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

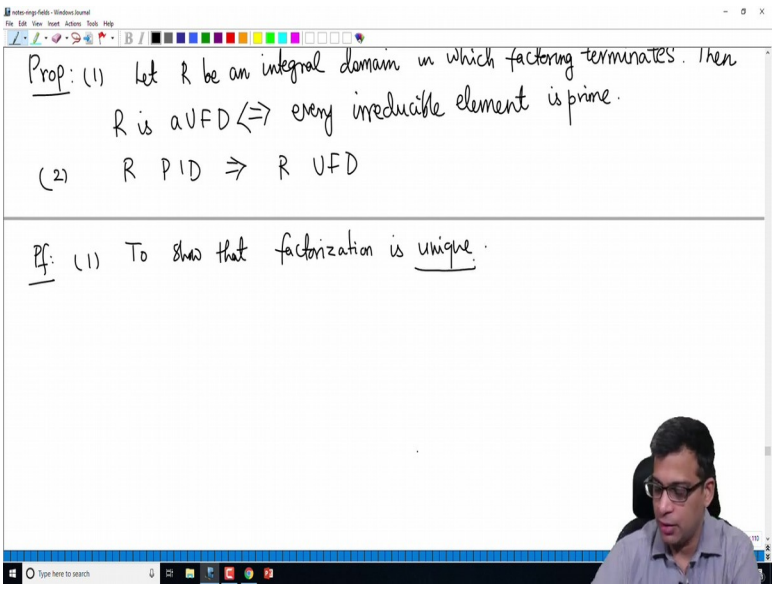
Lecture – 27
Unique Factorization Domains 2

Let us continue with our study of Unique Factorization Domains. I defined in the last video what a unique factorization domain is right, it is a ring which is an integral domain where factorization exists and is unique. And, we also looked at examples where the ring does not have factorization. So, they there is no factorization, if you do start factorizing an element it keeps going and you never stop.

But in most nice rings that we normally deal with factorization, factorization does exist. For example, we proved that factorization exists in a ring, if the principle ideals satisfy ascending chain condition, in particular if you have a Noetherian ring, factorization exists. Then the question is Noetherian ring certainly factorization exist, the question then becomes, is it unique and we saw that it is not in general unique.

For example, we looked at the ring Z adjoined square root minus 5, it is a Noetherian ring. So, factorization exists, but we know that it is not unique. And, we want to continue that study today, we want to give a few more conditions for verifying that a ring is a UFD.

(Refer Slide Time: 01:25)



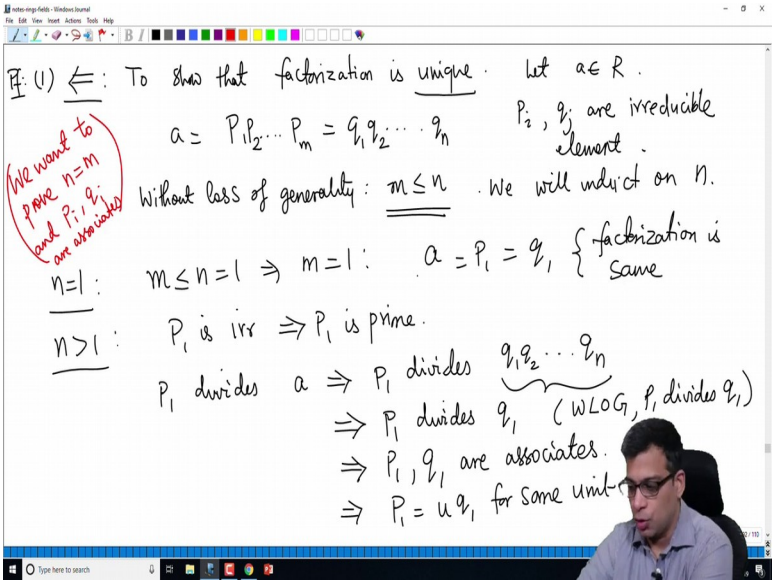
So, let me start today with this proposition. So, it has two parts: the first part says let R be an integral domain in which fact in which factoring terminates. So, as I told you just now you keep in mind any Noetherian ring, it has this property. It need not be Noetherian even non-Noetherian rings have this property, but Noetherian rings do have this property and we know lots of Noetherian rings. Then we say that R is a u f, then we can say that R is a UFD if and only if every irreducible element is prime.

If you recall from a couple of videos back I defined the notion of prime and irreducible elements in an arbitrary integral domain. And we also proved that in any integral domain prime elements are automatically irreducible and we know in general irreducible elements are not prime. In PIDs they are prime because, there is a notion of GCD in PID. So, we use that to conclude that irreducible elements are prime.

Now, we are learning that that is the characterization for UFDs, assuming that factorization terminates and using this part 1 we will prove the second part of the proposition which says that R is a PID implies R is a UFD. So, this is nice; that means, any PID that you know has also the UFD property. So, our examples of UFDs now increase right because, every PID that we know is also UFD.

So, let us do the first part first, second part is a very easy if you think about it because a u f PID in a PID factoring terminates and in a PID every irreducible element is prime. So, PID is automatically UFD. So now, let us do the first part. So, what is it that we have to show? We have to show that factorization is unique, note that in a unique factorization domain there are 3 words unique, factorization, domain; by hypothesis our ring is domain integral domain. It has factorization so, the only remaining thing is that it that the factorization is unique. So, let us prove that.

(Refer Slide Time: 04:07)



So, what does that mean? So, let a be any element of R and suppose it has 2 potential factorizations. So, let us call them p 1 through p m, p 1 dot p 2 p 1 times p 2 times p 3 and so on up to p m and at the same time let say it has another factorization q 1 dot q 2 dot q 3 dot q n. So, what is the hypothesis here? p i's and q j are irreducible elements ok. So, actually what I am now doing is the first part is an if and only if statement right.

First part says that a ring is a UFD if and only if every a irreducible element is prime, assuming that the ring is an integral domain and factorization terminates in that ring. So, I am proving one direction of this. So, I am using I am assuming that every irreducible element is prime and I will prove that it is a UFD and to prove UFD we just need to show that factorization is unique. So, I have taken a arbitrary element, written two possible factorizations.

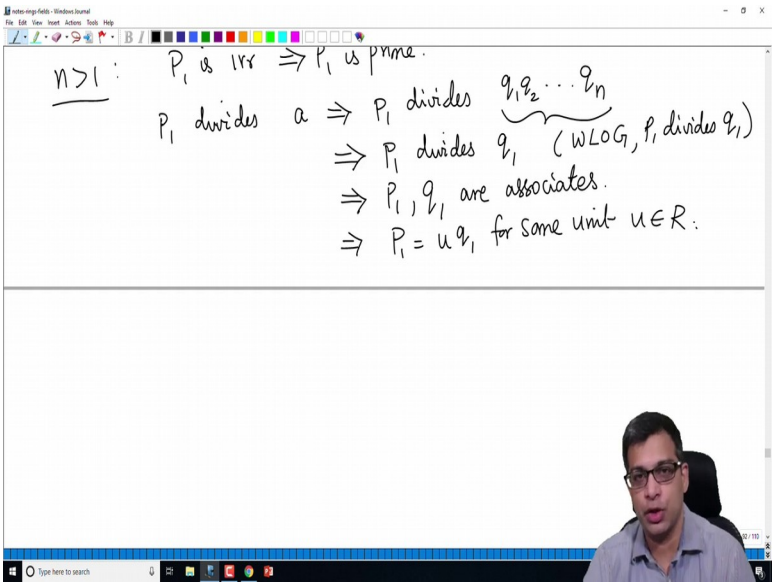
What we want to prove is, we want to prove we want to prove that n equal to m and p i equals q i after permuting them right. So, of course, if you write p i's in a different order we do not think of that as a different factorization. So, 2 times 3 is same as 3 times 2 in the integers, but that is not a that they do not give two different factorizations of 6. So, after permuting; so, I should really write this after permuting if necessary p i's is q i's.

So, let us prove this. So, without loss of generality we can assume that m is lesser than or equal to n right; m is a number p i's, n is a number of q j's. Assume that m is lesser than or equal to n and we will induct on n ok. So, n is a positive integer, the number of q i's q

j's. So, we will induct on n; so, the base case is n equal to 1. If n equal to 1 then m is less than or equal to n; that means, m is also equal to 1. That means, what?

So, we have a is equal to p 1 equals q 1 and that is it, right so; that means, factorization is same so, this is trivial. So, if n equal to 1 the factorization is same there is nothing to prove there, base case is trivial. So, now suppose n is strictly more than 1. So, we have the factorization that I have written p 1 times p 2 times p m, q 1 times q 2 times q n.

(Refer Slide Time: 07:09)

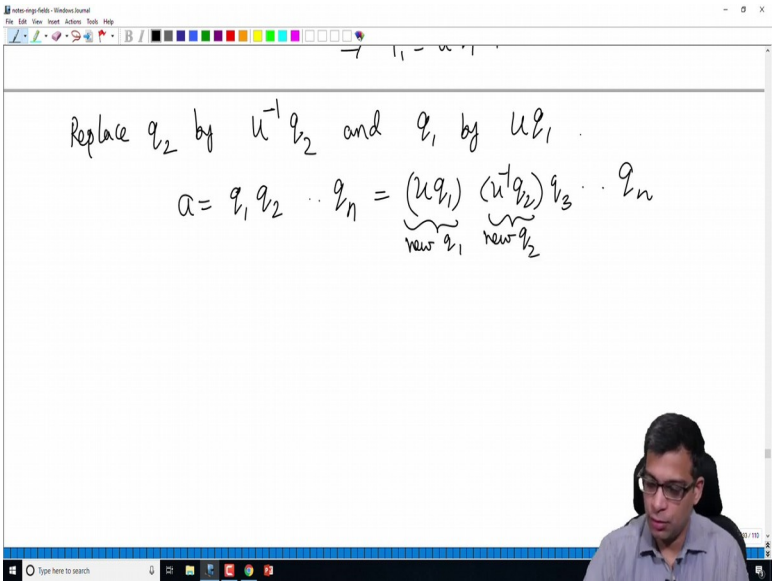


Now, note that p 1 is irreducible, this implies p 1 is prime by hypothesis because I am assuming that every irreducible element in our ring is a prime element. p 1 is irreducible because we have take an irreducible factorization and by hypothesis of the proposition it is prime. Now, what we know is that p 1 divides a right, a is equal to p 1 times p 2 times p n. So, p 1 divides a implies p 1 divides q 1 times q 2 times q 3 all the way up to q n it divides this product. But, a prime element if it divides a product it divides one of them.

So, say p 1 divides q 1. So, we can assume without loss of generality that p 1 divides; note that p 1 divides one of them may be divides q 2, but I can call that q 1. There is no reason for us to not change these things; so, I am going to assume that p 1 divides q 1. But, remember p 1 is an irreducible element, q 1 is an irreducible element. How can an irreducible element divide another irreducible element? This happens only if p 1 and q 1 are associates; remember; that means, 2 elements are associates, if one is a unit times the other. So, p 1 divides q 1 both are irreducible; that means, p 1 and q 1 are associates.

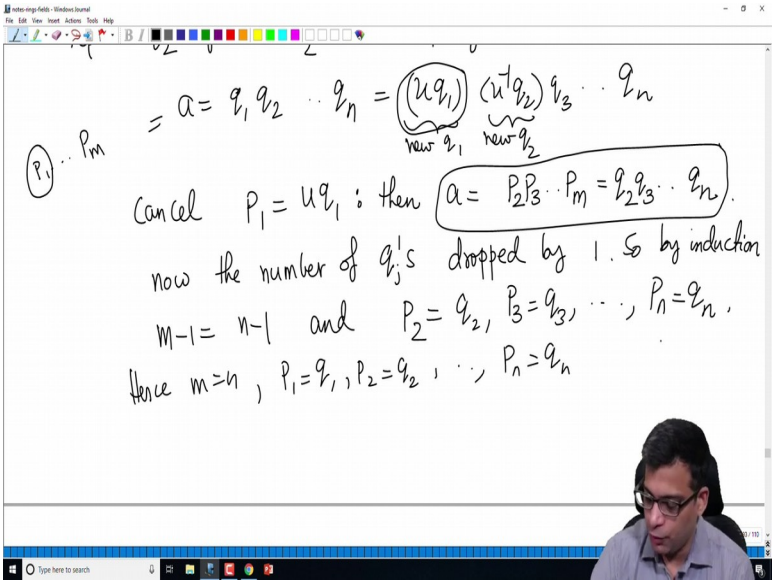
So that means, we can write p 1; so, I am going to write this as p 1 is equal to u times q 1 for some unit u in R right. This is the only possibility, if we have two irreducible elements for example, in the ring of integers 2 is an irreducible element minus 2 is an irreducible element. And, 2 divides minus 2 because 2 is minus 2 times minus 1 whereas, 2 and 3 are not associates and they do not divide each other. So, p 1 is u 1 u times q 1.

(Refer Slide Time: 09:17)



Now, I am going to replace q 2 by u inverse q 2 and q 1 by u q 1. So, then what do I have? A is equal to I am not changing anything q 1 q 2 up to q n, I am writing this as u q 1 u inverse q 2 q 3 up to q n. So, nothing is changed, I am just calling this new q 1 and this is new q 2 ok.

(Refer Slide Time: 09:57)



So, that means and we now know that this also has other factorization p 1 through p m. So now, p 1 the first term in this factorization is same as the first term in this factorization. So, we can cancel this. So, cancel p 1 equals u q 1. So, what do we have then? Then a is equal to p 2 p 3 up to p m equal to q 2, q 2 is actually this u inverse q 2, but q 3 up to q n right.

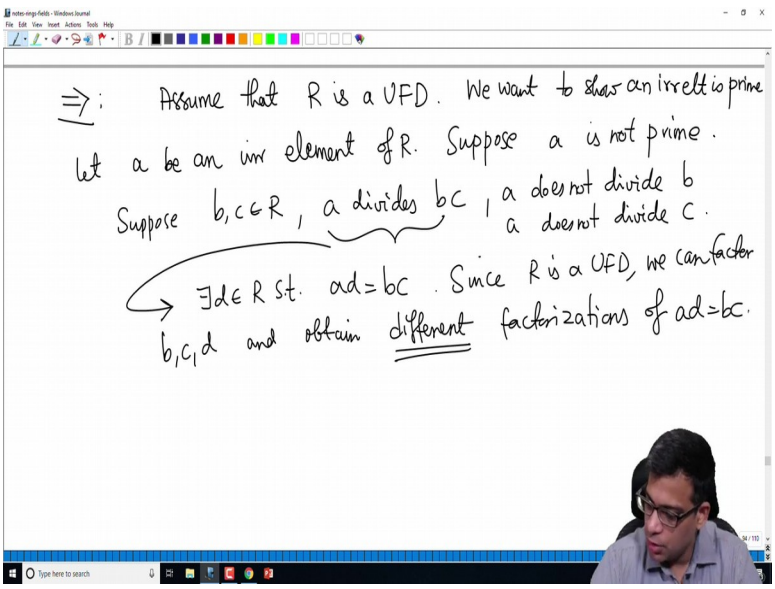
So, we have now again two possible different factorizations of a, but with one less q i. So now, the number of q j's dropped by 1. So, induction so, by induction remember that we are inducting on n, n equal to 1 we have settled and we have taken an n; that means, up to n minus 1 we have solved the proposition, proved the proposition. So that means, by induction m minus 1 equal to n minus 1 and p 2 equal to q 2 p 3 equal to q 3 and so on ok.

So, we have proved this by induction so; that means, hence m equal to n and so on, p 1 equal to q 1 because I have replaced q i by u q 1. So, p 2 equal to q 2 p n equal to q n which is what we wanted to prove right. We have taken two possible irreducible factorizations and proved that really what we have proved is that, the number of irreducible factor is same and the irreducible factors are associates of each other ok.

So, I really should say when I write p i is equal to q i I am not really claiming that they are same, but I am claiming that they are associates. So, we have shown this. So, I should correct this p i and q i are associates so, we have proved that. So, remember replacing,

considering associates does not give us a new factorization. So, we have the same number of irreducible factors in a and in the two factorizations here m and n are same. And, the corresponding irreducible factors are actually associates. So, we have proved one direction right.

(Refer Slide Time: 12:49)



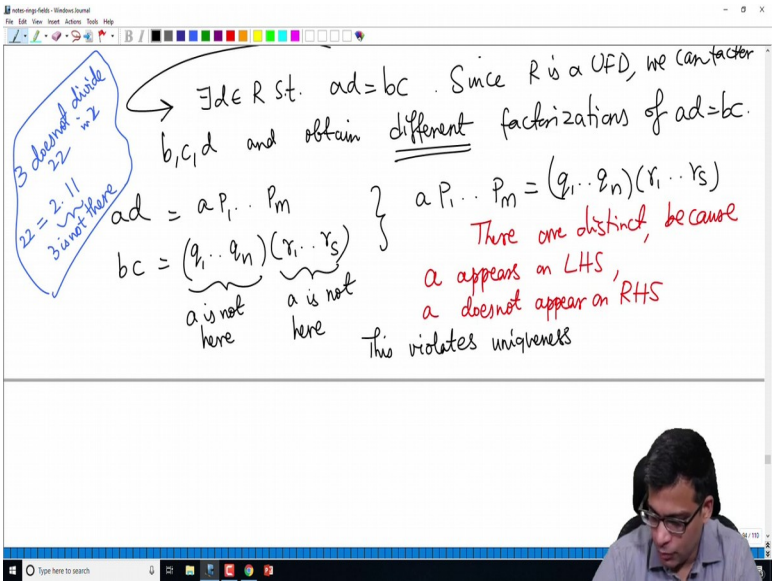
We have shown that if you have an integral domain where factorization is exists and if irreducible elements are prime, factorization is unique. So, R is a UFD ok. So now, that proves one direction of the first part of the proposition, now let us prove the other direction. So now, we assume that R is a UFD. So now, we assume that R is a UFD. What do I have to show? We want to show an irreducible element is prime right.

So, that is the proposition: we want to so show that if you have a UFD then every irreducible element is prime. So now, I am assuming that it is a UFD I will show that every irreducible element is prime. So, let a be an irreducible element of R. Suppose a is not prime, suppose a is not prime. What does that mean? That means, there are 2 elements b and c in the ring R such that a divides the product, but a does not divide b and a does not divide c.

So, suppose b and c are in R and a divides b c, a does not divide b, a does not divide c; that means, a is not prime element we want to get a contradiction. So, if a divides b c this implies there exists d in R such that a d is equal to b c. This is the meaning of remember this is the meaning of an element dividing another element, a d is equal to b c. Now,

since R is a UFD we can factor b, c, d and obtain different factorizations of a d equal to b c. So, what I am really saying is a is already irreducible right.

(Refer Slide Time: 15:25)



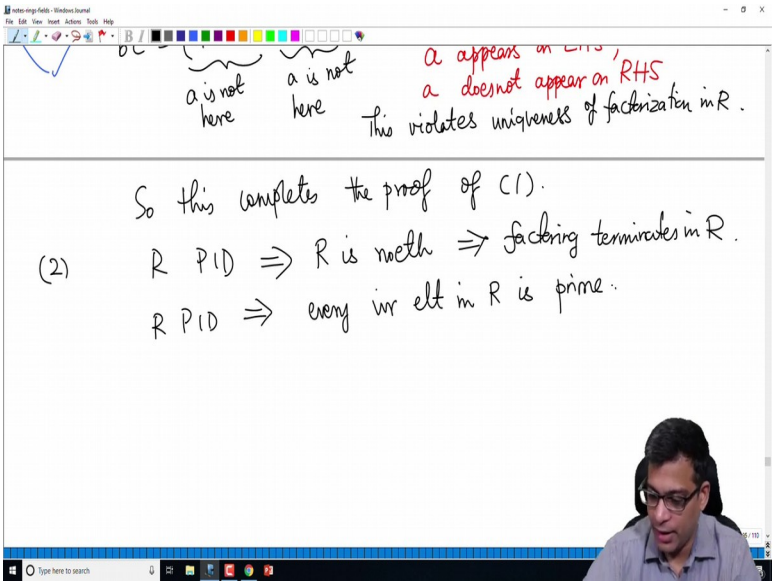
So, we have a d on the one side and b c on the other side. So, a d can be factored as a times a is already irreducible. So, let say d is p 1 times p m, b can be factored as some q 1 times q n and c can be factored as some r 1 times r s right. Every element in UFD factors uniquely into irreducibles so, a is irreducible. So, I am not disturbing a, d can be written as p 1 through p m, b and c are factored like this; that means, we have a p 1 p m is one factorization of a, d q q 1 times q n r 1 times r s is another factorization of b c.

I now claim these are actually distinct. These are distinct why? Because, a appears on the left hand side, a does not appear on the right hand side, a certainly appears on the left hand side. You can see that a is there. Why does a not appear on the right hand side? A does not appear on the right hand side because, remember by hypothesis a does not divide b and a does not divide c.

So, none of the q i's a is not here, remember if an irreducible element divides an another element in a UFD, the irreducible factorization of that second element must contain that irreducible element. And, these are irreducible factorizations of b and c respectively a does not divide them. So, a must not be there right, if 3 does not divide 22; that means, in the factorization of 22.

So, I am just saying something very simple: 3 does not divide 22 in Z right; that means, if we factor 22 as product of irreducible elements you get 22 is equal to 2 times 11, 3 is not there because, if 3 is there then 3 divides 22 by definition. So, if a is one of these q i's or a is one of these r i's then a divides b or a divides c which we know cannot happen. So that means; that means and we have a does not divide b a does not divide c.

(Refer Slide Time: 18:17)



So that means, a is not on the right hand side, a is on the left hand side. But this violates what? Uniqueness of factorization in R right, R is a UFD we are assuming. So, in UFD factorization is unique, but here is one element who is to and we found two different factorizations which violates the uniqueness of factorization of R. So, this completes the proof of 1, again let me remind you this is an very important proposition for us.

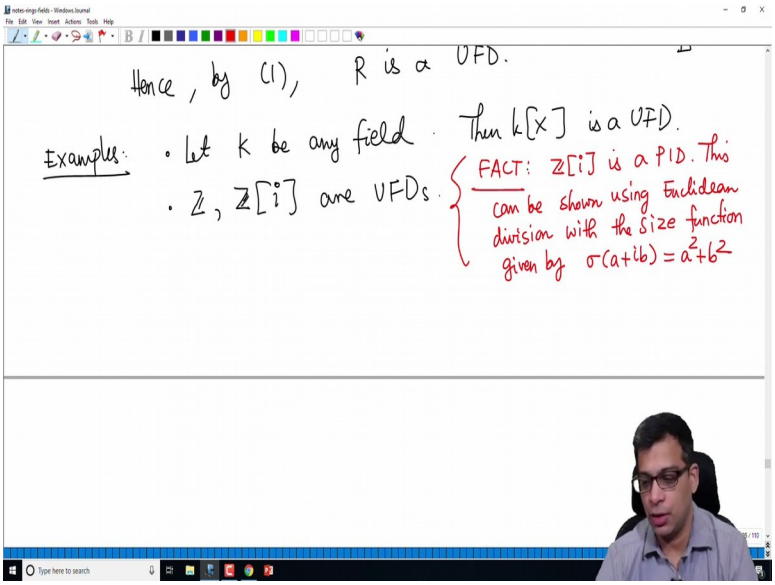
We have said that if you have an integral domain, in which factorization terminates then we now completely characterize UFD; we just need to check whether every irreducible element is prime. So, R is a UFD if and only if every irreducible element is prime. We prove this first by assuming that every irreducible element is prime, we took two potentially different factorizations and showed that they are in fact same.

Then we assume that R is a UFD and then we showed that every irreducible element has prime by assuming by considering a irreducible element which is not prime and obtaining a contradiction. So, that is the proof of 1, let us now prove 2 this is very easy now. If

R is a PID we know that factorization terminates, we can simply say that R is Noetherian, PIDs by definition by definition of PID every ideal is principle.

So, every ideal is certainly finitely generated. So, R is Noetherian so, factoring terminates in R. So, we can apply 1, remember the hypothesis were 1 is R is integral domain and factoring terminates in R. A PID is automatically an integral domain and now we have shown that factoring terminates in R. Now, to use 1 and conclude that R is a UFD, we show that every irreducible element in a PID not show we recall. We have already proved this, if R is a PID every irreducible element in R is prime.

(Refer Slide Time: 20:29)



Hence, by the first part of the proposition R is a UFD, nice. So, the second part is also now complete. So, we have shown that any PID is a UFD. So, immediately that tells us that the following are UFDs. So, let k be any field then k X, the polynomial ring in one variable over k is a PID is a UFD. We already know that it is a PID because, we can divide elements in k X using Euclidean division using the degree as our size function so, it is a UFD.

Similarly, Z of course, is a Z of course, is a UFD that we know, but we know also that Z i are UFDs. Z is something that we are familiar with of course, Z every element is principle. So, UFD PID hence UFD, but in school for example, you know that integers can be factored uniquely into a product of prime members. So, that is already known to us that Z is a UFD. The new thing is Z i is a UFD; so, I do not recall if I commented on this. So,

I will just comment this without proving it recall Z i is a PID; this can be shown using Euclidean division for the with the size function given by.

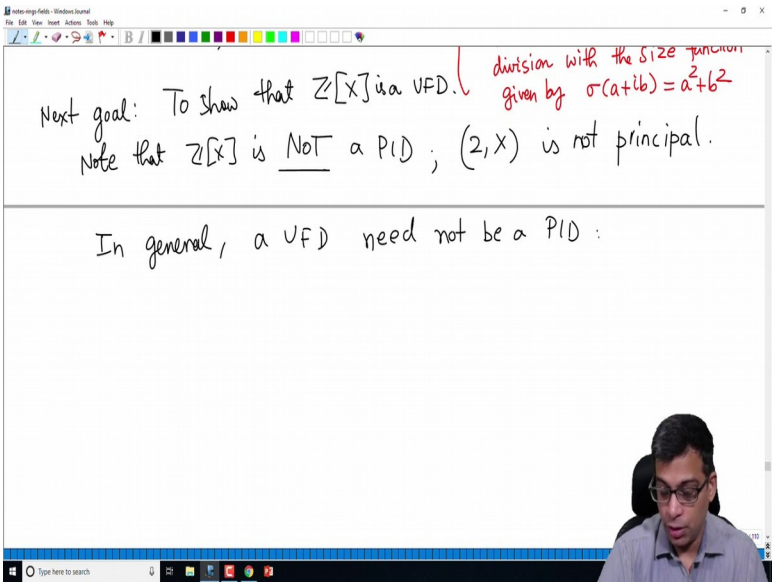
So, size of some a plus i b, remember an element of Z i is an element of the form a plus i b where a and b are integers. So, if you take the size function to be this so, this is a fact for us. So, maybe I will write that as a fact, I am not planning to do this in this course, but its not difficult to show this.

You can read this in Artin's book for example, just like we have shown that Z is a PID, where the size function is just the absolute value. You can divide any integer by another integer. Similarly, polynomial ring in one variable or a field, the size function it just the degree of a polynomial; that means, size of any polynomial is equal to its degree.

Then we can divide and insure that the remainder has a smaller size, meaning reminder has smaller degree. In this case the size function is this so, and we can perform the Euclidean division and show that every ideal is actually generated by a single element. So, what do we do? We take an ideal and take inside that ideal an element with the least size and then show that that generates the entire ideal. So, this is a fact that you can use in the exams and assignments. So, Z is Z i is a PID; so, it is a UFD by the proposition that we just proved. So now, that is good; so, we have got and hold of some more examples of UFDs.

But in the proposition second part we only said that PID implies UFD. The question is the converse to true? Does a PID is a UFD also a PID? And, the answer is no.

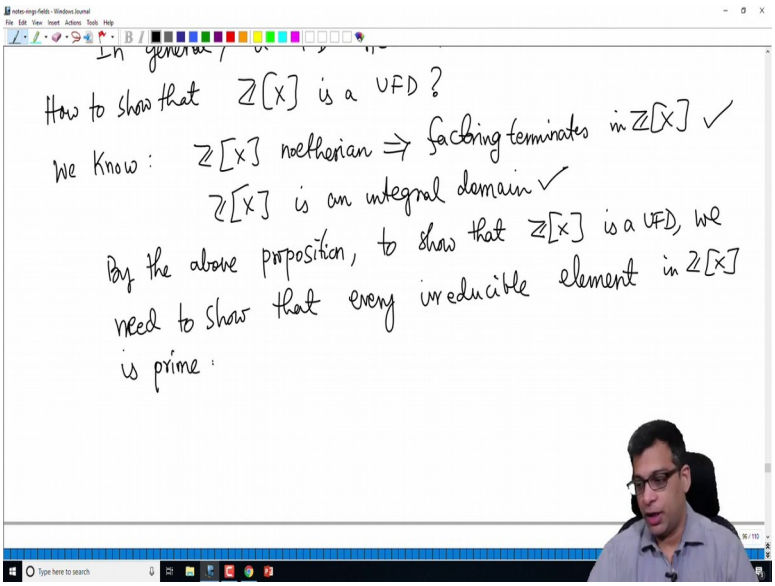
(Refer Slide Time: 24:15)



So, the next goal for us is to show that, this what I will do in the rest of this video and then the next video to show that the polynomial ring in one variable is a UFD. And, this immediately tells us that a UFD need not be a PID. So, note that Z X is not a PID right. Why is it not a PID? The ideal for example, generated by 2 and X is not principle.

We saw this in the video when we discussed PID's we saw this, the ideal generated by 2 X is not a principle ideal. So, Z X is not a PID whereas, we will prove that Z X is a UFD. So, in general in other words a UFD need not be a PID, a UFD is not necessarily a PID ok. So, the goal and it requires a proof and it will take us a little bit of time, but we will prove that Z X is a UFD. So, as an attempt what do we do?

(Refer Slide Time: 25:33)

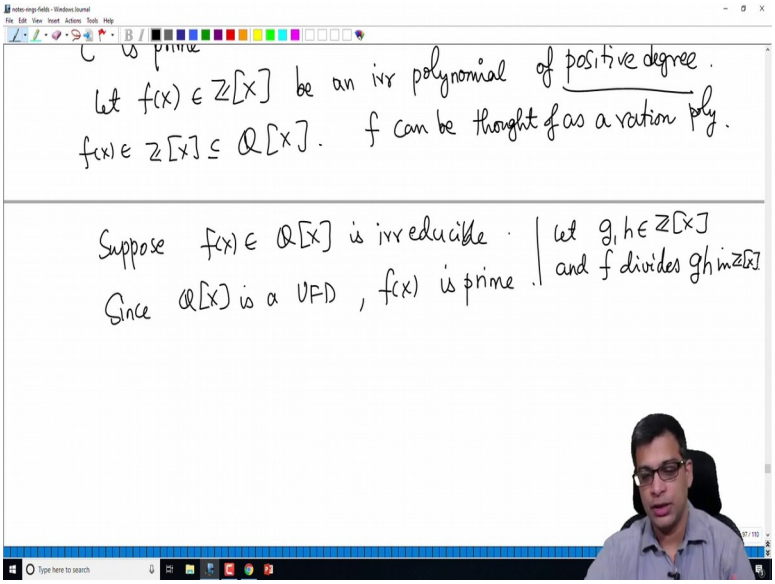


So, what is how to show that Z X is a UFD? So, I am we are going to use all the results that we have so far showed. So, we know Z X is Noetherian right. The Hilbert basis theorem says that if R is Noetherian, the polynomial ring over R in one variable is Noetherian. So, Z is Noetherian for sure, Z X is Noetherian. So, factoring terminates in Z X that is not a problem, that is good. So, the first part is clear, unique factorization domains Z X is the domain. So, let me just write that for clarity.

So, Z X is an integral domain, Z X is Noetherian; so, factoring terminates. By the proposition above, by the above proposition to show that Z X is a UFD we need to show that every irreducible element in Z X is prime; every irreducible element is a prime element ok. So, that is all right, in the first part of the previous proposition we saw that an irreducible element; if you have an integral domain we are factoring terminates. And, if every irreducible element is prime that integral domain is automatically UFD. So, we have going to do this part; so, this is what we will do.

So, there are two kinds of irreducible elements in Z X one is prime numbers 2, 5, 3, 7, 11 and so on. So, we want to show that those are prime which is the easy part, every irreducible integer is actually a prime integer.

(Refer Slide Time: 27:51)



The other thing is we want to show; so, I am going to give you a preview of what we want to do. So, let us say this is an irreducible element. What is an irreducible element? Irreducible polynomial; so, as I said there are two kinds of irreducible elements. One is actually integers which are irreducible in other words prime, other is irreducible polynomials which are of positive degree.

So, I am going to take a, we will settle both cases, but first we will take an irreducible polynomial of positive degree right. Remember if you recall the definition of an irreducible polynomial, it says that it cannot factor into polynomials of smaller degree which is exactly the definition of irreducible element in an arbitrary integral domain. It has no factorization into further other elements other than units and associates. So, let f be an irreducible polynomial.

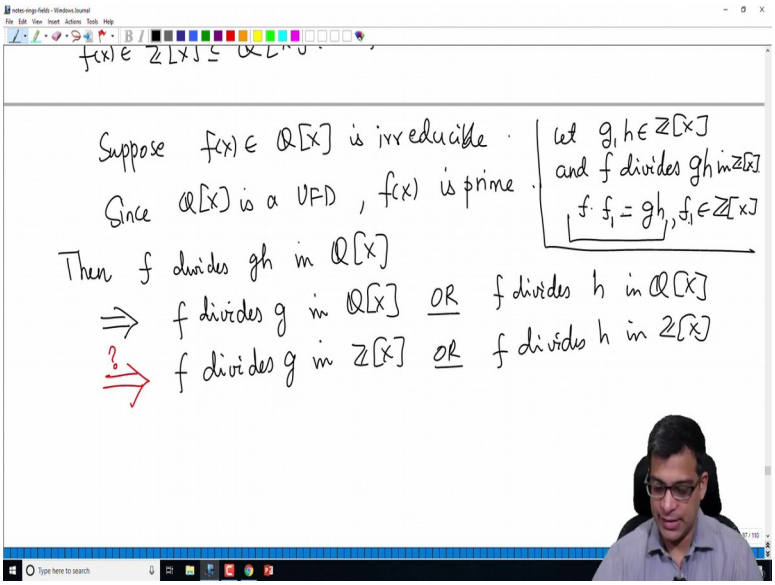
So, note that Z X naturally its sits inside Q X right; so, Z X naturally sits inside Q X. So, f is given here so, f can be thought of as. So, f is an integer polynomial, but it can be thought of as a rational polynomial, this is the first observation. So, it can be thought of as a rational polynomial. So now, suppose its irreducible as a rational polynomial, suppose f X is irreducible.

See we are assuming that it is irreducible in Z X, we have to prove that it is also irreducible in Q X that we will show later; suppose it is irreducible. Now, since Q X is UFD, remember Q X is polynomial ring or a field in one variable. So, it is a PID, hence it is a

UFD. So, f X is prime f X is a prime element; that means, suppose now let f and g and h be two integer polynomials.

And, suppose f divides g h; remember what I am trying to do; I am trying to show that every reducible element in Z X is prime, f, I have taken an irreducible polynomial of positive degree. Suppose, it divides a product of two polynomial g h in Z X, this distinction is important for us. So, f divides g h in Z x; that means, there is another polynomial such that f times that polynomial is equal to there is another integer polynomial, such that f times that is equal to g h.

(Refer Slide Time: 30:43)

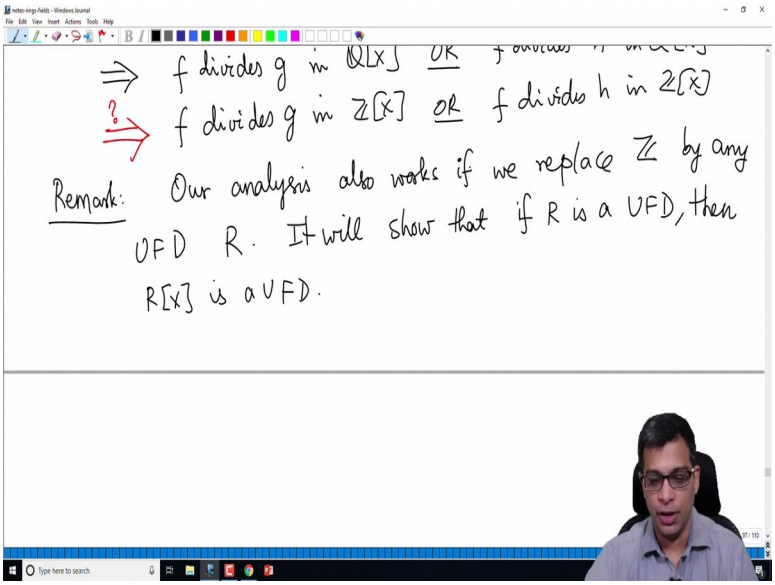


But certainly then f divides g h in Q X also because right; that means, f times sum f 1 is g h where f 1 is in Z X. If f 1 is in Z X f 1 is also in Q x so, this equation also holds in Q x so, f divides g h in Q X. But, this means because f is a prime element of Q X f divides g in Q X or f divides h in Q X. Now that means, that f can be written as g can be written as f times something in Q X that something is in Q X or h can be written as f times something that something in Q X.

But, the big question now is does this imply f divides, does this imply f divides g in Z X or f divides h in Z X? Remember f g h are all integer polynomials, but f divides g or f divides h in Q X. The question is does that division also happen in Z X? So, the two things to check is, if you take an irreducible polynomial in Z X, is it irreducible in Q X? And, if a polynomial divides another, an integer polynomial divides another integer polynomial

in Q X does a divide in Z X? So, we were going to address both these questions and conclude that Z X is a UFD.

(Refer Slide Time: 32:31)



So, before I stop I will stop this video and start again next time, but the remark I will make and I will repeat this also in next time is that the same process our analysis that we will perform now also works for if we replace Z by any UFD R ok. So, Z and Z X and Q X is what we are considering, but we can also consider R X and the quotient field of R bracket X. So, and it will show so, this is the ultimate theorem that we will show. It will show that if R is a PID, sorry if R is a UFD then R X is a UFD ok.

This is similar to the Hilbert basis theorem, if R is Noetherian, R X is Noetherian, if R is UFD, R X is UFD. Remember that the same statement is not true for PIDs, we know that Z is a PID, but Z X is not a PID. So, it is only true for UFDs. So, in particular after this we know that all polynomial rings over UFDs are polynomial rings in any number of variables are UFDs because, one we can keep attaching variables one by one.

So, we will stick to Z, but the proof goes through for any UFD. So, that is a good exercise for you, as we are doing all the steps make sure that you prove all the statements for any arbitrary UFD. So, let me stop the video here. In the next video I will continue and prove that Z X is a UFD.