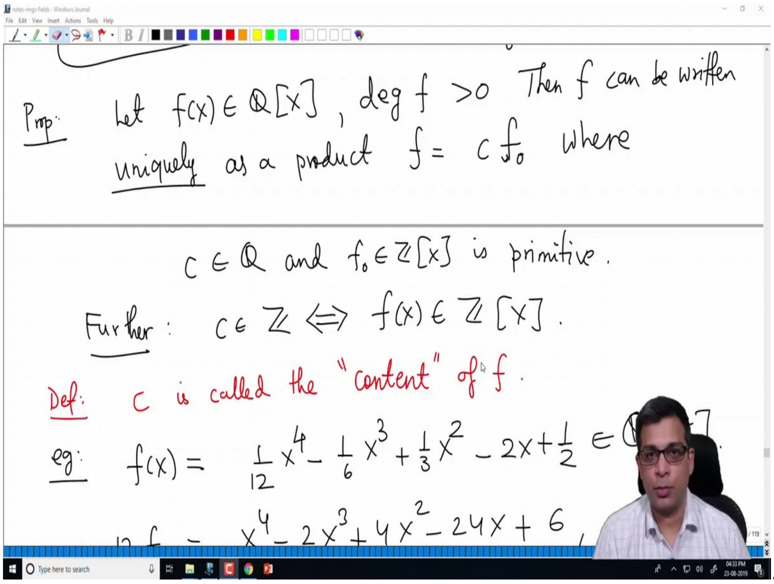
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 29
Z[X] is a UFD

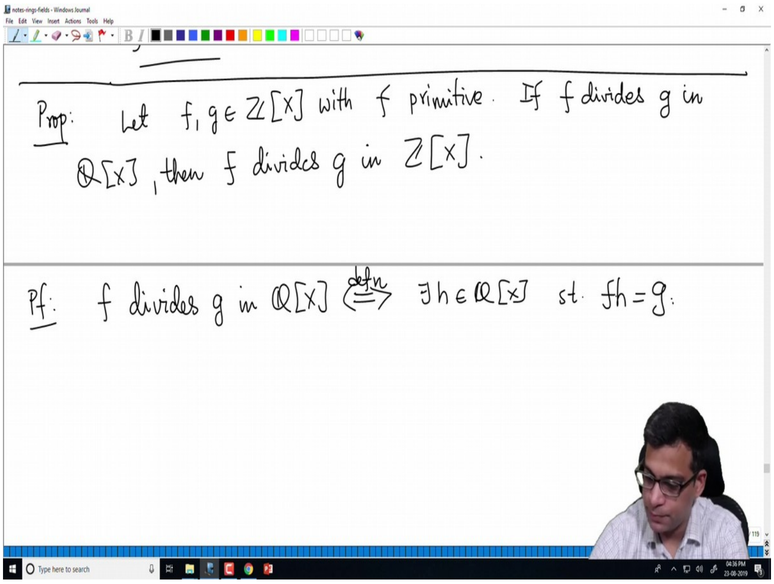
(Refer Slide Time: 00:17)



In the last video we talked about primitive polynomials and proved a very important theorem called Gauss lemma and in this video, we are going to finish that circle of ideas and show that the polynomial ring over integers in one variable polynomial ring in one variable over the integers is a UFD.

So, let me start today's video by recalling the proposition, we proved at the end of the last video. We showed that any rational polynomial which has positive degree can be written uniquely as a product of a rational number and a primitive polynomial; c is a rational number f 0 is a primitive integer polynomial. Remember primitive by definition means it is an integer polynomial and this expression is unique and c is then called the content of f. So, this is an important proposition for us.

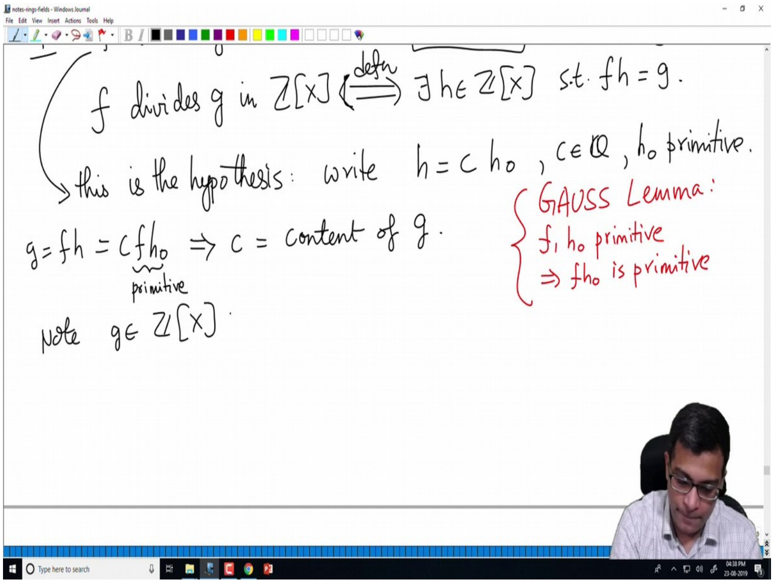
(Refer Slide Time: 01:15)



So, today we are going to start with the following proposition which is the key proposition that we are going to use to prove that the polynomial ring Z X is a UFD. So, the proposition says the following. Let us say f and g are two polynomials over integers that f and g being Z X with f is primitive. Then if f divides g in Q X then f divides g in Z X; this is the important proposition for us.

If a primitive polynomial divides an integer polynomial in Q X it actually divides in Z X itself. So, before we start the proof, let me quickly recall what it means for division to happen in a certain ring. If f divides g in Q X remember this means by definition this means there exists a rational polynomial h in Q X such that f h is equal to g, right. If an element divides another element in a ring R; that means, as the third ring elements such that the first element times the third element is the second element. So, here the crucial thing is f h is in Q X.

(Refer Slide Time: 02:39)



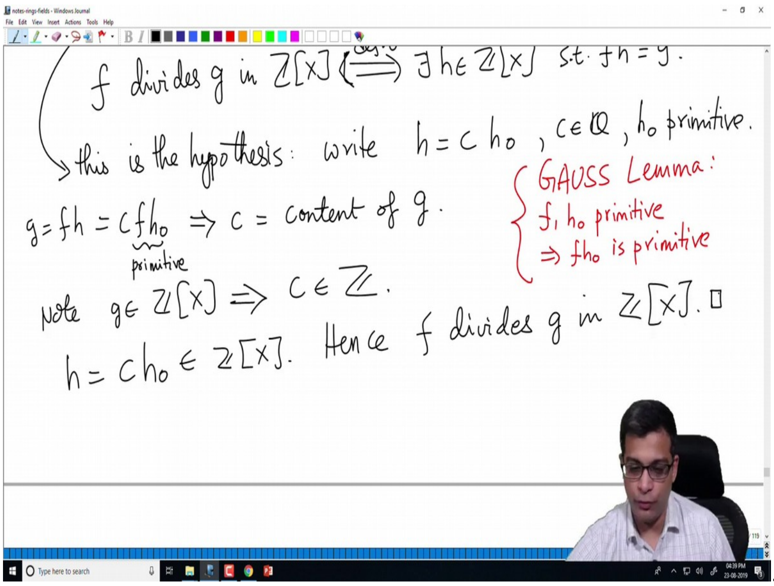
So, now, what is the meaning of the same thing right f divides g in Z X means by definition this means there exists h, possibly different, in Z X such that f h is equal to g. So, the crucial difference between dividing in Q X and Z X is that this h may live only in Q X. In this case we only say f divides g in Q X, but if it also lives in Z X we say f divides g in Z X. So, this is a very easy proof. But main thing to keep in mind is the difference between division in Q X and division in Z X.

So, we know that this is a hypothesis right. We are given that f divides g in Q X. So, we know that there is a rational polynomial h such that f h is g. Now using the previous proposition, we write h as c times h 0 where c is in Q which is the content of h and h 0 is primitive. Remember this is a crucial proposition that we proved at the end of last video. Every rational polynomial can be written as a product of a rational number and a primitive polynomial and it is a unique expression.

So, now, we know that f h or rather g is equal to f h which is equal to f we can write it like this c f h 0. Now, I am going to recall for you the Gauss lemma. What is Gauss lemma? Remember that was a crucial theorem from the last video. Gauss lemma says that if f and h are primitive.

If f and h 0 are both primitive; f h 0 is primitive gauss lemma says simply that product of primitive polynomials is primitive. So, if two primitive polynomials are there their product is also primitive. So, in other words this is primitive because h 0 is primitive by construction, f is primitive by a hypothesis. So, g equal to c f h 0 must be the unique expression of g as a rational number times a primitive polynomial. That means c is the content of f; content of g right; c is the content of g and note that g is actually in Z X, remember that is the hypothesis the crucial thing is f and g are both integer polynomials.

(Refer Slide Time: 05:23)

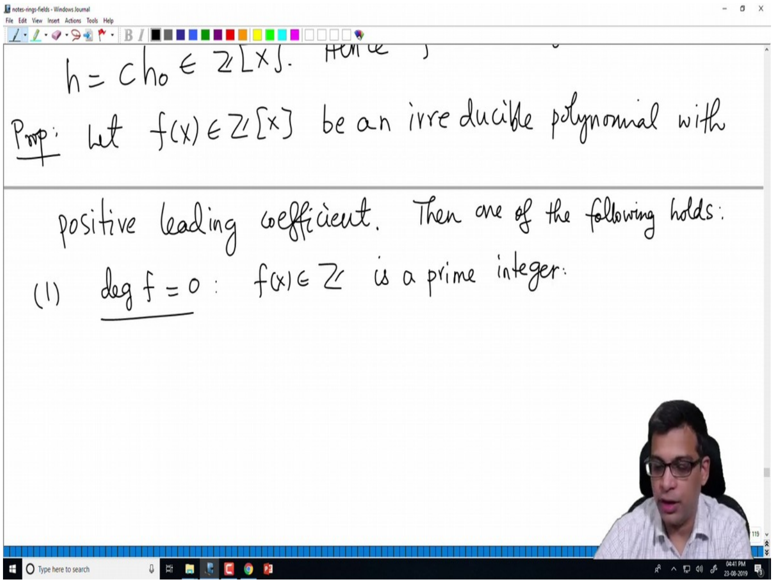


So, g is in Z X; that means, c equal c which is the content must be an integer, this is something that we proved in the last proposition. We can write every rational polynomial as a content which is in general a rational number times a primitive polynomial. But the polynomial we started with is rational if the polynomial, we started with is actually integer polynomial, then the content is actually an integer.

Now c is in Z and h remember is c times h 0; h 0 is an integer polynomial because h 0 is primitive, c we have just concluded is an integer. So, h itself is in Z X and hence f divides g in Z X that is all. So, very simple proof right; so, this is a very simple proof and it shows that division in Q X implies division in Z X.

But the important two things to remember; both polynomials in question are integer polynomials and the first polynomial is primitive that is very important only under that situation division in Q X implies division in f x, sorry division in Q X implies division in Z X. Now I am going to prove a nice fact before we finally, proved that Z X is a UFD.

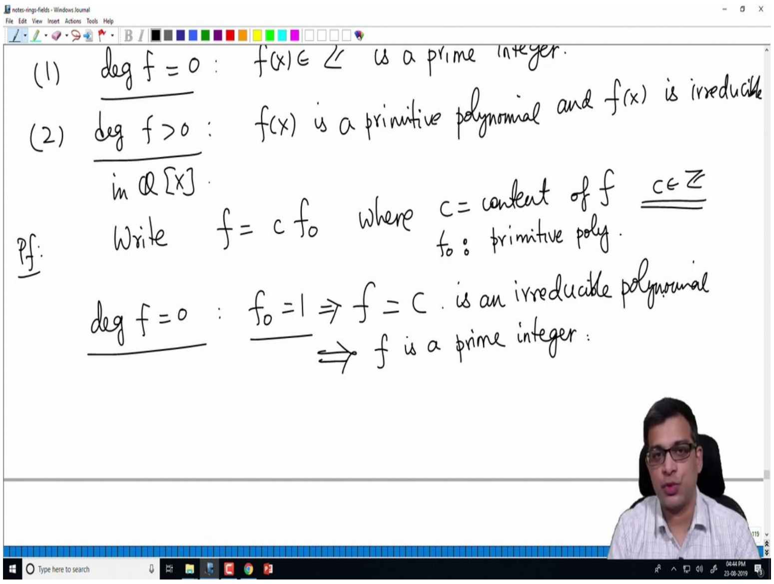
(Refer Slide Time: 06:37)



So, I am going to call this is a different proposition. It says that let f X be an irreducible polynomial; let f X be an irreducible polynomial in Z X with positive leading coefficient. So, I am going to take an irreducible polynomial remember irreducible in Z X. It is irreducible in ZX means what? When you write it as a product of; when you write f as a product of two other polynomials, one of them must be a unit because irreducible means it has no proper factorization.

So, suppose also that it has positive leading coefficient then one of the following holds, one is degree of f is 0 this is possible in which case f X which is actually in Z now is a prime integer. So, one possibility is it is a constant polynomial in which case it must be a prime number.

(Refer Slide Time: 07:57)

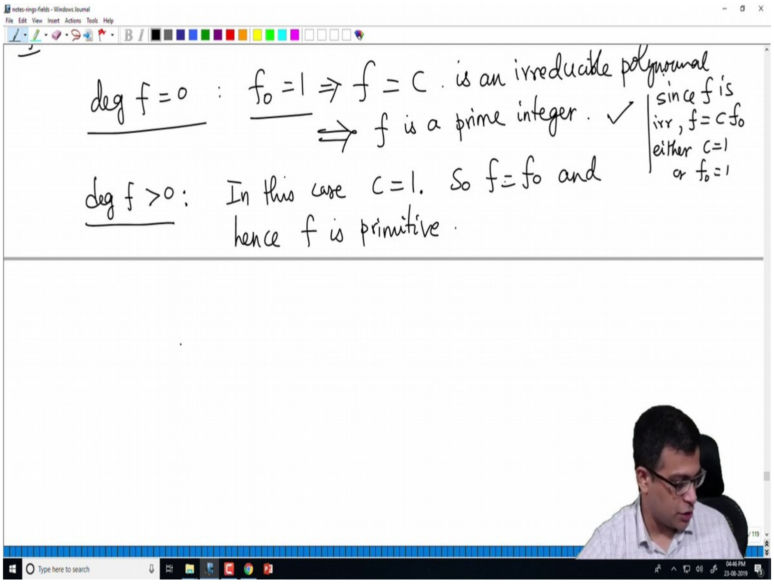


Second possibility is it is not constant in other words its degree is positive, then f is actually a primitive polynomial and more importantly f is irreducible in Q X. So, the hypothesis is that it is irreducible in Z X, but it is actually also irreducible in Q X. So, let us prove this quickly. This is again not difficult given whatever we have done so far. So, we will first consider the case first assume that actually we know that we let me say that like this, write f as c f 0 where c is the content of f and f 0 is primitive. Remember we can write every rational polynomial as a product of rational number and a primitive polynomial.

In particular we can write every integer polynomial as a product of an integer and a primitive polynomial; of course, c is in Z here because. c is a; f is an integer polynomial. Now if degree f is 0 remember degree f will be equal to degree f 0 because c is a constant. So, by multiplying by a constant, we do not change the degree; c is of course, non-zero. So, degree of f is 0; that means, f 0 must be one right because f 0 is a; so, in other words there is no f 0. So, when you factor it in terms of into unit and a primitive polynomial, there is no f 0; that means, f is actually c.

So, f is c and when is an integer irreducible is an irreducible polynomial; so that means, this implies that f is a prime integer because in for example, we can simply use the fact that the ring of integers is a PID. So, an element is irreducible if and only if it is prime. So, f is an irreducible polynomial of degree 0; that means, it is an irreducible integer. An irreducible integer is prime because in the ring of integers irreducible automatically implies prime.

(Refer Slide Time: 10:41)

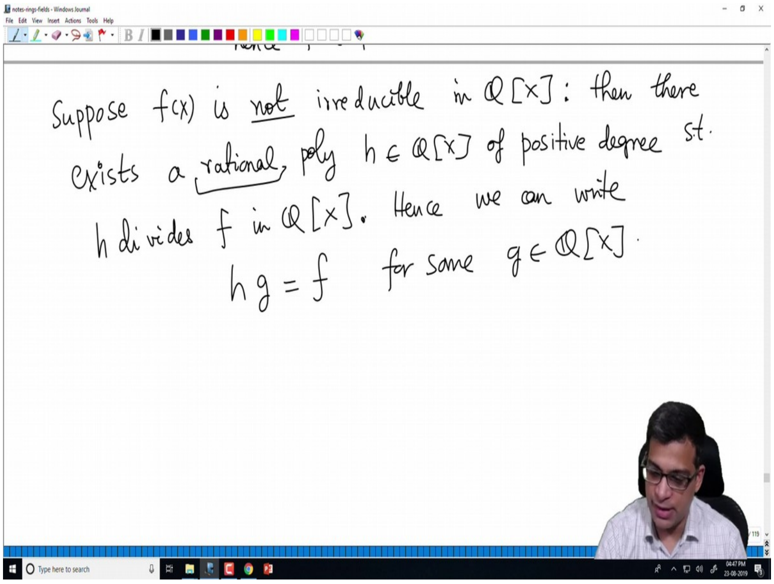


So, now we consider the second case, degree of f is positive, but; that means, in this case c must be 0 sorry c must be 1 because if c is not 1, remember c is an integer f is irreducible. So, either c is 1 or f 0 is 1. So, I should write that somewhere since f is irreducible and f is c f 0 either c is 1 or f 0 is 1, ok. Technically f 0 cannot be 1 because f 0 is a primitive polynomial what we really mean is that you cannot factor it into and it is an integer by itself.

But if degree is positive, f 0 is not a unit because f 0 is a positive degree polynomial, you know in other words c must be 1 because remember leading coefficient of f is positive. So, any reducible factorization of f must contain a unit. So, either c is 1 or f 0 is 1, minus 1 is also unit, but minus 1 cannot appear here because the leading coefficient is positive, in this case c is 1 so, f is equal to f 0.

So, f is automatically primitive; f is primitive right, because f 0 is primitive in this factorization f 0 is primitive and f is equal to f 0 so, it is primitive. So, what is it that we have to prove? Now we have showed that f is a primitive polynomial we need to now show that f is irreducible in Q X, that is what we will show now. Suppose it is not irreducible in Q X, what does that mean? Suppose, the next order of business is to show that f is irreducible in Q X.

(Refer Slide Time: 12:31)

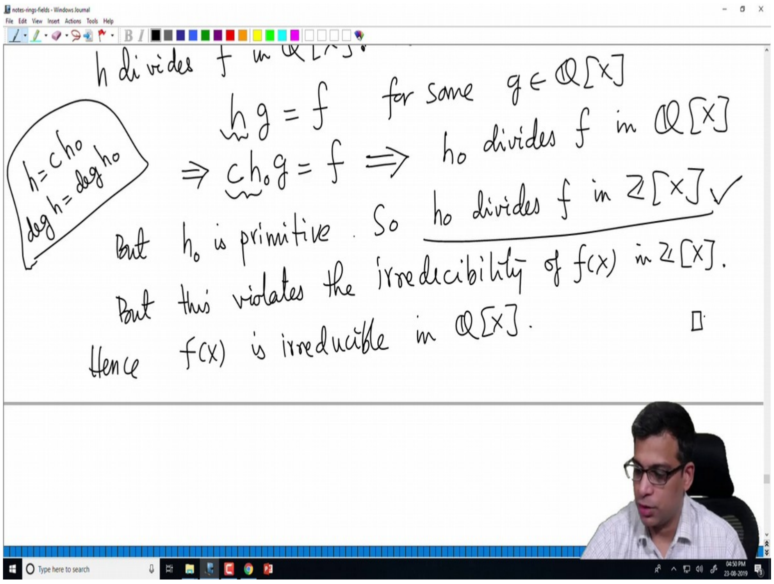


Suppose f X is not irreducible in Q X, what is the meaning of f not being irreducible. If it is not irreducible, then there exists a rational polynomial h in Q X. I am just repeating this rational polynomial so, h is in Q X of positive degree such that h divides f of course, in QX right. If some polynomial is not irreducible in QX; that means, a positive degree polynomial divides it. So, we can factor it; so, I am taking one of the factors so that the other factors are not units.

So, the degree is positive and it divides f in Q X because irreducibility is failing in Q X. So, f h divides f in Q X now what we can do is so, this in particular means hence we can write h g equal to f for some g in Q X that is the meaning of division right I recalled this at the beginning of this video if when we say h divides f; that means, there exists g in Q X such that h g equal to f.

But now again we use our crucial proposition: every rational polynomial can be written as its content times a primitive polynomial.

(Refer Slide Time: 14:17)



So, this implies c times h 0 times g equal to f, I am just replacing h by c h is 0, c h 0 g is equal to f. This implies h 0 divides f in Q X only I can say for now because g c is only a rational polynomial for us; g is the rational polynomial. So, h 0 times cg is f. So, h 0 divides f in Q X.

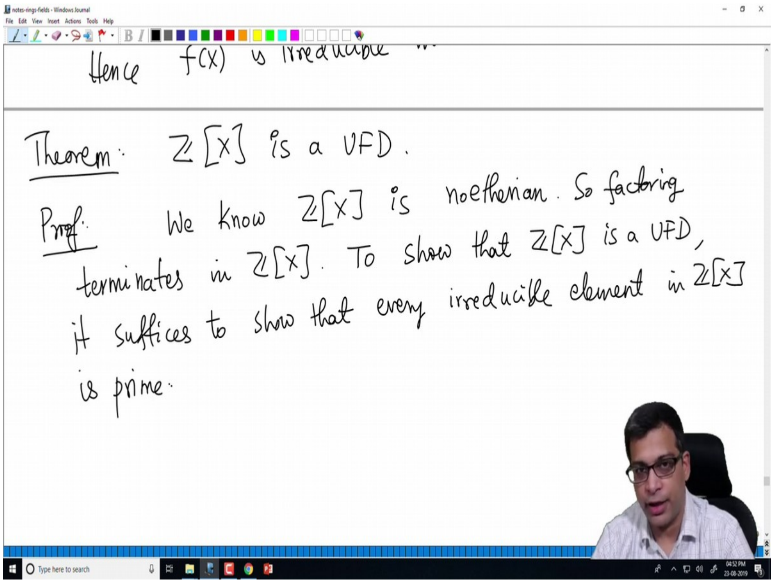
But what did we prove in the previous proposition? If a primitive polynomial divides another integer polynomial in Q X, then it divides that polynomial in Z X also; so, but h 0 is primitive by construction right. So, h 0 divides f in Z X itself, right; if a primitive polynomial divides another integer polynomial in Q X that primitive polynomial divides a polynomial in Z X. So, h 0 divides f in Z X, but this violates remember this violates the irreducibility of f X in Z X.

Remember what is hypothesis f X is irreducible right; f X is irreducible in Z X, but here whatever we done we have produced a polynomial of positive degree. Remember you know when we divide it like when we express it like this degree of h is degree of h 0 and h is a positive degree polynomial h 0 in other words is a positive degree integer polynomial which is a factor of f in Z X; that means, f is not irreducible this contradiction shows that f is actually irreducible in Q X.

So, all these things are a bit confusing I think and when you are seeing them for the first time especially. So, you have to keep track of the results carefully. So, if you need to, please see this video again so that all the ideas are clear in your mind. What did we show? We showed that if you take an irreducible integer polynomial with positive leading coefficient then either its degree is 0, in other words it is constant in which case it must be a prime integer. Otherwise it is a positive degree polynomial, then it is actually irreducible in Q X; it is primitive and it is irreducible in Q X.

And now finally, we are ready to show that Z X is a PID sorry Z X is a UFD. So, I am going to prove this and then I will at the end of this video, I will revise the whole sequence of arguments.

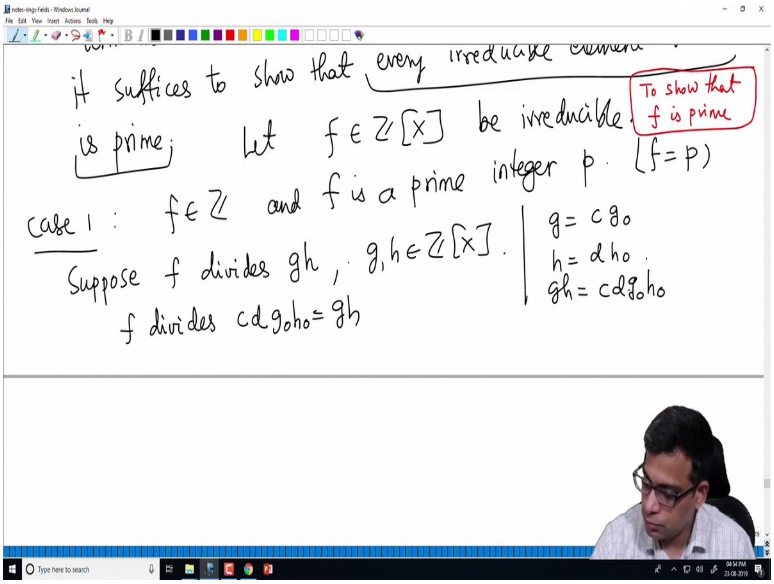
(Refer Slide Time: 17:13)



So, finally, our main theorem Z X is a UFD. This is the goal of this whole theory. The proof is we already know Z X is noetherian right by Hilbert basis theorem Z X is noetherian because Z is noetherian. So, factoring terminates; remember in an integral domain factoring terminates if the ascending chain condition on principal ideals stabilizes. In fact, in Z X ascending chain of a condition holds for every chain of ideals. So, it is a stronger condition. So, it; so, factoring terminates so, to show that Z X is a UFD, it suffices to show that every irreducible element in Z X is prime, right.

So, this is also something we did in the previous video. In an integral domain where factoring terminates that integral domain is UFD if and only if every irreducible element is prime. So, that is what we are going to show. So, we are going to show that every irreducible element of Z X is prime.

(Refer Slide Time: 18:47)

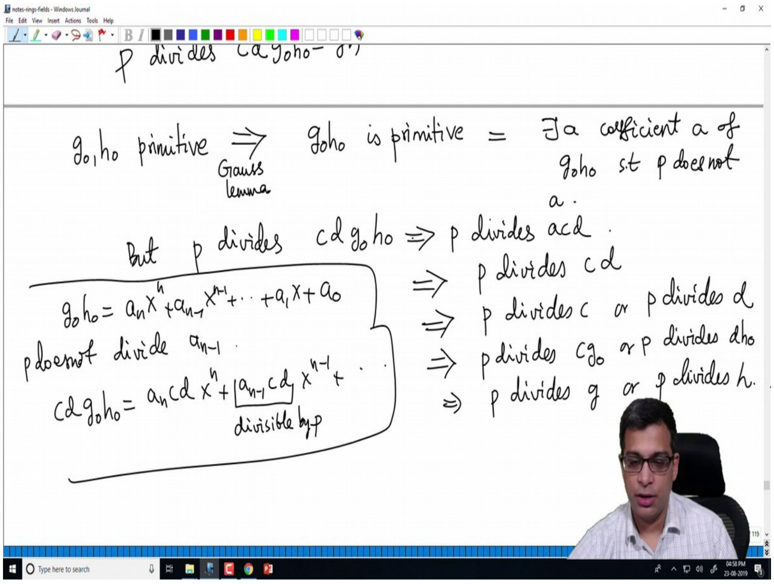


So, in order to do this, let us take an irreducible element. You see where the previous proposition, now will come in handy. So, let f be an irreducible element, we have two cases; by the previous proposition f is actually a constant; in other words which is degree 0. In other words, it is in Z and f is a prime integer, right. So, f is not the normal way of writing prime integer. So, let us call it p so; that means, f is equal to p. So, this is case 1. So, it is actually a degree 0 polynomial in which case it is a prime integer.

Suppose so, it is very easy here, but I will just go through the proof again for completeness. So, what is the meaning of being prime? So, actually I should call this case 1 by the way, what are we trying to show? f is irreducible, we want to show that f is prime that is the goal.

You want to show f is prime, what is the meaning of being prime? Prime means if f divides a product of two elements in Z X f divides one of them. So, suppose f divides g h where g and h are in Z X. We would like to conclude that f divides either g or f divides h. So, now, using again the big tool for us is that every polynomial can be written as a content times a primitive polynomial. So, we do that here g is equal to c g 0 h equal to d h 0. So, we write it like this, g is cg 0 h is d h 0. So, now, f divides g h; that means, f divides c d g 0 h 0 right because that is what g h is. So, g h is c d g 0 h 0.

(Refer Slide Time: 20:55)



So, f divides that, but remember g 0 h 0 are primitive. This implies g 0 h 0 is primitive the product is primitive again Gauss lemma. So, this is Gauss lemma. What does that mean? What is a primitive polynomial? It means that the coefficients of g 0 h 0 have no common factor. So, by the way I have called f equal to p. So, I am going to stick to that. So, actually maybe I will write p. So, p divides g h. So, p divides c d g 0 h 0.

But g 0 h 0 is primitive; that means, there is no common gcd of all the coefficients of g 0 h 0 is 1; that means, there exists a one of the coefficients; a is a coefficient of g 0 h 0 such that p does not divide. So, what this is not properly stated, but properly written. What I really mean is no prime number divides all the coefficients of g 0 h 0 because g 0 h 0 is primitive.

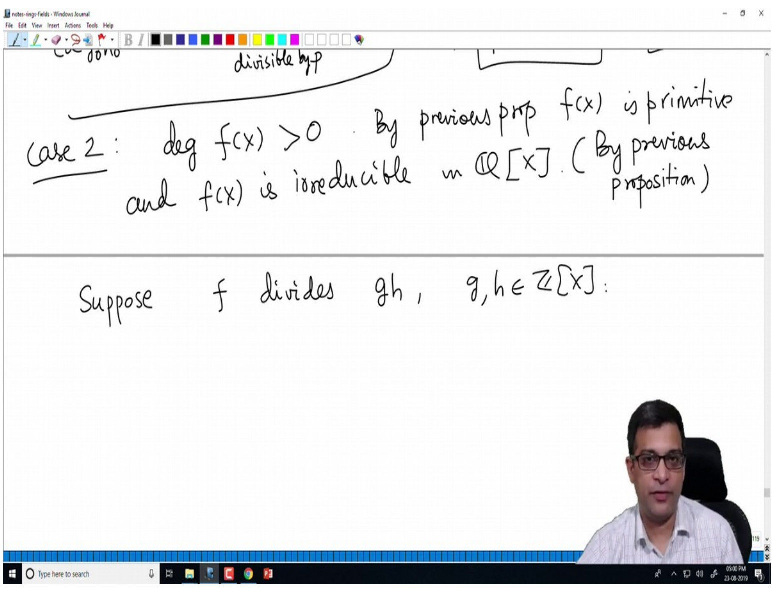
So, let us say let there exists a coefficient a of g 0 h 0 so, that is what I should say: there exist a coefficients a of g 0 h 0 such that p does not divide here. So, think of g 0 as a polynomial g 0 h 0 as a polynomial something X power n plus something times X power n minus one and so on. If p divides all the coefficients g 0 h 0 cannot be primitive right. So, one of the coefficients is not divisible by p so, call that a, but p divides c d g 0 h 0. Remember the coefficient of c d g 0 h 0 one of the coefficients will be a c d. So, p divides a c d, right. So, what am I really saying this is very easy; g 0 h 0 is some something times X power n a n minus 1 X power n minus 1 and so on a 1 X a 0

So, one of these coefficients so, this is just explanation for this. One of these coefficients is not divisible by p. So, let us say for simplicity that p does not divide a n minus 1. Then what is c d g 0 h 0? This is a n c d; c d remember are integers and because we are really dealing with integer polynomials. So, the contents are both integers. So, a n cd X power n an minus 1 c d X power n minus 1 and so on.

So, this now is divisible by p, because p divides the polynomial g h which is actually c d g 0 h 0. So, the coefficients of c d g 0 h 0 is c d a n minus 1. So, p divides a c d, but; that means, p divides, p is a prime number that does not divide a; so, p divides c d. That means, p again prime number; so, p divides c or p divides d, but that means, p divides c g 0 or p divides c or d h 0 ; that means, p divides g or p divides, ok. So, that is all it is a long argument for a very simple fact.

If a prime in; so, what I will be saying is a prime integer in Z X is a prime element that is what we are saying right, a prime integer is a prime element. Because we have taken two polynomials whose product is divisible by p and we concluded that p must divide one of them. So, if it is confusing please just go over this proof again and it should be clear to you because it is not very difficult at this point.

(Refer Slide Time: 25:21)

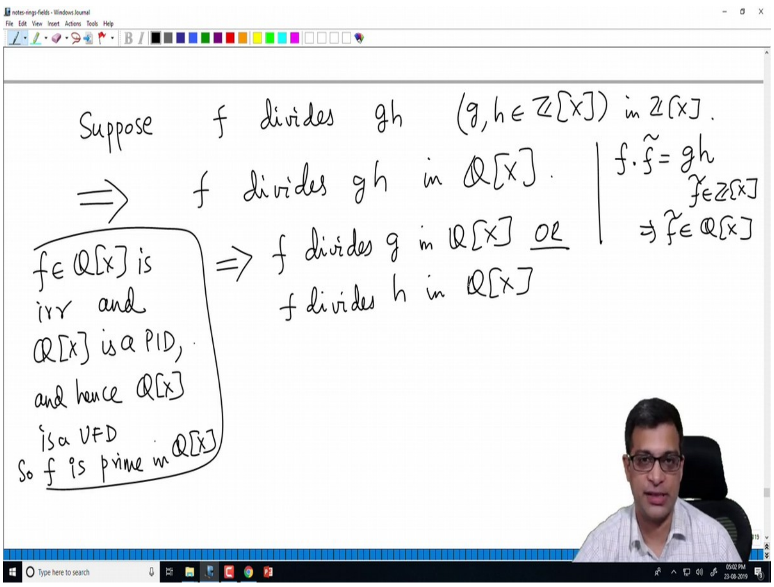


So, suppose now second case, suppose degree f is positive. Remember again I am trying to prove that every irreducible element in Z X is prime. So, I have taken an irreducible element by the previous proposition, it falls into one of the two cases. If it is in case 1, it is degree 0 in which case it is a prime integer; in case 2, it is positive degree by previous proposition f X is primitive. So, f X is primitive and f X is irreducible in Q X right.

So, we know both of these facts. So, any positive degree irreducible polynomial in Z X is primitive and it is also irreducible in Q X. So, this is by previous proposition. This is really the only argument only fact we need to know the rest as you will see is very easy from previous proposition; any irreducible integer polynomial whose degree is positive must be primitive and it is irreducible in Q X.

Now, suppose as before in case one suppose f divides g h where g and h are in Z X. I am trying to prove f is prime; that means, I am trying to prove that if f divides a product of two integer polynomials; I will show that it divides one of them.

(Refer Slide Time: 27:09)



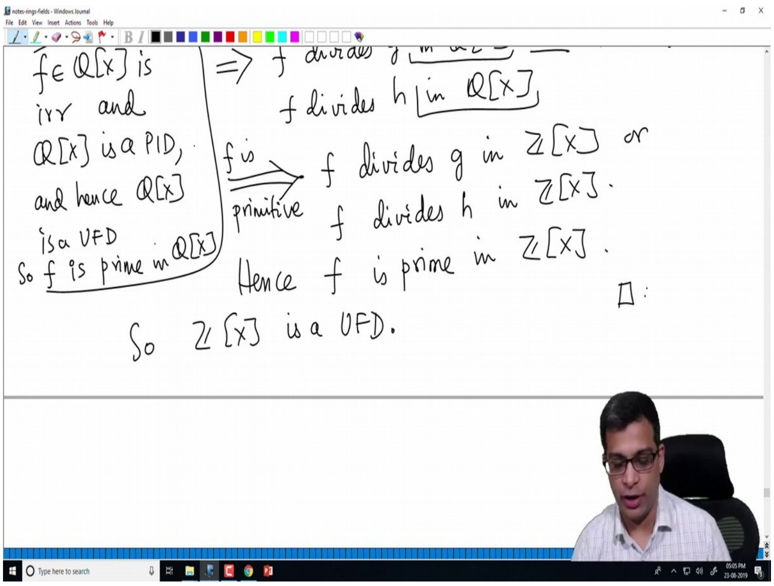
Suppose f divides g h in Z X of course, right by which I mean g and h are in Z X. But this implies that f divides g h in Q X. This is not mysterious right what we know is that f times some f tilde is g h where f tilde is in Z X because f divides g h in Z X means f times f tilde is in g h, but f tilde is also in Q X because f tilde is in Z X it is in Q X. The other way is not always true and for that we need some hypothesis that f is prime primitive and so on, but division in ZX certainly implies division in Q X. So, f divides g h in Q X.

But now f this is what I should emphasize f in Q X is irreducible right that I have said here f is irreducible in Q X and Q X is a PID and hence Q X is a UFD right. This is the sequence of arguments: f is a polynomial in Q X which is irreducible and Q X is so, this is and a PID because it is a polynomial in one variable over a field so, hence a UFD because the PID is automatically a UFD.

So, f is an irreducible element in a PID so, f is prime in Q X. So, any irreducible element is prime. So, f is prime so, f divides g in Q X or f divides h in Q X. In this step, we are using the irreducibility of f along with the fact that Q X is a PID, we are using that f is irreducible in Q X and if it is irreducible in a PID or UFD it is automatically prime.

So, it divides the product then it divides one of them in QX that is the important point.

(Refer Slide Time: 29:27)



Now, we are going to use the primitiveness, f is primitive; if any primitive integer polynomial divides another a polynomial, it divides in if it divides in Q X it also divides in Z X. So, f divides g in Z X or f divides h in Z X and hence f is prime in Z X, ok.

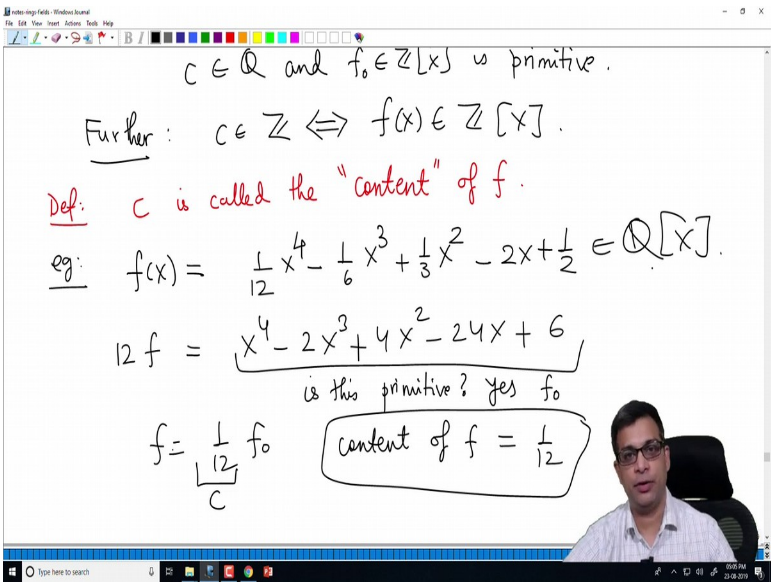
So, just let me review the proof what am I doing I am trying to show that ZX is a UFD; what we want to show is that every irreducible element in Z X is a prime element because Z X already is noetherian. So, factoring definitely terminates in Z X. So, all we need to show is that irreducible elements are prime. Let us take any irreducible element and suppose it divides a product g h, f is irreducible it divides a product g h.

There are two cases; in the first case f is actually a degree 0 polynomial, a constant. In other words in which case it has to be a prime integer and we did that case here a prime integer dividing a product of two polynomials easily implies that it divides one of the polynomials that we have settled here in case 1. In case 2, we are treating the case degree is positive and now by the previous proposition. We have two important assertions f is primitive and f is irreducible in Q X

So, now if f divides g h in Z X it certainly divides g h in Q X because f is irreducible in Q X and Q X is a UFD f is prime. So, f divides g in Q X or f divides h in Q X. Now f is primitive it says that f divides g Z X because if f divides g in Q X f is primitive so, f divides g in Z X; if f divides h in Q X f is primitive so, f divides h in Z X. So, we conclude that f divides either g in Z X or f divides h in Z X and hence f is prime so, Z X is a, ok. So, this is the main result of this video and the last two three videos to conclude that Z X is a UFD.

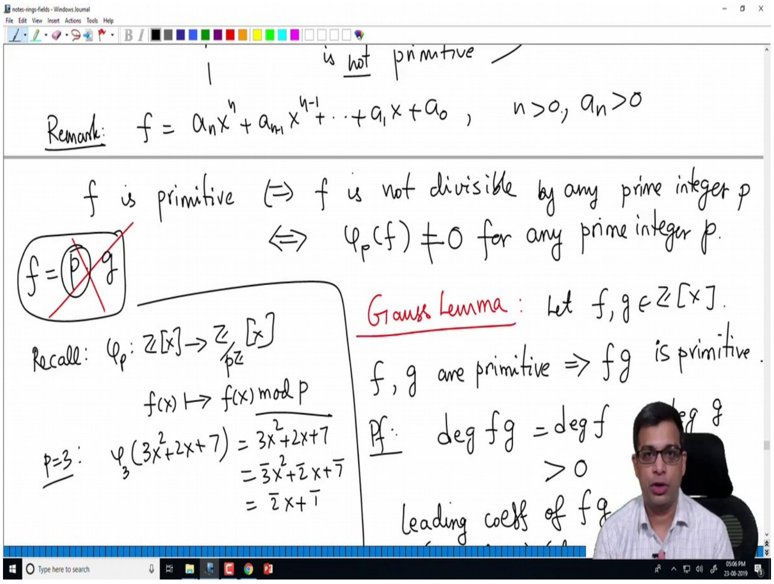
So, let me quickly review this before I make a generalized statement. What we have really done is we have essentially used the fact that the polynomial ring over rational numbers is a UFD.

(Refer Slide Time: 31:59)



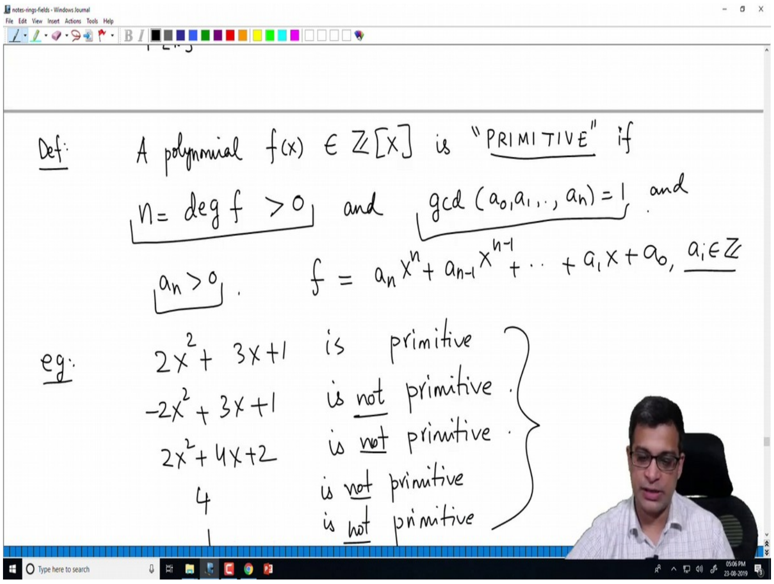
Because that separately we know because polynomial ring in one variable over a field is a PID because we can divide you use Euclidean algorithm to divide using the degree as our size function. So, that is easy to prove is a PID and a PID is UFD we have settled all that.

(Refer Slide Time: 32:27)



Now, to prove that Z X is a UFD what we want to do is basically use the fact that Q X is a UFD. In order to do that we need to understand how to talk about irreducible elements in Z X versus irreducible elements in Q X. Because to prove that something is a UFD, we need to show that factoring terminates and factoring is unique. In ZX because its noe-therian factoring terminates automatically, there is no problem. Only thing to show is that factoring is unique and for that the crucial observation is in an integral domain where factoring terminates to prove uniqueness of the factorization. All you need to do is irreducible elements are prime all this was done in the previous videos. So, we want to show prime irreducible elements in Z X are prime.

(Refer Slide Time: 33:07)



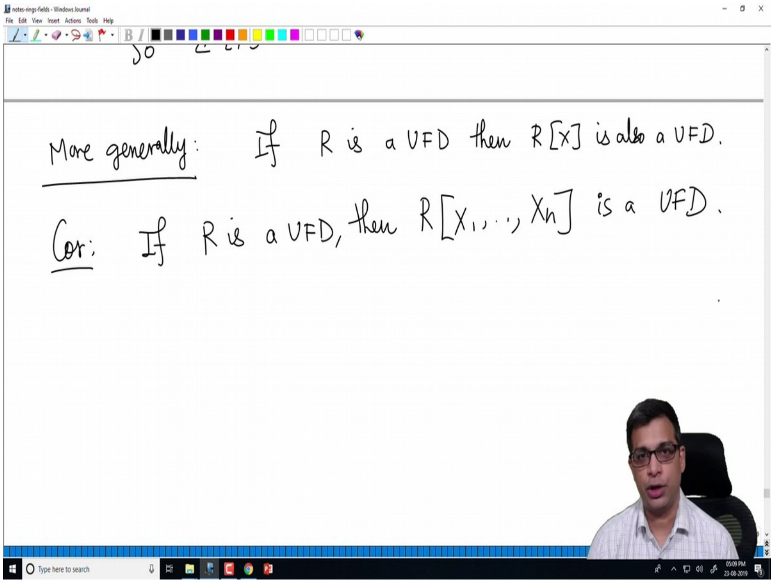
In order to do that we have defined primitive polynomials which are automatic which are by definition integer polynomials. We proved that Gauss lemma which says that two product of two primitive polynomials is primitive and using the Gauss lemma, our important observation is that every rational polynomial can be written as rational number times a primitive polynomial and that is a unique expression.

Once we have that, we are able to prove this very crucial observation that if you have two integer polynomials f and g, and f is primitive and f divides g in Q X f divides g in Z X. See this is in general not true that if a two integer polynomials have this property that one divides the other in Q X, it does not mean that it divides it in Z X; we need the fact that it is primitive. So, I will in the next videos when I do problem sets, I will show why this primitive is important assumption. So, this is supposed to be just a review. So, let me quickly review this.

So, using this observation we have characterized irreducible polynomials in Z X they are either degree 0 in which case they are just prime integers or they are positive degree in which case they are primitive and irreducible in Q X. Using that we have finally settled that Z X is a UFD ok. So, all this is very important and somewhat confusing perhaps.

So, please make sure that you watch this again if you need to and understand this proof; this is a very crucial theorem in this whole course.

(Refer Slide Time: 34:41)



And now, more generally I will say this without proof. We can prove that if R is a UFD then R X is the polynomial ring in one variable over R is also a UFD, exactly the same proof carries over R, now we will play the role of Z and Q will be replaced by the field of fractions of R everything goes through. So, you can do this as a good exercise, you can step by step check all the statements and prove it in this general case.

Hence, we can say by corollary if R is a UFD, then R polynomial ring in any number of variables finitely many is a UFD, ok. So, if because this is just like Hilbert basis theorem if R is noetherian, R X is noetherian then R X another variable is also noetherian; similarly if R is a UFD R X is UFD. So, you can keep adding variables at each stage you have a UFD.

So, in the next stage you are adding one more variable it is a UFD. So, this is the conclusion of this video we have proved a very important result for Z and Z X and it is not difficult to show that the whole proof carries over for any UFD. And finally, you are able to show that if R is a UFD, R X 1 X 2 X n a polynomial ring over R infinitely many variables is also a UFD.

So, I will stop the video here. In the next video, we will do some more results; one of them being Eisenstein criterion using this circle of ideas and then we will do some problems.

Thank you.