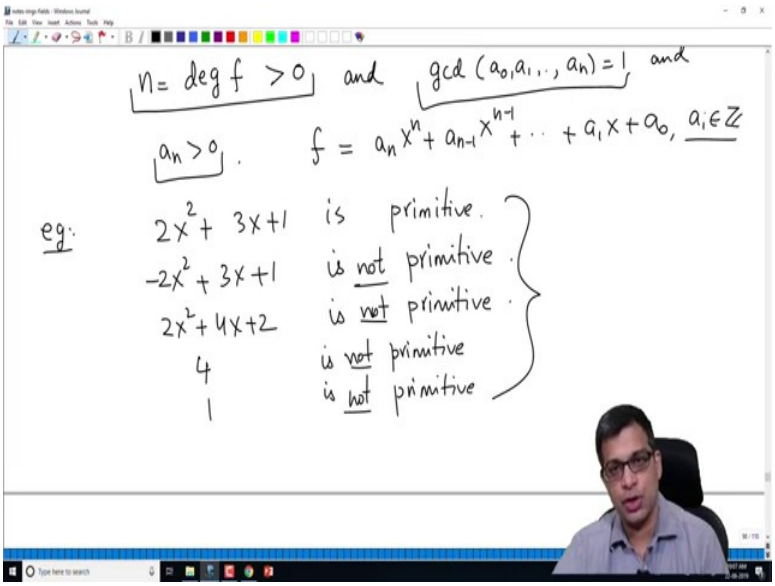


So, our whole video today is about keeping track of what is integer polynomial, what is rational polynomial, whether something is true in Z X is true in Q X, if something is an Q X is it true in Z X and so on. So, in order to clarify all these things we are going to define the following. Say polynomial in Z X, let us say polynomial f X. So, I am going to usually just denote polynomials by f instead of f X, just in the beginning I will write this.

A polynomial f X in Z X is called primitive, this is a very important word for us; primitive, if the following happens. If the degree is positive that means, we are excluding all constants. We are not going to call constants primitive. So, it must be at least degree 1 polynomial. And so, it has two properties: the first is that degree is positive, it has 3 properties really we will show that; gcd I will explain this a 1, a n, is 1, this is the second condition and a n is positive, this is the third condition. What are the ai's ai's? These are just the coefficients of f. So, I am going to write f as a n, X n, a n minus, 1 X n minus 1 plus a 1 X plus a 0.

So, remember a is are all integers because I am taking an integer polynomial. So, these are integers. I want 3 things for a primitive polynomial, m is positive that means, the degree is positive, the gcd of all the coefficients is one and the leading coefficient is positive.

(Refer Slide Time: 03:22)

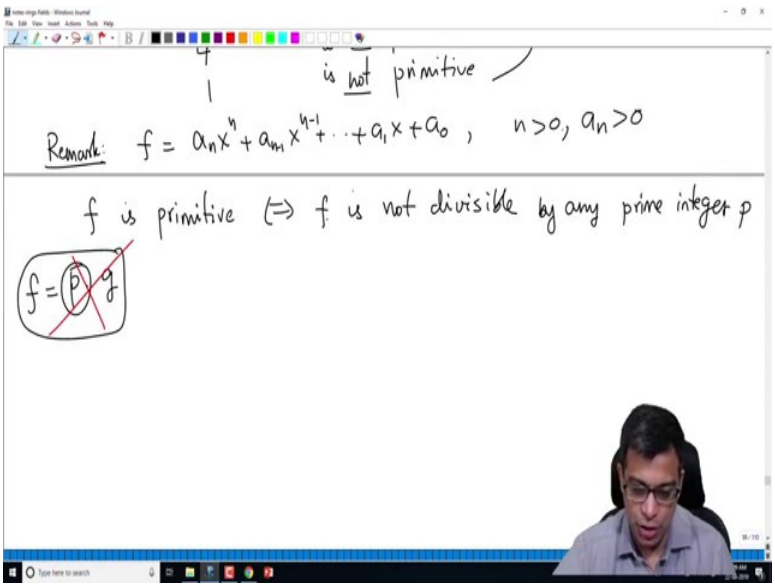


So, what are the examples of this? For example, if we take 2 X squared plus 3 X plus 1. Is it primitive or not? It is primitive because degree is too positive, the leading coeffi-

cient too is positive, gcd of the coefficients which is 2, 3 and 1 is 1 whereas, if we take minus 2 X squared plus 3 X plus 1 is not primitive because it has true the 3 properties, but not the third. The leading coefficient is negative, so that violates this condition. So, n has to be positive. The gcd is 1, degree is positive, but the leading coefficient is negative. So, this is not primitive.

Similarly, we have 2 X squared plus 4 X plus 2. Here also its not primitive because leading coefficient is positive, degree is positive, but the gcd of the coefficient is not 1, but gcd is 2 here. Similarly, 4 is not primitive, 1 is not primitive. 4 is not primitive for many reasons. Degree is not positive, gcd of the coefficient is not 1 whereas, 1 gcd of the question is 1, but the degree is not positive. So, just primitive polynomial is nothing, but a polynomial positive degree with positive leading coefficient and there is no common devisor for all the coefficients; very simple, right. So, that is what a primitive polynomial is.

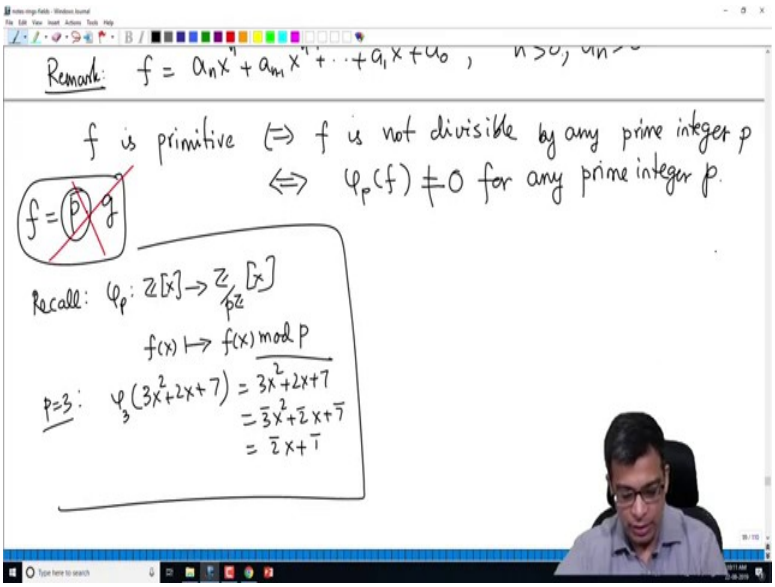
(Refer Slide Time: 04:57)



So, and we make the following easy remark. So, the remark is if f n is an, f is as before, a n, X n, a n minus 1, X n minus 1 plus a 1 X plus a 0 and let us say n is positive, a n is positive. So, these are the 2 of the 3 conditions. The degree is positive, leading coefficient is positive. Now, when is f primitive; we can characterized that by saying the following. f is primitive if and only if f is not divisible by any prime integer, right. All we want is that.

So, because we are assuming degree is positive and that leading coefficient is positive, primitiveness is simply the remaining property which is that the gcd of the leading coefficients is 1, that means no prime number divides all the gcd's, all the coefficients which is same say if you divides all the coefficient that means it divides f. If a prime number divides f it means divides all the coefficients because if f can be written as p times g that means, p divides each coefficients, each coefficient a n. So, p dividing f is equivalent to p dividing each coefficient. If that does not happen, so in other words we do not want this to happen, then it is primitive.

(Refer Slide Time: 06:36)



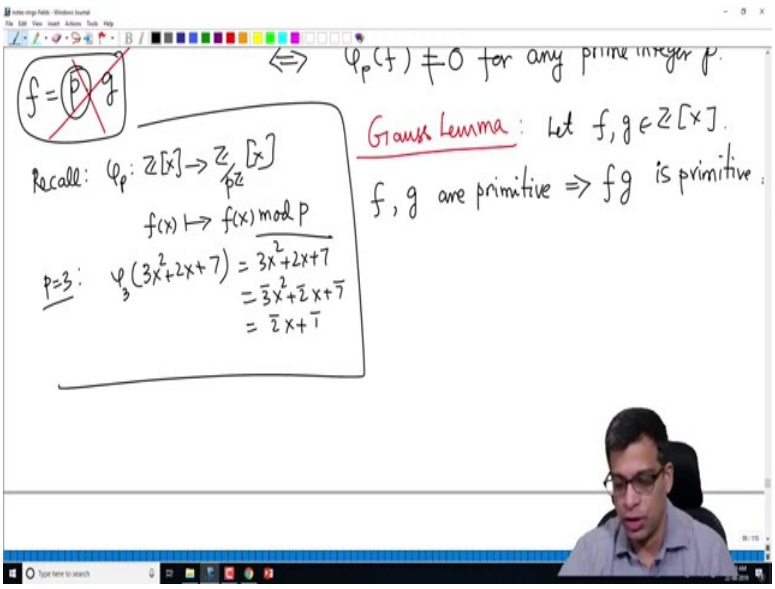
This second condition can be further characterized. Recall, that we have the natural, we will write that here. Recall, the map phi p from Z X to Z mod p Z X. Remember, there is a natural subjective homomorphism from Z to Z mod p Z. In general for any ring R any idea I we have a natural subjective homomorphism from R to R mod I.

So, here we have Z X to Z, Z to Z mod p Z first then we just attach a variable. So, Z X to Z mod p Z X. Here, what are we doing? We take a polynomial and we just view this mod p, right. So, for example, if p is 3 and the function sense let us say phi 3 of 3 X squared plus 2 X minus 7 or plus 7 goes to 3 X squared plus 2 X plus 7 bar which is 3 is; so, this is like 3 bar X squared plus 2 bar X plus 7 bar. So, this is actually just 2 bar X plus 1 bar. This is just a digression, right. We are just going modulo p for each of the coefficients.

So, 3 X squared plus 2 X plus 7 under phi 3 maps to 2, the leading coefficient goes away because 3 is the leading coefficient. And what survives is 2 X, 2 bar X plus 1 bar because 7 is 1, in Z mod 3 Z. So, if f is not divisible by any prime integer p that means, phi p f f is not 0 for any prime integer p, right because if every coefficient of f is divisible by p which is same as saying f is divisible by p, then the image of f and f p will be 0 because we are going modulo p for each coefficient. If each coefficient is divisible by p that means, the polynomial itself become 0 that means, if phi p f is 0. So, if phi p f is not 0 that means, at least one coefficient of f is not divisible by p that means, f itself is not divisible by p.

So, this is the convenient way of remembering how to check that f is primitive. And this leads to the most important lemma in this video, and in this all prove that Z X is UFD is the following. It is called Gauss lemma it is very simple, but it is very important.

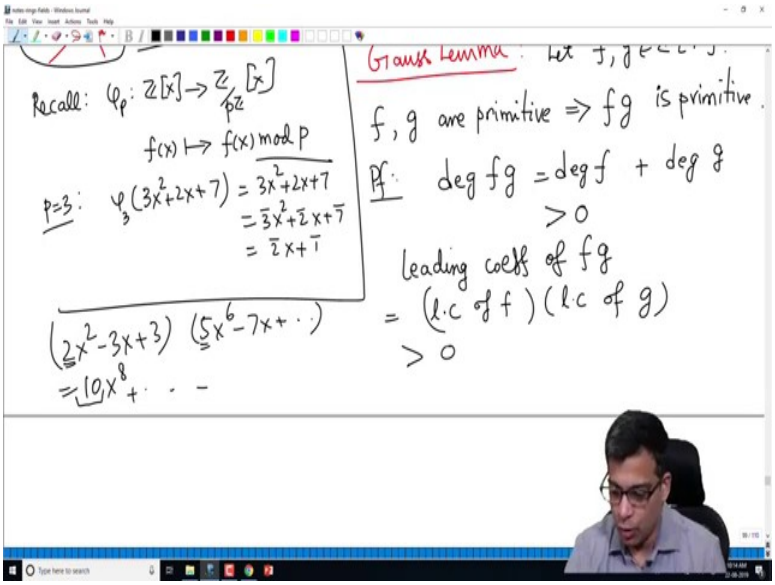
(Refer Slide Time: 09:14)



I will also remind you that a primitive polynomial is by definition an integer polynomial. Remember, the definition of primitive is it is an integer polynomial with 3 additional conditions. So, primitive polynomials are automatically integer polynomials. So, the Gauss lemma says that, let f and g be two polynomials in the integer polynomial ring, that means, f and g are integer polynomials. If f comma g are both primitive then the product f g is primitive. This is a very simple and easy to verify fact, but it has this name Gauss lemma because it is extremely useful. It is applied all the time.

So, it is not saying very surprising fact, right. If you have two polynomials which are both integer polynomials which are both primitive then their product is primitive, ok. Some conditions are trivial, because if f and g have positive degree f g has positive degree. If f and g have positive leading coefficient their product also as positive leading coefficient, ok.

(Refer Slide Time: 10:29)



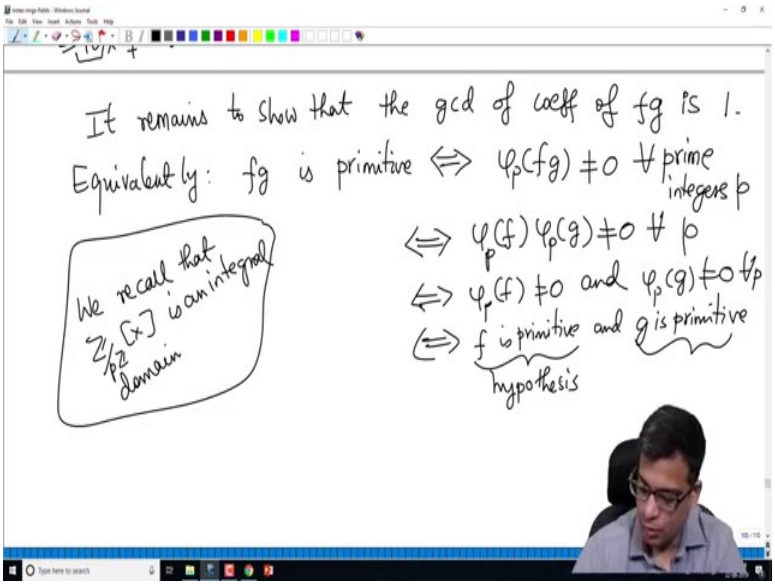
So, the proof of Gauss lemma says that degree of f g is degree of f plus degree of g, right because if X squared is a leading term of f, X power 4 is a leading term of g, when you multiply them X power 6 will be the leading term of f g. So, the degree is 2 plus 4. And f and g are primitive so that means, degree of f is positive, degree of g is positive, the sum is positive, degree of f g is positive.

So, what is a leading coefficient of f g? If you think about it, if you for example, multiply 2 X squared minus 3 X plus 6 or plus 3 times 5 X power 4, 5 X power 6 minus 7 X plus whatever. The leading coefficient is the coefficient of the largest degree term. Here it is 2, here it is 5, so if you multiply them you get 10 X power 8 and we are not interested in what happens next.

So, the leading coefficient of f g is the leading coefficient, so I am going to write this as l c of f times l c of g, l c is stands for leading coefficient, l c of f g is l c of f times l c of g because leading term of f g is just the leading term of f multiplied by leading term of g.

So, leading coefficient has this property. But we know the leading coefficient of f is positive leading coefficient of g is positive. So, leading coefficient of f is positive.

(Refer Slide Time: 11:59)



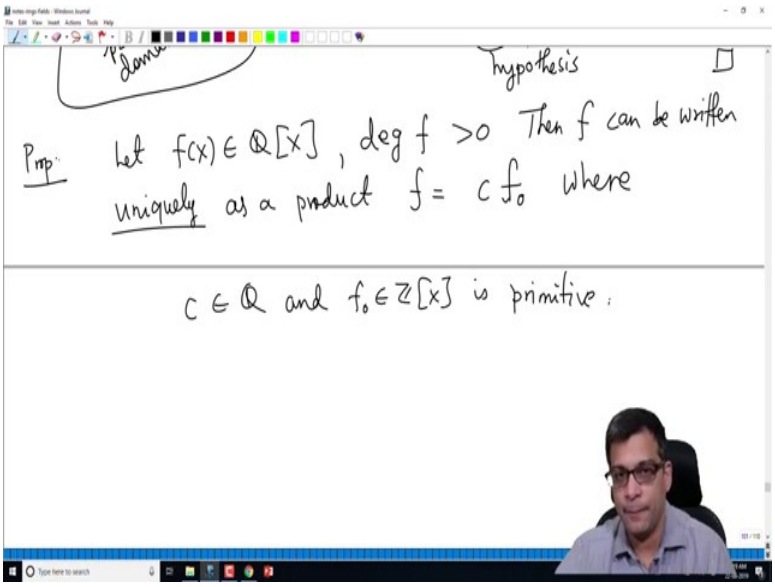
So, it only remains to show that the gcd of coefficients of f g is 1 equivalently that is the third condition, right of primitive polynomials. But as we observed here once the degree is positive and leading coefficient is positive primitiveness is characterized by phi p f is nonzero by any integer p, prime integer p. So, f g is primitive if and only if phi p of f g is not equal to 0 for all prime integers. If you notice, I am using the word prime integer because now that we have notion of prime elements in an arbitrary ring, I want refer to primes in Z as prime integers. So, we want to show phi p f g is nonzero, right. If that happens p does not divide all the coefficients of f g, that means, the gcd of all the coefficients of f g is 1.

So, we want this true, we want this be true to every prime integer p. But the important thing now is phi p is a homomorphism of rings. So, phi p of f g is same as phi p of f times phi p of g. So, we want this product to be nonzero. But if this product is nonzero that means, now, we use the fact that Z, Z mod p Z X is an integral domain, right Z mod p Z is in fact a field, so it is an integral domain. When you attach a variable to an integral domain it remains an integral domain. It is a simple fact, right if you multiplied two nonzero polynomials over an integral domain the product is also nonzero.

So, in an integral domain when it is a product nonzero that means, phi p f is nonzero and phi p g is nonzero for all p. Remember that in an arbitrary ring to nonzero elements can multiply to 0. So, it is not equivalent to this statement, product nonzero is not equivalent to individual facts not 0, but in integral domain product nonzero if and only if individual terms are nonzero. But now what is the meaning of phi p of f not equal to 0 for all p? That means, f is primitive and g is primitive for phi p not 0 for all p that means, because g is positive degree polynomial with leading coefficient positive g is primitive if and only if phi p is nonzero, but these are hypothesis, right.

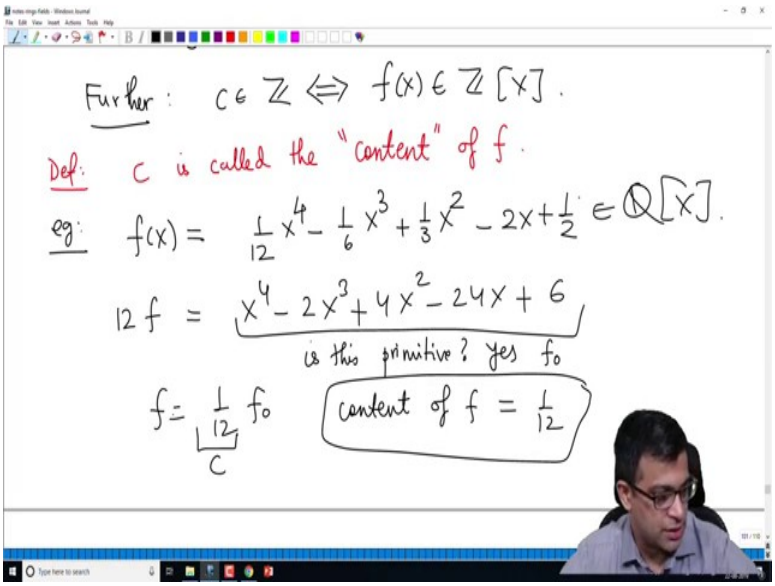
We are given that f and g are primitive. So, this proves that product of primitive polynomials is primitive. This is a very important thing for us. So, if you have two primitive polynomials, their product is also primitive.

(Refer Slide Time: 15:18)



So, let me now continue and prove the next important proposition. So, the proposition says the following. So, I will write this down and give some examples after this. So, let f be rational polynomial now, ok. So, f X is in Q X, and suppose degree of f is positive. Then f can be written as uniquely as, this word uniquely is extremely important for us, can be written uniquely as a product f is equal to c f naught, where c is actually a rational number and f 0 is an integer polynomial is primitive, ok. So, what we have is f can be written uniquely as a product of a rational number and a primitive polynomial.

(Refer Slide Time: 16:24)



Further, c belongs to Z, the c is in general rational number, but c belongs to Z if and only if f X itself belongs to Z X, ok, c belongs to Z if and only if f X is in Z X. Remember, we started with a rational polynomial. The c that we get is an integer if and only if the rational polynomial is in fact, an integer polynomial. So, the definition is c, remember this is the unique factorization. So, c is something uniquely attached to rational polynomial. c is called the content of f. So, this is called the content of f.

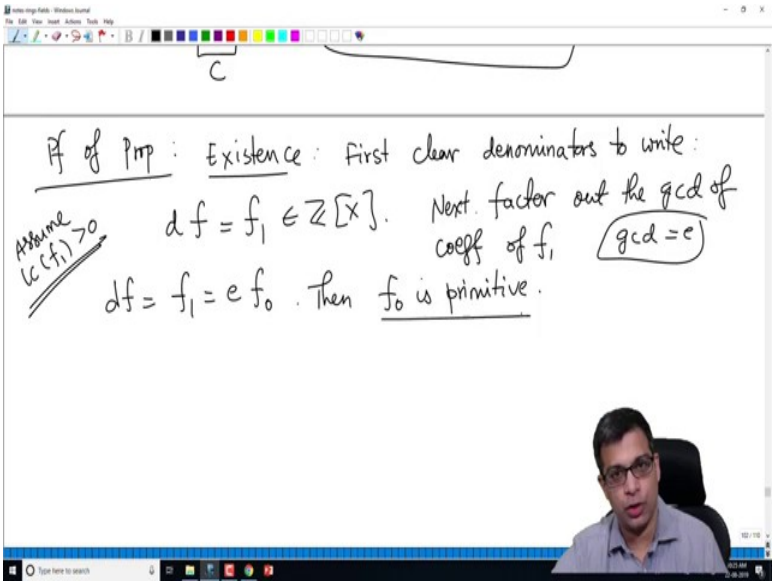
So, before I prove this let me first give you one example. So, let us take f X to be, I am not take this 1 by 12 X power 4 by time minus 1 by 6 X cube plus 1 by 3 X squared minus 2 X plus 1 by 2. Remember, this is a rational polynomial. It is not an integer polynomial, coefficients are rational numbers and they are not integers. So, how do you write f as c times a, rational number times a primitive polynomial? It is very simple. So, first we can actually clear the denominator. So, we will consider 12 f to be X power 4 minus 2 X cube plus 4 X squared minus 24 X plus 6, right. So, clear denominator to get an integer polynomial.

Now, see if that integer polynomial is primitive or not. Is this primitive? It is, right, because it is positive degree, degree for leading coefficient is 1 which is positive and the coefficients have gcd 1 because one of the coefficients is 1. So, f is this is our f 0. So, now, f can be written as 1 by 12 times f 0. So, this is c. So, the content of f X is 1 by 12.

So, in this example content is 1 by 12. So, exactly the same process we now perform, ok. So, there is nothing strange here.

So, remember we have to do two things, given any rational polynomial we have to show that it can be written as a product of a rational number and a primitive polynomial and we also have to show that it is unique.

(Refer Slide Time: 18:56)



So, let us prove, prove the proposition. So, there are two parts, first we will do existence which is the easy part. What is the existence of the factorization? So, what do we do? First, clear denominators to write. So, f is given to us, so again keep in mind this example. So, I have taken an example here, clear denominator means multiply by the gcd of the rather the LCM of all the denominators. So, multiply by some d to get df is equal to f 1 in Z X, right that is what I have done here, multiplied by 12 to get an integer polynomial. So, here in general I might multiplied by is whatever d is. So, clear denominators. So, d f is equal to f 1 in Z X.

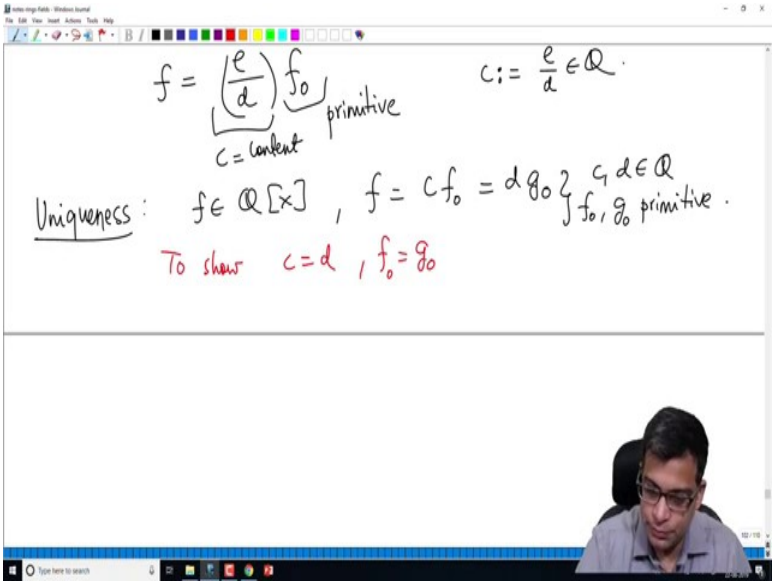
Now, factor out the gcd of the coefficients of f 1; so, f 1 is an integer polynomial you look at all the coefficients. In that example the gcd happened to be 1 itself, so we do not need to factor, but maybe there is a there is something else some common factor. So, we can write it this as e times f 0; gcd is equal to e let us say, e times f 0. So, I have an integer polynomial all the coefficients have gcd is, so I pull it out.

Then, it clearly follows that f 0 is primitive, right, is that clear to you because f 0 as the same degree as f 1 which is positive, right. The polynomial f is positive degree we are assuming. So, multiplying by integers does not change the degree of the polynomial. So, degree of f 1 is positive, degree of f 0 is positive. Also, the leading coefficient of f 0 is positive because the leading coefficient of f 1 is positive.

We are going to assume that degree of f is positive and when you f may have negative leading coefficient, but when you clear out the gcd, gcd always picks out the negative part and f 0 now has leading coefficient positive. So, it has positive degree, positive leading coefficient. And because we have factored out the gcd the remaining coefficients have no common factor. So, we can, we can show that f 0 is primitive.

So, just correct what I said couple of minutes ago, I factor out the denominator I clear the denominator in such a way that assume that l c of f 1 is positive. So, I can assume that l c of f 1 is positive because if f has negative leading coefficient I can adjust that in d to make sure that leading coefficient of f 1 is positive, once the leading coefficient of f 1 is positive leading coefficient of f 0 is positive. So, f 0 is primitive, right, because we have factored out all the common factors and put it in e.

(Refer Slide Time: 22:23)

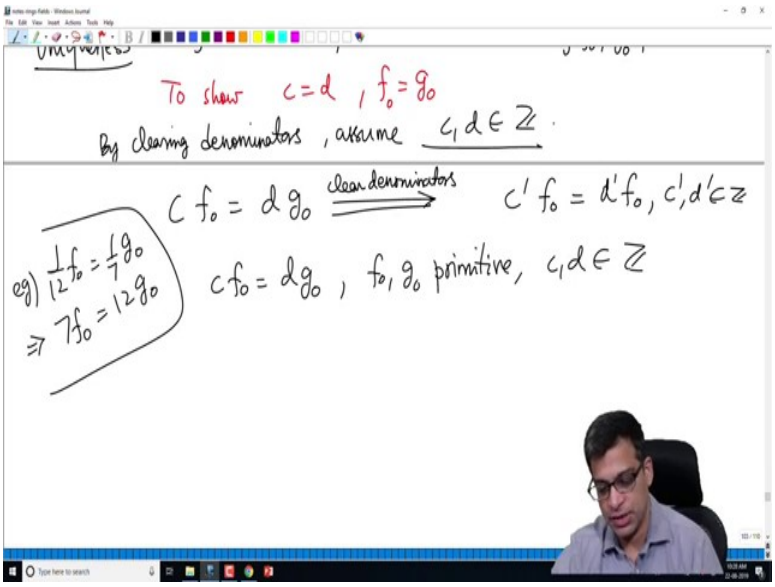


So, now we can write f as e by d and f 0. So, this is going to be c which is the content and this is the primitive, right. So, we have written f as a rational number. Remember, c is now, c is defined to be e by d and it is in Q. As this example shows content is in gen-

eral not an integer. It is an integer if and only if f is a integer polynomial. Here, we have started with a non-integer polynomial, so the content is actually a non-integer. It is a rational number which is not an integer.

So, we have written this as some rational number times, we have primitive polynomial. So, this is the existence. We have to now show uniqueness. Uniqueness is also easy. So, let us take f is a rational polynomial and suppose f can be written as c times f 0 and at the same time as d times g 0. And what is the property of c d, f 0, g 0? c and d are in Q they are rational numbers, and f 0 g 0 are primitive. Primitive by definition means integer polynomials. So, we have two possible descriptions, we would like to show that they are exactly the same description. In other words, we want to show c is equal to d f 0 is equal to g 0. So, let us show that.

(Refer Slide Time: 24:02)

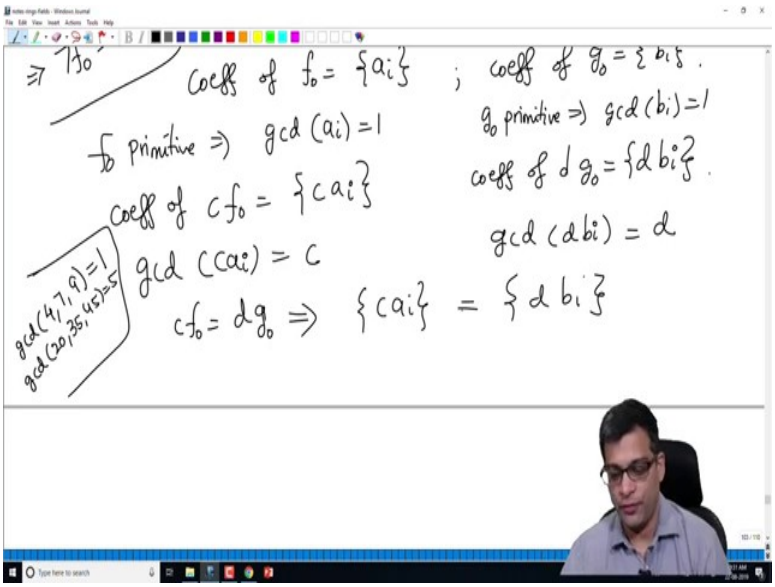


What we now know is that by clearing denominators, we can assume c d are in Z. So, what I am really doing is I am looking at this equation c f 0 equal to d g 0 and by multiplying by some common factor, common denominator I can write these clear denominators. I am basically writing c of c prime f 0 equals d prime f 0.

For example, if you have 1 by 12 f 0 times 1 by 7 g 0. What I am doing is just multiply by 84, so I get 7 f 0 is equal to 12 g 0, ok, as an example. So, the now if I forget f really, I have an equation and multiply by some common denominator and now c prime d prime are in Z. So, I can again read rename them and call them c and d. So, I will assume with-

out loss of generality that c and d are in Z. So, we have c f 0, d g 0, f 0 g 0 primitive that means, they are integer polynomials, c d are integers. Originally they are rational numbers, but now I have cleared denominators to make them integers.

(Refer Slide Time: 25:28)

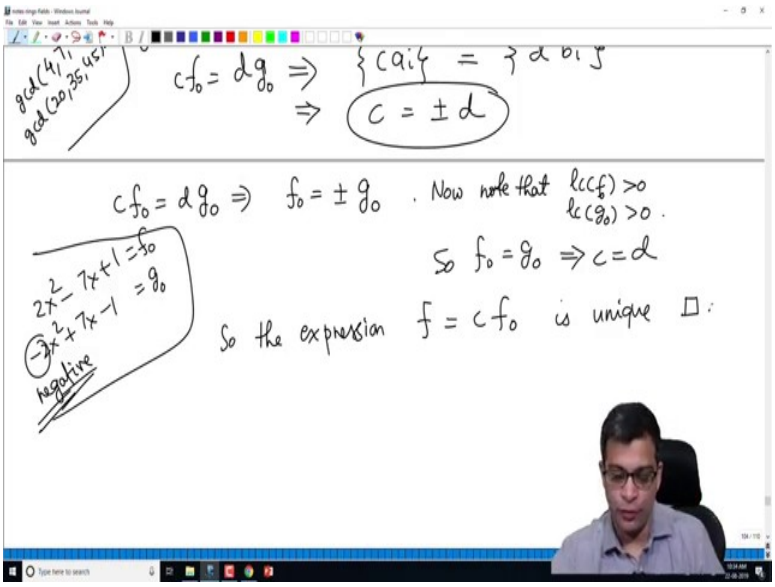


Let us say coefficients of f 0 are a i. Remember, f 0 and g 0 have the same degree because a constant times f 0 is equal to a constant time g 0. So, they have same degree. So, the coefficients are a n, a n minus 1, a 0, similarly coefficients of g 0 or let us say b i. Because f 0 is primitive gcd of a i is 1. Similarly, g 0 is primitive implies gcd of b i is 1, right. f 0 is primitive polynomial. In this example, X power 4 minus 2 X cube and so on in primitive polynomial. So, a a 4 is 3, a 3 is 2, a 2 is 4, a 1 is minus 24, a 0 is 6, the gcd is all this coefficients is 1.

But what are the coefficients of c f 0? This is just c a i, right we are multiplying every coefficient by c multiplying f 0 by c means every coefficient by c. So, coefficients of c f 0 is c a i. What are the coefficients of c g 0, d 0 rather? d g 0 is d a b i, d b i because b i are the coefficients of g 0 d g 0 has coefficients d b i. Since, ok, so two things to say now. What is the gcd of c a i? gcd of a i is 1, so the gcd of c a i is c; gcd of d b i is d. So, you have a bunch of integers who are co-prime to each other that means, the gcd is 1, you multiply all of them by the same integer the gcd become c. So, gcd of 4 7 and let us say 9 is 1, right because they have no common factors.

But if you multiply all of them by 5, so you have 20, 35, 45, so the gcd will become 5, because 5 certainly divides all of them. No other integer can divide them, no other prime, so it is gcd 5. So, a i's have gcd 1. So, c i have gcd, similarly g d b is have gcd d, but we now use the important fact that c f 0 is equal to d g 0 that means, the set c a i is equal to the set d b i, right. c f 0 is the same polynomial is d g 0 that means, the coefficient sets are same, c a i is equal to d b i.

(Refer Slide Time: 28:20)



But once a coefficient sets are same, their gcds are same, ok. So, except that there is a there is some confusion about positive negative. So, what we can say is that c is equal to plus minus d, because if the gcd is 2 minus 2 is also gcd. Any associate times gcd is also a gcd. gcd is just greatest common divisor. We are now trying to do this in general. In integers typically convention is to show that define the gcd is positive, but in general for an arbitrary ring you have the gcd is just the largest common factor. So, any such thing multiplied by an associate is also going to be gcd.

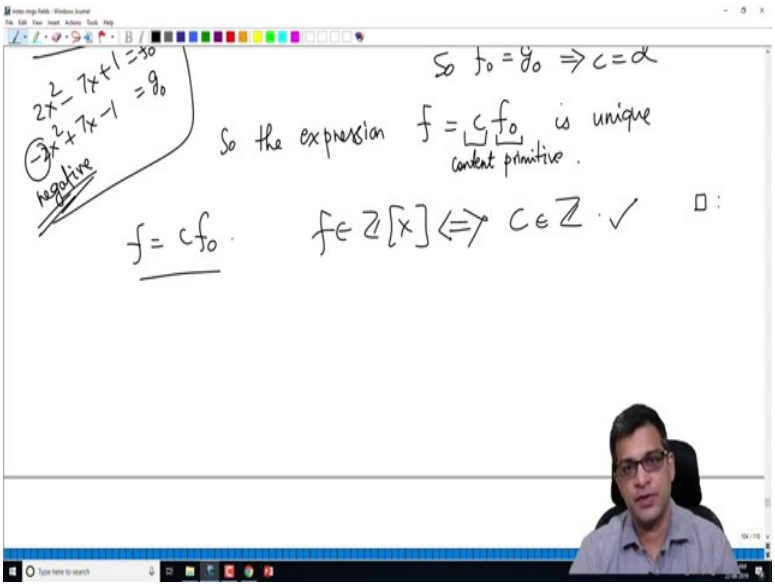
And remember the remark at the beginning of this video, I am trying to show that Z X is a p UFD, but the same proof carriers over for any UFD R and shows that R X is a UFD. So, I am only going to use that c is equal to plus minus i d. Once c is equal to plus minus i d and we know that c f 0 is equal to d g 0 that means, f 0 is equal to plus minus g 0, c and d are actually same plus minus of same number. So, you cancel c, and only issue would be that maybe f 0 is minus g 0 or f f 0 is equal to actually equal to g 0.

But in fact now we know that, note that leading coefficient of f is f 0 is positive leading coefficient of g 0 is positive. Why is that? That is because f 0 and g 0 are primitive polynomials. By definition a primitive polynomial has leading coefficient positive. So, leading coefficient of f 0 is positive, leading coefficient of g 0 is positive that means, f 0 is equal to g 0. They cannot be negative of each other, right, because if f 0 minus g 0 and if f 0 is relative coefficient positive then leading coefficient of g 0 has to be negative because if 2 2 X squared minus 7 X plus 1 is f 0 and g 0 is minus f 0, it will be minus 2 X squared plus 7 X minus 1, but then the leading coefficient is negative which it cannot be. So, f 0 must be g 0, ok. So, f 0 is equal to g 0.

Once this happens, c equal to d also because c f 0 is equal to d g 0, f 0 and g 0 are same, so c and d are same. So, originally we said c and d are possibly negatives of each other, but that cannot happen. We have concluded that, c equal to d. So, this shows that the expression of any arbitrary rational polynomial into its content times a primitive polynomial is unique, ok. So, this is the proof of this proposition.

So, in this example that we did before we proving this preposition, this particular integer rational polynomial is contained c 1 by 12 and f 0 is the primitive polynomial. In other words, what we have now shown is that there is no other expression. Every time you write it as a content as a rational number times a primitive polynomial, that rational number has to be 1 by 12 in that primitive polynomial has to be this X power 4 minus 2 X cubed and so on.

(Refer Slide Time: 31:53)



So, in general every rational polynomial can be written as a product of its content which is a rational number and a primitive polynomial. Now, that the there is actually the proof is not quite complete because the proof also says that c is in Z if and only if f X is in Z X. This is now easy, right, because we have written f as c times f 0. So, suppose f is in Z X, if f is in Z X we know that f 0 is also in Z X that means, and f 0 has no common factors, coefficient of f 0 have no common factors.

So, if c is not an integer that means, c has a denominator which is not 1, but the denominator cannot be cancelled by any of the factors have f 0. So, c must be Z in Z itself, because if c is not in Z that violates the fact that f is in Z X. Similarly, if c is in Z that is easy. If c is in Z f 0 also in Z X, so f is in Z X; this now completes the proof. So, if you take a rational polynomial find its content, if that content happens to be integer then the rational polynomial is actually an integer. Similarly, if you take an integer polynomial, right its content then that content must be integer. So, that is what we have shown, ok.

So, let me stop the video here. In this video, we defined primitive polynomials, and we proved a very important theorem called Gauss lemma which says that product of primitive polynomials is primitive and then we have shown that every rational polynomial can be written as a rational number times a primitive polynomial and that rational number is called the content.

And I will final remark, I will make in this video is that everything that we have done in this video carries over to any UFD, not just Z. You can replace Z by any UFD R, and all the definitions and theorems we gave today carry over to that. So, in the next video, we will prove the prove finally, that Z X is a UFD and more generally if R is a UFD, R X is a UFD.

Thank you.