

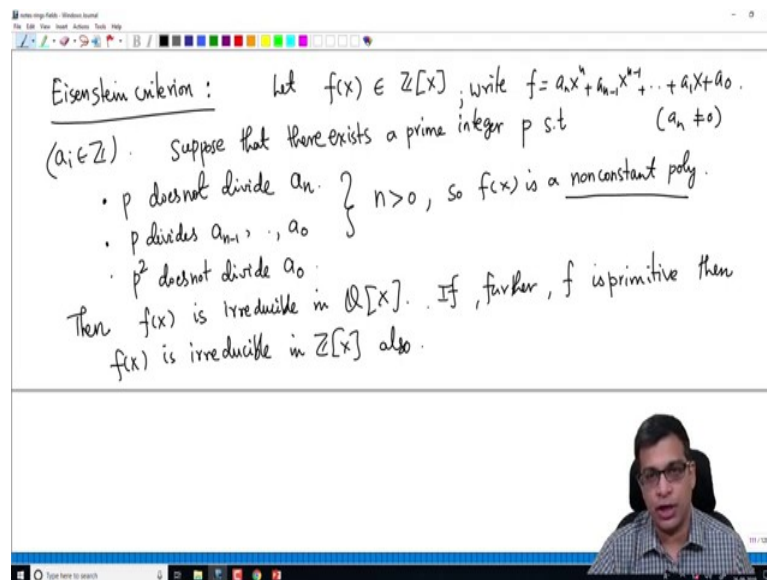
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 30
Eisenstein criterion and Problems 7

In the last video, we looked at polynomial rings over the integers, or polynomial rings in one variable and showed that it is a UFD. In fact, we also commented that with the same proof shows that if R is a UFD, a polynomial ring over R in any number of variables finite number of variables is a UFD. In the crucial facts we use were the notions of primitive polynomials and Gauss lemma, and using that we have written any rational polynomial as a rational number times a primitive polynomial and that allowed us to compare irreducibility over the integers and irreducibility over the rationals. And we ended with the important theorem which says $\mathbb{Z}[X]$ is a UFD.

So, today I am going to use those ideas to prove a very important criterion for verifying that polynomials are irreducible over integers or rationals, and it is called Eisenstein Criterion, ok.

(Refer Slide Time: 01:10)



Eisenstein criterion: Let $f(x) \in \mathbb{Z}[x]$, write $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. ($a_n \neq 0$) ($a_i \in \mathbb{Z}$). Suppose that there exists a prime integer p s.t.

- p does not divide a_n .
- p divides a_{n-1}, \dots, a_0 .
- p^2 does not divide a_0 .

$n > 0$, so $f(x)$ is a nonconstant poly.

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$. If, further, f is primitive then $f(x)$ is irreducible in $\mathbb{Z}[x]$ also.

It is a very useful method to check if a given polynomial is irreducible or not. It does not always work, but it works often and it is very useful to conclude that, irreducibility here.

So, let me just go ahead and write the criterion first. Let f be a rational integer polynomial write f as $a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$. So, since it is an integer polynomial we of course, know that the coefficients are integers.

So, now, suppose that there exists a prime integer there exists a prime integer that means, a prime number in \mathbb{Z} , p such that it satisfies the following conditions, p divides or does not divide, first let me say p does not divide a_n . So, I am assuming whenever I write like this of course, remember, when we write a polynomial like this we will always assume that the leading coefficient is nonzero because we will start with the largest degrees. So n is not 0.

So, suppose p does not divide a_n , p divides a_{n-1} up to a_0 , and also p^2 does not divide a_0 , ok. So, this is the assumption. p divides a_n , p divides a_{n-1} , p does not divide a_n , p divides a_{n-1} through a_0 p^2 does not divide a_0 . So, remember, these two conditions already imply that n is positive. So, f is non-constant polynomial. Remember, that we are asking for p not to divide a_n and p divide p divides a_0 that means, a_n and a_0 are different, that means, f has at least degree 1. So, it is a non-constant polynomial.

So, if this happens what is the conclusion? Then we can immediately say that $f \in \mathbb{Q}[X]$ is irreducible in $\mathbb{Q}[X]$, then $f \in \mathbb{Q}[X]$ is irreducible in $\mathbb{Q}[X]$ that is the conclusion of Eisenstein criterion not that it is irreducible in $\mathbb{Z}[X]$. However, if we also know that if f is primitive, if further f is primitive then $f \in \mathbb{Q}[X]$ is irreducible in $\mathbb{Z}[X]$ also, ok. So, this is a good criterion to prove, so that it actually uses all the notions that we developed in the last couple of videos and it gives us a very useful criterion.

If there is a prime number satisfying some conditions with respect to the coefficients of the polynomial, we can right away conclude that its irreducible in $\mathbb{Q}[X]$. We cannot conclude in general that it is irreducible in $\mathbb{Z}[X]$, but if it is primitive, it is a irreducible in $\mathbb{Z}[X]$.

(Refer Slide Time: 04:49)

$f(x)$ is irreducible in $\mathbb{Z}[X]$ and

eg. $f = 2X^3 - 5X^2 - 10X + 15 \in \mathbb{Z}[X]$; $p=5$ satisfies the hypothesis of the Eisenstein criterion.

So f is irreducible in $\mathbb{Q}[X]$. Since f is also primitive, f is also irreducible in $\mathbb{Z}[X]$.

$f = 12X^6 - 10X^5 + 50X^4 - 10X + 60 \in \mathbb{Z}[X]$. Again $p=5$ works. So f is irr in $\mathbb{Q}[X]$. ✓

So, I am going to give a couple of examples before I prove this. So, for example, if you take X power 3 minus 5 X squared plus 10 X plus 15, right. So, let us take this in the polynomial ring over integers. So, this is a, this is an integer polynomial, then p equal to 5 satisfies the hypothesis of the Eisenstein criterion, right. We might even write something like this.

So, let me write f equals to 2 X cubed minus 5 X squared minus 10 X plus 15. So, it satisfies the hypothesis of the Eisenstein criterion because 5 does not divide 2, a 3 here is 2, right a 3 is 2, a 2 is minus 5, a 1 is minus 10 a 0 is 15. So, 5 does not divide 2, 5 divides minus 5, 5 divides minus 10, 5 divides 15 and 5 squared which is 25, does not divide 15. So, we conclude that f is irreducible in $\mathbb{Q}[X]$, right. This is the conclusion of the Eisenstein criterion.

Since, f is also primitive f is also primitive, right. Why is that? Because. Remember, a primitive polynomial is a positive degree polynomial with positive leading coefficient and such that gcd of all its coefficient is 1. Here the coefficients are 2 minus 5 minus 10, 15 gcd is 1, right. There is no number greater than 1 that divides all these coefficients. So, f is primitive, and hence f is also irreducible in $\mathbb{Z}[X]$. See, this is a very useful criterion as you can see. It may be very difficult in general to conclude irreducibility of polynomials, in this case we have already just immediately concluded that it is irreducible.

So, similarly we can take for example, f as let us say $12X^6 - 10X^5 + 50X^4 - 10X + 60$, I am just arbitrarily writing some polynomial. So, again p equal to 5 works, right. Why does it work? Because if you check 5 it divides all the coefficients other than the leading coefficients, leading coefficient, right, p does not divide 12, but p divides 10, p divides 50, 5 divides 10, 5 divides 60, 5 does not divide 12 and 25 does not divide 60. So, f is irreducible in $\mathbb{Q}[X]$. So, this is, ok. That is immediate conclusion of Eisenstein criterion.

(Refer Slide Time: 08:33)

So f is irreducible in $\mathbb{Q}[X]$.
 f is also irreducible in $\mathbb{Z}[X]$.
 $f = 12X^6 - 10X^5 + 50X^4 - 10X + 60 \in \mathbb{Z}[X]$. Again $p=5$
 Works. So f is irr in $\mathbb{Q}[X]$. ✓
 f is Not primitive: $f = 2(6X^6 - 5X^5 + 25X^4 - 5X + 30)$
 content of $f = 2$ not 1
 f is not irr in $\mathbb{Z}[X]$: $f = 2 \cdot \frac{f}{2}$
 irr irr

What about in $\mathbb{Z}[X]$? For that you have to ask if it is a primitive polynomial? Is f primitive? It is not primitive, right because f can be written as 2 times, you can factor 2, $6X^6 - 5X^5 + 25X^4 - 5X + 30$, right. This is not primitive because the content is not 1, content of f is 2 not 1. So, f is not primitive that means, we do not get that f is irreducible in $\mathbb{Z}[X]$ because clearly you can see that, this gives you a factorization 2 is an irreducible element in $\mathbb{Z}[X]$. So, f can be written as 2 times g , where g is this, right. So, this is irreducible this is irreducible.

So, f can be written as a product of two irreducible polynomials that means, it is not irreducible. Whereas, this is not a valid factorization in $\mathbb{Q}[X]$ because 2 is a unit in $\mathbb{Q}[X]$. So, we this is not a valid factorization in to two proper irreducible divisors, whereas, in $\mathbb{Z}[X]$ it is. So, f is irreducible in $\mathbb{Q}[X]$, but it is not irreducible in $\mathbb{Z}[X]$. So, this gives you an ex-

ample of a polynomial integer polynomial which is irreducible in $\mathbb{Q}[X]$, but it is not irreducible in $\mathbb{Z}[X]$.

(Refer Slide Time: 10:16)

Proof of Eisenstein criterion: consider the natural ring homomorphism:
 $\varphi_p: \mathbb{Z}[X] \rightarrow \mathbb{Z}/p\mathbb{Z}[X]$.

claim: If f is reducible in $\mathbb{Q}[X]$ then it is reducible in $\mathbb{Z}[X]$.
Pf: Write $f = gh$ where $g, h \in \mathbb{Q}[X]$ $\deg g > 0$
 $\deg h > 0$

$f = gh = c g_0 \cdot d h_0 = cd \underbrace{g_0}_{\text{primitive}} \underbrace{h_0}_{\text{content of } f} \Rightarrow f = \underbrace{cd}_{\text{content of } f} \underbrace{g_0 h_0}_{\text{primitive}}$

$c, d \in \mathbb{Q}$
 g_0, h_0 are primitive

So, now this after these examples, I am going to quickly prove the Eisenstein criterion. It is not difficult using the theory that we developed in the last few videos. It is not difficult to now show that, now prove the Eisenstein criterion. So, what we are going to do is consider the natural map ring homomorphism I should say, natural ring homomorphism, homomorphism, ϕ_p from $\mathbb{Z}[X]$ to $\mathbb{Z}/p\mathbb{Z}[X]$.

Remember, what is this ring homomorphism? It takes a polynomial and simply changes the coefficients by the residues mod p . So, given we are, we are given a fixed p , right p is that fixed ϕ_p , given in the statement of Eisenstein criterion, p is a prime number, prime integer that divides all the coefficients of f other than the leading coefficients, coefficient and also p^2 does not divide the constant. So, for that we consider this.

And now, since; what I am now going to do is a simple claim here. If f is reducible, remember, I am trying to show that f is irreducible in $\mathbb{Q}[X]$. If suppose it is not; that means, if f is reducible in $\mathbb{Q}[X]$ then it is reducible in $\mathbb{Z}[X]$. So, first I will prove this claim. Let me comment that in the previous video when we proved that $\mathbb{Z}[X]$ is a UFD, one of the results we proved was if f is a non-constant irreducible polynomial in $\mathbb{Z}[X]$ that means, it is an integer polynomial and in $\mathbb{Z}[X]$ it is irreducible and it has positive degree, then it is also irreducible in $\mathbb{Q}[X]$. In this case f is a non-constant polynomial, so if f is irreducible in $\mathbb{Z}[X]$

it would be irreducible in $\mathbb{Q}[X]$. So, that this claim is proved already. But I am just going to give you a direct proof, so that it becomes more clear to you. Even if the previous argument was not clear, you can follow this, right. This is a more direct argument for this statement.

If f is reducible in $\mathbb{Q}[X]$ then it is reducible in $\mathbb{Z}[X]$. Why? So, write f as gh where g and h are in $\mathbb{Q}[X]$. Remember, what is the meaning of being reducible that means, it can be written as product of two polynomial of positive degree in $\mathbb{Q}[X]$. So, both g and h are non-constants and f can be written like this.

Now, because of the proposition that we did earlier, every rational polynomial can be written as its content times, content times a primitive polynomial. Similarly, g can be written as say g_0 , h can be written as $d h_0$, right. We this is not, now at this point you are comfortable with this I hope. Every rational polynomial can be written as a rational number. So, c, d are in \mathbb{Q} and g_0 and h_0 are primitive, right. So, I am writing gh as cg_0 and $d h_0$ respectively. So, we have this.

Now, remember, g_0, h_0 is primitive because g_0 and h_0 are primitive, their product is primitive like Gauss lemma and f is $cd g_0 h_0$. So, this must be the unique expression of f into its product of its content and a primitive polynomial. So, content of f is cd . But remember f is a, f is an integer polynomial that is given to us, in the Eisenstein criterion f is an integer polynomial.

(Refer Slide Time: 14:27)

claim: If f is reducible in $\mathbb{Q}[X]$ then it is reducible in $\mathbb{Z}[X]$.

Pf: Write $f = gh$ where $g, h \in \mathbb{Q}[X]$ $\deg g > 0$
 $\deg h > 0$

$c, d \in \mathbb{Q}$
 g_0, h_0 are primitive

$f = gh = c g_0 \cdot d h_0 = cd \underbrace{g_0 h_0}_{\text{primitive}} \Rightarrow f = \underbrace{cd}_{\text{content of } f} g_0 h_0$ | g_0, h_0 primitive
 $g_0, h_0 \in \mathbb{Z}[X]$.

f is an integer poly $\Rightarrow cd \in \mathbb{Z} \Rightarrow f = cd g_0 h_0$: factorization of f in $\mathbb{Z}[X]$.

If the conclusion of the Eisenstein criterion is false, then f is reducible in $\mathbb{Q}[X]$. By the above claim, f is reducible in $\mathbb{Z}[X]$.

This means cd is in \mathbb{Z} , right because content is a for an integer polynomial content is an integer. Content is simply then the gcd of its coefficients. So, cd is in \mathbb{Z} that means, f can be written as $g_0 h_0$, right. And remember, $g_0 h_0$ are primitive that means, by definition they are in $\mathbb{Z}[X]$. So, they are in $\mathbb{Z}[X]$ that means, here is an irreducible factorization here is a factorization of f . Remember, the degree of g_0 and h_0 are equal to degree of g and degree of h , respectively, because c and d are constants. When you write g as $c g_0$, g and g_0 have the same degree. So, this is factorization of f in $\mathbb{Z}[X]$.

That means, if we started with the factorization in $\mathbb{Q}[X]$ a priori g and h may not be integer polynomials we may have that they are only rational polynomials. But by writing them as product of their contents and primitive polynomials and observing that the product of the contents is an integer, we can write this. So, this is actually not f is equal to $cd, g_0 h_0$, I should not say f is equal to $g_0 h_0$, it is $cd g_0 h_0$. So, it is an irreducible factorization, it is a factorization into product of smaller degree polynomials, hence f is not irreducible in $\mathbb{Z}[X]$ that means, f is reducible in $\mathbb{Z}[X]$.

So, now, if the conclusion of, now, I am going to go back to the proof of Eisenstein criterion. If the conclusion of the Eisenstein criterion is false then f is reducible in $\mathbb{Q}[X]$, right. If the conclusion of the Eisenstein criterion is false, then f is reducible in $\mathbb{Q}[X]$. By the above claim f is also reducible in $\mathbb{Z}[X]$, right, it is reducible in $\mathbb{Z}[X]$ claim is if a polynomial is reducible in $\mathbb{Q}[X]$, then it is reducible in $\mathbb{Z}[X]$. So, it is reducible in $\mathbb{Z}[X]$.

(Refer Slide Time: 17:09)

in $\mathbb{Q}[X]$. By the above claim, ...

Write $f = gh$, $g, h \in \mathbb{Z}[X]$. Now consider the image of f by $\varphi_p: \mathbb{Z}[X] \rightarrow \mathbb{Z}/p\mathbb{Z}[X]$. $\varphi_p(f) = \varphi_p(gh) = \varphi_p(g)\varphi_p(h)$

$\varphi_p(f) = \varphi_p(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0)$
 $= \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + \dots + \bar{a}_1 x + \bar{a}_0 = \bar{a}_n x^n \neq 0$ | p does not divide a_n

*p divides a_{n-1}
 p divides a_{n-2}
 p divides a_1
 p divides a_0*

So, I am going to now write f as g times h , g times h , g and h in $\mathbb{Z}[X]$. Now, consider the image of f in $\mathbb{Z}/p\mathbb{Z}[X]$ that are equal to earlier, φ_p is the map from $\mathbb{Z}[X]$ to $\mathbb{Z}/p\mathbb{Z}[X]$. So, what do we have is φ_p of f is φ_p of g h because g h see f , g and h are all here, right and f is equal to g h . So, φ_p is a ring homomorphism, right. So, $\varphi_p f$ is $\varphi_p g$ h which is equal to $\varphi_p g$ times $\varphi_p h$. Now, what is $\varphi_p f$? f remember, I have written f as $a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ that means, because φ_p is a ring homomorphism, this means this is φ_p by definition of φ_p rather this is $a_n \bar{a}_n X^n + a_{n-1} \bar{a}_{n-1} X^{n-1} + \dots + a_1 \bar{a}_1 X + a_0 \bar{a}_0$, right.

This is what φ_p does. φ_p takes a polynomial and simply changes the coefficients, it does not change X , this is equal to this. But remember, this is 0, this is 0, this is 0. So, this is nothing, but $a_n \bar{a}_n X^n$. Why is this? Because, remember, p divides a_{n-1} , p divides a_{n-2} and so on all the way up to p divides a_1 p divides a_0 . This is the hypothesis. So, we have this and also p does not divide a_n that means, $a_n \bar{a}_n$ is not 0, so $a_n \bar{a}_n X^n$ is a non-zero polynomial.

(Refer Slide Time: 19:41)

p divides a_{n-1}
 p divides a_{n-2}
 p divides a_{n-3}
 p divides a_0

$$\varphi_p(g) \varphi_p(h) = \bar{a}_n X^n$$

Recall that $\mathbb{Z}/p\mathbb{Z}[X]$ is a UFD. In fact, it is a PID.

So $\varphi_p(g)$ and $\varphi_p(h)$ must also be monomials of the form

So, $\varphi_p f$ is actually just $a_n \bar{a}_n X^n$, but $\varphi_p f$ remember, is $\varphi_p g$ times $\varphi_p h$, so $\varphi_p g$ times $\varphi_p h$ is $a_n \bar{a}_n X^n$. Now, we have two polynomials in $\mathbb{Z}/p\mathbb{Z}[X]$ whose product is this. Now, recall that $\mathbb{Z}/p\mathbb{Z}[X]$ is a UFD, right because it is a polynomial ring over a field. In fact, it is a PID which we do not need for now, we only need that it is a UFD because $\mathbb{Z}/p\mathbb{Z}$ is a field; it is a UFD, so any

polynomial ring in over a UFD is UFD. So, it is a UFD and you have a factorization of a monomial like this. So, this is remember, a single monomial, so $\phi_p g$ and $\phi_p h$ must be must also be monomials of the form. So, what can it be?

(Refer Slide Time: 20:55)

In fact, if u a PID.

So $\phi_p(g)$ and $\phi_p(h)$ must also be monomials of the form:
 $(\bar{b}_i x^i) (\bar{c}_j x^j) = \bar{a}_n x^n, i+j=n, \bar{b}_i, \bar{c}_j \in \mathbb{Z}/p\mathbb{Z}[X].$

Irreducible factors of $\bar{a}_n x^n$: there is only one irr factor, namely X

$x^n = \underbrace{X \cdot X \cdot \dots \cdot X}_{n \text{ times}}$

So, you have some polynomial times another polynomial is; so, you have product of $\phi_p g$ times product of $\phi_p h$ is $\bar{a}_n x^n$, \bar{a}_n is some constant, right, \bar{a}_n is some constant in the underlying ring here which is $\mathbb{Z} \text{ mod } p \mathbb{Z}$. So, how can what can they be? They can be something a coefficient, something like $\bar{b}_i x^i$, $\bar{c}_j x^j$, where $i+j$ is equal to n and \bar{b}_i and \bar{c}_j are in $\mathbb{Z} \text{ mod } p \mathbb{Z}$, right.

This must be the only possible factorization. This is the only possible factorization of a monomial of the form a constant times X^n because if there is any other factorization that means, if for example, $\phi_p g$ has two terms then in the product also you will have two terms. So, there will be two terms of different degrees. Whereas, this is the one, there is only one monomial here. In other words, what are the irreducible factors of another way of saying this is irreducible factors of $\bar{a}_n x^n$ are there is only one irreducible factor namely X , right.

X^n has only one irreducible factor. You can write it as X times X times X n times. There is no other irreducible factor for $\bar{a}_n x^n$ there is only one that means, any divisor of $\bar{a}_n x^n$ must be a power of X . So, coefficients we do not care, but there will be some coefficients. So, it is $\bar{b}_i x^i$ $\bar{c}_j x^j$.

(Refer Slide Time: 23:06)

$X^n = \underbrace{X \cdot X \cdot \dots \cdot X}_{n \text{ times}}$

$f = gh \quad g, h \in \mathbb{Z}[X]$

$\phi_p(g) = \overline{b_i} X^i, \quad \phi_p(h) = \overline{c_j} X^j$

Hence the constant term of g is divisible by p
 the constant term of h is divisible by p .

constant term of $f = \underbrace{(\text{constant term of } g)}_{\text{divisible by } p} \underbrace{(\text{constant term of } h)}_{\text{divisible by } p}$

So, now what does this mean? So, $\phi_p(g)$ is $\overline{b_i} X^i$ or in my notation $\overline{b_i} X^i$, $\phi_p(h)$ is $\overline{c_j} X^j$. So, you should also write $\overline{c_j}$. So, now, think of what g is remember, f is gh . So, g is some polynomial in $\mathbb{Z}[X]$, h is some polynomial in $\mathbb{Z}[X]$. When you go modulo p only X^i survives, hence we can conclude that the constant term of g is 0. Similarly, the constant term of h is 0.

Why is this? Because; sorry this is not 0, I cannot say constant term of g $\phi_p(g)$ is 0 constant term of $\phi_p(h)$ is 0. So, what we can say is a constant term of g is divisible by p that is what I should say. Similarly, constant term of h is divisible by p . So, you have two polynomials you have a polynomial g when you go modulo p the constant term disappears, right because $\phi_p(g)$ is equal to $\overline{b_i} X^i$ and also I should say i is positive j is positive because this is a factorization that comes from the rational polynomials. So, you have two polynomials with positive degree.

So, when you go modulo p the constant term goes away because the only X^i term survives. So, the constant term of g goes away that means, it becomes 0 in $\mathbb{Z} \bmod p$ \mathbb{Z} that means, it is divisible p , it is divisible by p in \mathbb{Z} . Similarly, in the constant term of h becomes a 0 and $\mathbb{Z} \bmod p$ \mathbb{Z} that means, it is divisible by p in \mathbb{Z} .

Now, if that constant term of g is divisible by p and the constant term of h is also divisible by p , we note that constant term of f , remember, is just the constant term of f , constant term of g times constant term of h , right. When you multiply two polynomials g and

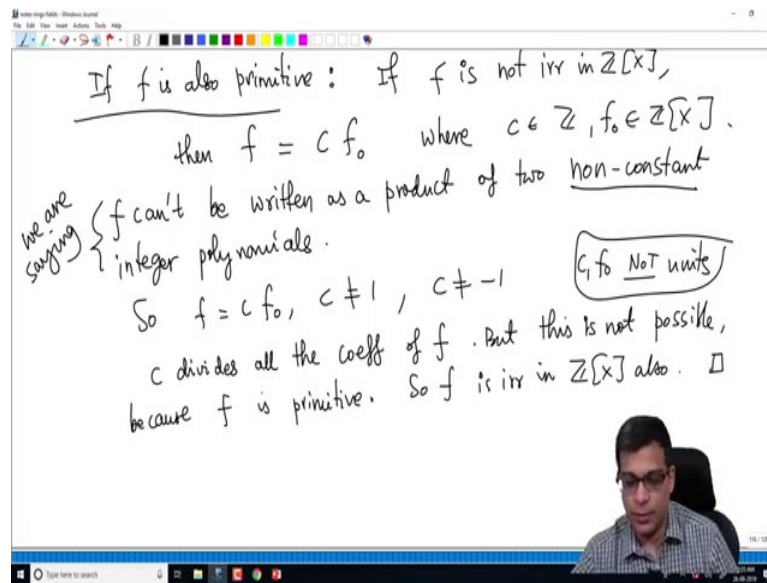
h in the product the constant term is just the constant term of g times constant term of h. Constant terms just multiply to give the constant term of the product. So, constant term of f is constant term of g times constant term of h. So, this is divisible by p, this is divisible by p.

(Refer Slide Time: 25:57)

$f = gh$ $g, h \in \mathbb{Z}[X]$ Hence the constant term of g is divisible by p
 the constant term of h is divisible by p .
 constant term of $f = \underbrace{(\text{constant term of } g)}_{\text{divisible by } p} \underbrace{(\text{constant term of } h)}_{\text{divisible by } p}$
 divisible by p^2
 But this contradicts the hypothesis: p does not divide a_0
 Hence f is irreducible in $\mathbb{Q}[X]$.

Hence, constant term of f is divisible by p squared, right because this is p time some thing, this is p time some thing. So, the whole thing is p squared times something. So, this is divisible by p squared, but this violates or contradicts the hypothesis that p does not divide a 0, right. So, remember, I not only assume that p divides a n minus 1 and up to p divides a 0, I did I also assume that p does not divide a 0. So, now, that gets the contradiction. So, this proves that hence f is irreducible in Q X, ok. So, now this proves the first statement of the Eisenstein criterion.

(Refer Slide Time: 27:00)



If f is irreducible in $\mathbb{Q}[X]$ and also primitive, if f is also primitive content of f is; so, we want to now show that f cannot be irreducible in $\mathbb{Z}[X]$. So, assume that f is also primitive. If f is not irreducible in $\mathbb{Z}[X]$ that means, f is reducible in $\mathbb{Z}[X]$, then f has to be then $f = cf_0$, f can be written as some c times f_0 , where c is in \mathbb{Z} and f_0 is irreducible or f_0 is another polynomial in $\mathbb{Z}[X]$, right.

In other words, what I am saying is that f cannot be written as, f cannot be written as a product of two non-constant integer polynomials. What we are saying is that, I am writing f as c times f_0 , where c is in \mathbb{Z} in $\mathbb{Z}[X]$ because f cannot be written as a product of two nonzero, sorry two non-constant integer polynomials. Why is that? If f can be written as a product of two non-constant integer polynomials, it can also be written as a product of two non-constant rational polynomials because any integer polynomial is a rational polynomial.

So, and we assumed or rather we already proved that f is irreducible in $\mathbb{Q}[X]$, right. So, f cannot be written as a product of two positive degree rational polynomials. And if it, hence, if it is not irreducible in $\mathbb{Z}[X]$, there is only one possible factorization of f into a product a product is of an integer and a integer polynomial, but of course, c is also your not a unit. So, so we have f is cf_0 , c is not equal to 1 or c is not equal to minus 1 because it is an irreducible factorization, right. So, it can be written as a product of two non-units.

So, c and f_0 are not units that is the meaning of not being irreducible. It can be written as two product of two non-units. So, f is $c f_0$, c is neither one nor minus 1 that means, c divides all the coefficients of f , right obviously, because f is c times f_0 c divides all the coefficients of f , but this is not possible. Why? Because f is primitive. Remember, we are given that f is primitive that means, the gcd of the coefficients of f is 1. So, there cannot be any non-unit in \mathbb{Z} that divides all the coefficients of f . So, f must be irreducible in $\mathbb{Z}[X]$ also. So, this completes the proof.

So, we first proved that f is irreducible in $\mathbb{Q}[X]$, then we immediately conclude that the only way that it is not irreducible in $\mathbb{Z}[X]$ is that it is an integer times a polynomial because it cannot be written as a product of two non-constant polynomials that is clear. Because, if it can be written as a product of two non-constant integer polynomials then it can be written as a product of two non-constant rational polynomials violating the irreducibility in $\mathbb{Q}[X]$. So, the only possible factorization is an integer times another integer polynomial, but then that integer must divide all the coefficients of f , but f is primitive, so that integer is 1 or minus 1. So, that proves the fact that if f is a primitive polynomial then f is also irreducible in $\mathbb{Z}[X]$, ok.

(Refer Slide Time: 31:36)

The whiteboard contains the following handwritten text:

Example:
 3 doesn't divide 1
 3 divides 27
 3 divides 213
 9 doesn't divide 213

(i) $X^{10} + 27X^6 + 213$ is irr in $\mathbb{Q}[X]$
 is also irr in $\mathbb{Z}[X]$.
 $p=3$ satisfies the required conditions.

(ii) $X^5 + 3X^2 + 2$ There is no prime that works!

So, now let me quickly give you some examples of Eisenstein criterion to illustrate how useful it is. So, I hope the proof is clear, if not you should just the it is fairly similar to the previous videos. So, you can just go back and see the video again, and hopefully it

will become clear to you. So, now, some examples; so, we already looked at some before. Just for example, I can take X power 10, let us say $27X^6 + 213$. Is this irreducible in $\mathbb{Z}[X]$ or $\mathbb{Q}[X]$?

It is because it is irreducible in $\mathbb{Q}[X]$ first and how because it is primitive it is also irreducible in $\mathbb{Z}[X]$, right. It is certainly primitive because the coefficient one of the coefficients is 1, so the gcd is 1. Because p equal to 3 satisfies the required conditions, right because 3 divides 27, 3 divides 213. And we also want 3 does not divide that is clear here 1, the leading coefficient is 1 and 9 does not divide 213, right. So, 9 does not divide 213 you can quickly check that means, p equal to 3 satisfies this.

So, every time you are asked to check or you want to know if a polynomial is irreducible or not. First, see if there is a prime that works sometimes it does not, sometimes Eisenstein criterion does not give you the answer; in general there is no algorithm which always works to verify a polynomial is irreducible or not. So, we are just trying to learn new techniques to do it and Eisenstein criterion is an extremely useful technique.

Sometimes, it might appear like initially you do not have you initially you might think that you cannot apply Eisenstein criterion, but some small modification works to give you the answer. For example, here you take $X^5 + 3X^2 + 2$ this is a polynomial and you want to know it is irreducible or not because it is primitive if it is irreducible in $\mathbb{Q}[X]$ its irreducible in $\mathbb{Z}[X]$.

So, now, certainly on the face of it no prime works, right, because only prime that divides constant is 2, only prime that divides the coefficient of X^2 is 3. So, there is no prime, right because 3 does not divide 2, 2 does not divide 3. So, you cannot work.

(Refer Slide Time: 34:34)

$f(x) = x^3 + 3x^2 + 2$ There is no prime p such that $f(x)$ is irr.
 $f(x+1) = (x+1)^3 + 3(x+1)^2 + 2 = x^3 + 6x^2 + 9x + 6$ ✓
 Now $p=3$ works: So $f(x+1)$ is irr. reducible in $\mathbb{Q}[x]$ or in $\mathbb{Z}[x]$
 $f(x)$ is also irr in $\mathbb{Q}[x]$: if not: $f(x) = g(x)h(x)$:
 $\deg g(x) > 0 \Rightarrow \deg g(x+1) > 0 \Rightarrow f(x+1) = g(x+1)h(x+1)$
 This violates irreducibility of $f(x+1)$.

 $f(x)$ is also irr in $\mathbb{Z}[x]$

However, let us take this as f of X , a small trick will do the job for you if you take f of $X+1$. So, actually let me take this as X^3 . If you take f of $X+1$, so f of $X+1$ is $(X+1)^3 + 3(X+1)^2 + 2$. If you take f of $X+1$ what is this is $X^3 + 6X^2 + 9X + 6$. I am replacing X by $X+1$ here. So, $(X+1)^3 + 3(X+1)^2 + 2$.

So, now, if you expand this and combine; so, I will quickly do this and you can check the it is correct you will have X^3 term plus $6X^2$ and there will be another $3X^2$ squared that will be $6X^2$ plus there will be a $3X$ here and $6X$ here. So, that will be $9X$ there will be a one there will be a 3 there will be a 2 . So, that will be 6 . Now, p equal to 3 works, right so that means, 3 does not divide the leading coefficient 3 divides 6 , 3 divides 9 , 3 divides 6 , 9 does not divide 6 . So, we can conclude f of $X+1$ is irreducible, right.

So, f of $X+1$ is irreducible. What can you say; because this is a polynomial to which Eisenstein criterion applies and that we can say its irreducible and I should actually say in $\mathbb{Q}[X]$ also in $\mathbb{Z}[X]$ because it is a primitive polynomial. So, it is also irreducible in $\mathbb{Z}[X]$. But original question is for f of X . And what can you say about f of X ? I claim that f of X is also irreducible in $\mathbb{Z}[X]$. Why? If not, we can write f of X as some g of X times h of X , this is a polynomial identity.

So, let me just first do \mathbb{Q} for simplicity, it is a polynomial identity, where g and h are positive degree polynomials. And every time you have a polynomial identity we can for-

mally replace the variable by any other expression. So, $f(X+1)$ can have to be $g(X+1)$ times $h(X+1)$ because both sides you are replacing by X . But this if $g(X)$ is positive degree the simplest degree of $g(X+1)$ is also positive degree is also positive, because again if $g(X)$ is X power, $3X$ power 2, X $g(X+1)$ is will be also there will be X^2 squared term there because $(X+1)^2$ will appear and then that will give you X^2 squared.

So, the degree of $g(X+1)$ is same as degree of $g(X)$, degree of $h(X+1)$ is degree of $h(X)$ and here you have written $f(X+1)$ as a product of two positive degree polynomials. This violates irreducibility of X, X $f(X+1)$. So, $f(X+1)$ is irreducible by Eisenstein criterion. If $f(X)$ is reducible $f(X+1)$ is also reducible violating the hypo the conclusion earlier. So, $f(X)$ is also irreducible. Once the $f(X)$ is irreducible in $\mathbb{Q}[X]$, $f(X)$ is $f(X)$ is primitive. So, $f(X)$ is also irreducible in $\mathbb{Z}[X]$, ok because, if its primitive and its irreducible in $\mathbb{Q}[X]$ we proved already that it is irreducible in $\mathbb{Z}[X]$.

(Refer Slide Time: 38:25)

$f(x)$ is also irr in $\mathbb{Z}[X]$
 (iii) Let p be a prime integer; $f(x) = X^{p-1} + X^{p-2} + \dots + X^2 + X + 1$.
 No prime divides $(X-1)f(x) = (X-1)(X^{p-1} + X^{p-2} + \dots + X^2 + X + 1)$
 $(X-1)f(x) = X^p - 1$
 Set $y := X-1$
 So $y+1 = X$
 $y f(y+1) = (y+1)^p - 1$
 $= y^p + py^{p-1} + \binom{p}{2} y^{p-2} + \dots$

So, the final example I will give for Eisenstein criterion which is actually a very useful example and it will come when we study fields and field extensions called cyclotomic field extensions and this is the following. So, let p be any prime integer, let p be a prime integer, let $f(X)$ be the polynomial given by $X^p - 1$ times $X + X^{p-2} + X^{p-3} + \dots + X^2 + X + 1$. So, again, I my question is: is it irreducible over $\mathbb{Q}[X]$, if so it will be irreducible over $\mathbb{Z}[X]$, but we cannot use

no prime works, right. Again, no prime works in the Eisenstein criterion because all the coefficients here are 1. So, certainly no prime divides the coefficients.

But again, the trick is to use what I have done in the previous example. But what I will do now is if I multiply $f(x)$ by $x - 1$, what do I get? So, I get $x - 1$ plus times $x^p - 1$ plus x^{p-2} plus x^2 plus $x + 1$. And now if you multiply this out what you get is simply $x^p - 1$ because all the other terms will cancel out, right. There will be an x^{p-1} , plus x^{p-1} , minus x^{p-1} and you will cancel all the terms except this.

So, what you will have is $x - 1$ times $f(x)$ is this. But then I said y is equal to $x - 1$. So, I am changing variables here. Now, what do I get? I get y this equation. So, $x - 1$ times $f(x)$ equals $x^p - 1$. So, in this I am replacing $x - 1$ by y that means, y times if y is $x - 1$ $y + 1$ is x . So, $f(x)$ is $f(y + 1)$. So, y times $f(y + 1)$ is $x^p - 1$ or rather $(y + 1)^p - 1$ because x is $y + 1$. So, y times $f(y + 1)$ is equal to $(y + 1)^p - 1$. But what is this? This is $y^p + p y^{p-1} + \binom{p}{2} y^{p-2} + \dots + p y + 1 - 1$.

(Refer Slide Time: 40:57)

No prime works

$$(x-1)f(x) = (x-1)(x^p + x^{p-2} + x^2 + x + 1)$$

$$(x-1)f(x) = x^p - 1$$

Set $y := x - 1$
So $y + 1 = x$

$$y f(y+1) = (y+1)^p - 1$$

$$y f(y+1) = y^p + p y^{p-1} + \binom{p}{2} y^{p-2} + \dots + p y + 1 - 1$$

$$y f(y+1) = y^p + p y^{p-1} + \binom{p}{2} y^{p-2} + \dots + p y$$

So, this until this is just $y^p + p y^{p-1} + \dots + p y + 1$. If you expand $(y + 1)^p$ by using binomial theorem this is what you get $y^p + p y^{p-1} + \binom{p}{2} y^{p-2} + \dots + p y + 1$.

minus 2 and so on plus 1 at the end. So, you cancel that 1 with this minus 1, what you end up with is y^p , $p y^{p-1}$, $\binom{p}{2} y^{p-2}$, ..., $p y$, ok.

(Refer Slide Time: 41:49)

$$y f(y+1) = y^p + p y^{p-1} + \binom{p}{2} y^{p-2} + \dots + p y$$

{ Note: p divides $\binom{p}{i}$ for all $i=1, \dots, p-1$. $i < p$
 exercise Reason: $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\dots(p-i+1)}{i!}$

~~$y f(y+1)$ is irr in $\mathbb{Q}[X]$ and $\mathbb{Z}[X]$, by Eisenstein criterion.~~

$$y f(y+1) = y^p + p y^{p-1} + \binom{p}{2} y^{p-2} + \dots + p y$$

Now, this looks more promising, right. You can conclude that this is irreducible using, so let us call I mean this is f of f times y times $f y$ plus 1 by Eisenstein criterion; what we need to claim is. And this, I will leave as an exercise for you this is a very easy exercise p divides p choose i for all, i from 1 up to p minus 1, ok. So, of course, when you take i equal to 1, p choose i is just p so p divides that, p also divides p choose 2, p choose 3 and so on. Here the important fact is that p is a prime. So, the reason is you can write p choose i as.

So, this is by definition p factorial, by i factorial times p minus i factorial, right. So, suppose you cancel i factorial or p minus i factorial you have p times p minus 1 up to p minus i plus 1 by i factorial, right. So, I have cancelled p minus i factorial from numerator and denominator. So, in the now if you look at this i is strictly less than p . So, p is not going to appear in the denominator, right, i factorial is 1 times 2 times 3 times up to i . So, p does not appear in the denominator whereas, p appears in the numerator so that means, p divides this. So, this is a quick hint, but I will let you finish the argument and show that p divides p choose i for all i .

So, y times $f y$ plus 1 is irreducible in $\mathbb{Q}[X]$ and $\mathbb{Z}[X]$ by Eisenstein criterion, right. This is because p divides all the coefficients other than the leading coefficient p divides this, p

divides p choose 2, p divides p choose 3, p divides p and p squared does not divide the last coefficient, ok. So, actually sorry, I should this is not quite correct. So, I should continue one more step. So, what we have is y times $f(y+1)$ is equal to y^p , p y^{p-1} , p choose 2, y^{p-2} plus p y .

(Refer Slide Time: 44:14)

~~Criterion:~~
 $y f(y+1) = y^p + p y^{p-1} + \binom{p}{2} y^{p-2} + \dots + p y$
 Divide by y : $f(y+1) = y^{p-1} + p y^{p-2} + \binom{p}{2} y^{p-3} + \dots + \binom{p}{2} y + p$
 Apply Eisenstein criterion: $f(y+1)$ is irr. in $\mathbb{Z}[x]$
 $\Rightarrow f(x)$ is irr. in $\mathbb{Z}[x]$

Now, I divide by y both sides so I cancel y . Divide by y . What, what I get is $f(y+1)$ is y^{p-1} , p y^{p-2} , p choose 2 y^{p-3} , p choose 2 y plus p . If I divide by the previous term is p choose 2 y squared, so that becomes p choose 2 y plus p . Now, apply Eisenstein criterion. See, earlier we cannot apply Eisenstein criterion because the leading coefficient the constant term is 0. Now, we can to conclude that $f(y+1)$ is irreducible. But, what is $f(y+1)$? $y+1$ is just X , right. So, remember, that was our change of variable $y+1$ is X . So, $f(y+1)$ is irreducible, so $f(X)$ is irreducible.

Remember, $f(y+1)$ is irreducible, again in $\mathbb{Z}[X]$ I can say, in $\mathbb{Q}[X]$ or $\mathbb{Z}[X]$ its irrelevant here. So, this is because p divides all the coefficients here other than the first coefficient which is 1 and p squared does not divide the constant coefficient. So, this Eisenstein criterion applies to this to conclude this is irreducible in $\mathbb{Q}[X]$, but this is also primitive, so this is irreducible in $\mathbb{Z}[X]$. So, $f(y+1)$ is irreducible in $\mathbb{Z}[X]$. So, $f(X)$ is irreducible in $\mathbb{Z}[X]$ because $y+1$ is equal to X , X . So, in this video we looked at Eisenstein criterion

which is an extremely useful technique to prove irreducibility in $\mathbb{Q}[X]$ or $\mathbb{Z}[X]$ and we also looked at some examples.

So, this completes whatever I wanted to say in this course in ring theory. So, in the next 1 or 2 videos I will do some problems on rings just to summarize whatever we have done and then we will go to fields.

Thank you.