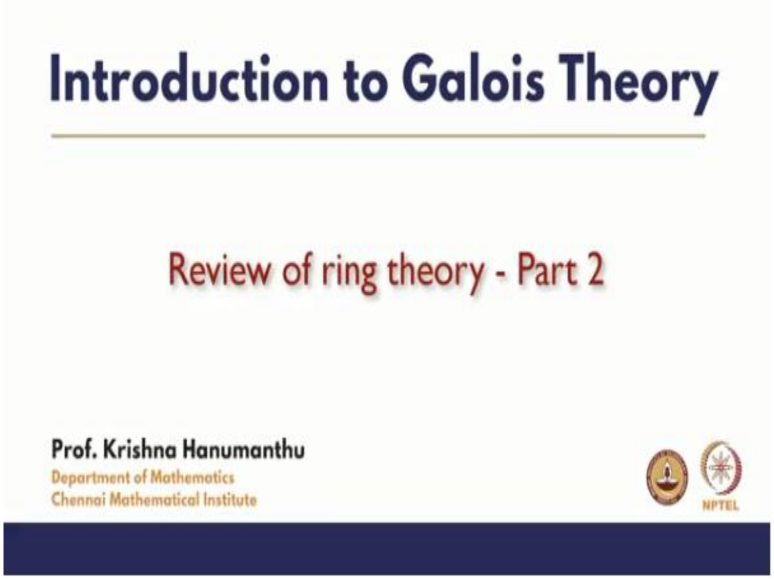
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Module: 01
Lecture 04: Review of ring theory – Part II

(Refer Slide Time: 0:11)



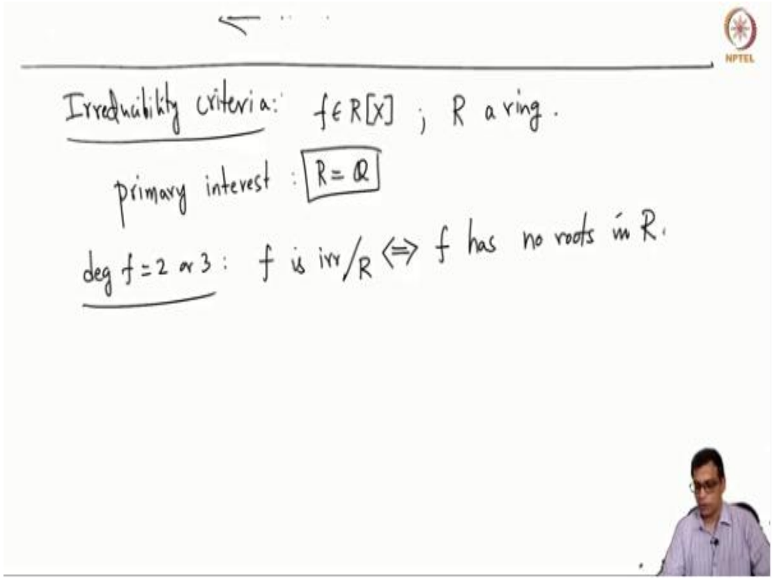
Introduction to Galois Theory

Review of ring theory - Part 2

Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Welcome back, in the last video we recall some important notions in ring theory and recalled certain important classes of rings called UFDs, PIDs, I talked about polynomial rings, when a polynomial is irreducible or not, what is the meaning of polynomial being irreducible or not.

(Refer Slide Time: 0:33)



Irreducibility criteria: $f \in R[X]$; R a ring.

primary interest : $\boxed{R = \mathbb{Q}}$

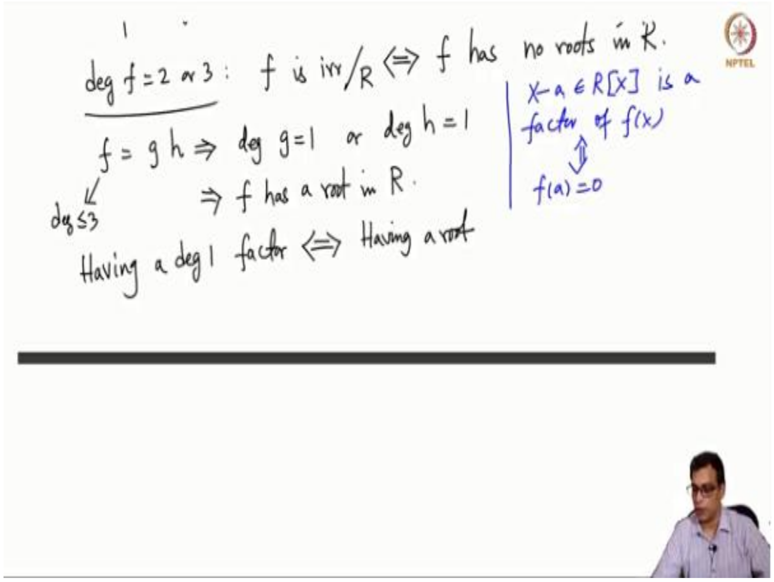
deg $f = 2$ or 3 : f is irr$/_R \iff f$ has no roots in R.

So today in this video I want to recall a few important notions of techniques to determine if a given polynomial is irreducible or not. So, so let us recall in this video, some nice methods to check for irreducibility so, the goal is to understand if a given polynomial is reducible or not.

So, let us say F is a polynomial and over a ring R, our primary interest will be in when R is Q so, as you will see later in the course, often we will be interested in figuring out whether a rational polynomial is irreducible over Q or not. And I want to emphasize again that irreducibility is dependent on the ring that you are studying, X square plus 1 is irreducible over rational numbers or real numbers, but not irreducible over complex numbers. So, always we will say irreducible over a given ring.

So, a few quick things if degree is small for example, degree is 2 or 3, one very nice way of checking for irreducibility is to check if the polynomial has a root or not. So, here f is irreducible over R whatever your base ring is, if and only if f has no roots R.

(Refer Slide Time: 2: 13)



deg f = 2 or 3 : f is irr/$_R$ $\Longleftrightarrow$ f has no roots in R.

$f = g\,h \Rightarrow \deg g = 1$ or $\deg h = 1$

deg ≤ 3

$\Rightarrow$ f has a root in R.

Having a deg 1 factor $\Longleftrightarrow$ Having a root

$X - a \in R[X]$ is a factor of $f(x)$

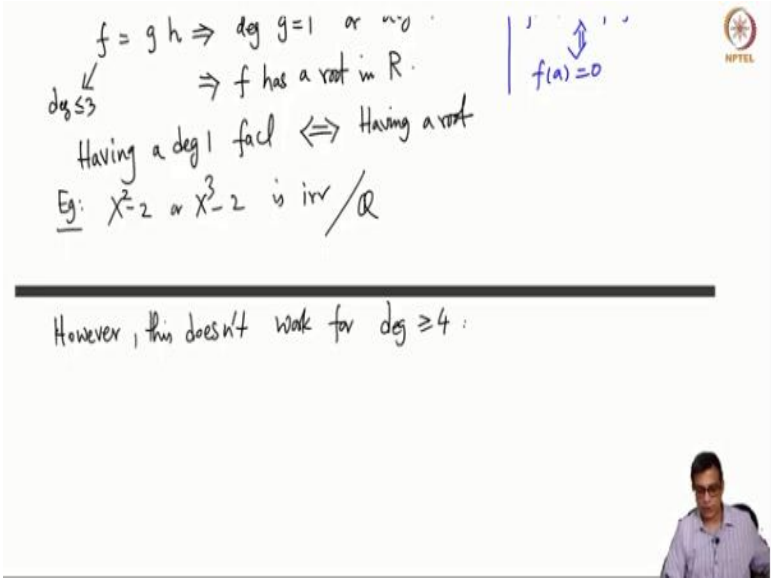
$\Updownarrow$

$f(a) = 0$

And this is simply because if f is a degree 2 or 3 polynomial, and you are able to write it as a product of two smaller degree polynomials, so, this has degree less than or equal to 3 implies and g and h have smaller degree than f implies, degree g is 0, sorry degree g is 1, or degree h is 1 and if degree of f is 2, both have degree 1. So, in this case, f has a root in R.

So, the point I want to basically highlight here is having a degree 1 factor is equivalent to having a root. So, the point here is, if for example, X minus A in RX is a factor of small fx, this is if and only if fa is 0. So, f has a root in R, small a is remember an element of R.

(Refer Slide Time: 3:23)



$f = gh \Rightarrow \deg g = 1$ or ...

$\deg \leq 3$

$\Rightarrow f$ has a root in R.

$\Updownarrow$

$f(a) = 0$

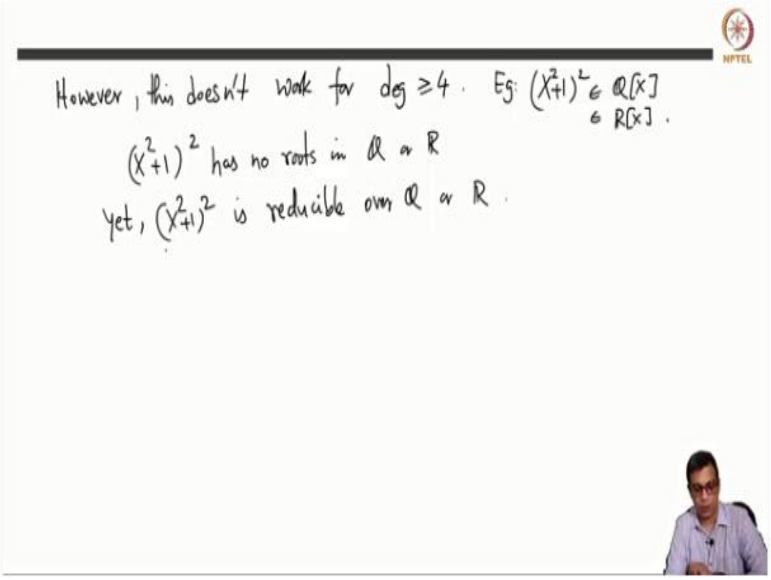
Having a deg 1 fact $\Longleftrightarrow$ Having a root

Eg: X^2-2 or X^3-2 is irr $/Q$

However, this doesn't work for deg ≥ 4 :

So, for degree 2 or 3, this is very convenient to check, for example, X cube minus 2 or X cube minus 2, X square minus 2 or X cube minus 2 is irreducible or both irreducible over Q. So there is no square root of 2 or cube root of 2 in Q, so they are irreducible. However, this method does not work for higher degree polynomials.

(Refer Slide Time: 3:56)



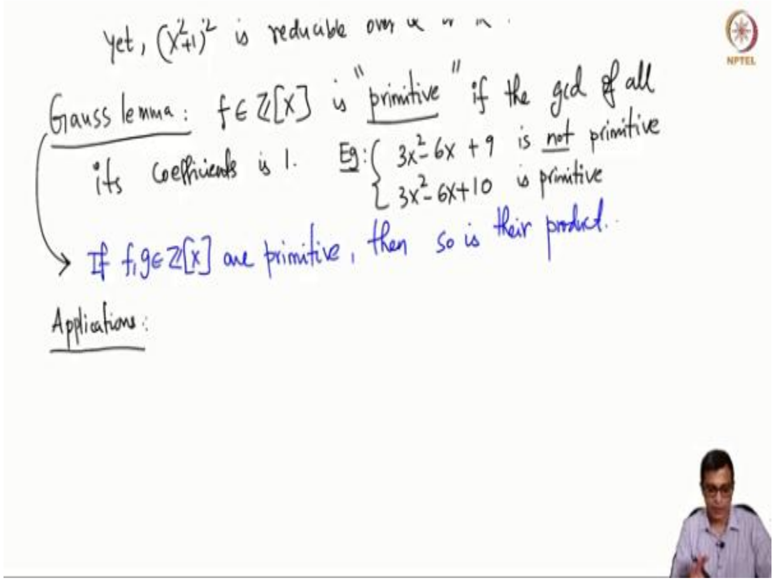
However, this doesn't work for deg ≥ 4. Eg: $(X^2+1)^2 \in Q[X]$ $\in R[X]$.

$(X^2+1)^2$ has no roots in Q or R

Yet, $(X^2+1)^2$ is reducible over Q or R.

This is very simple to see an example here is, for example, X square plus 1 whole square, if you take this over Q or R, so X square plus 1, square has no roots in Q or R, because any root of X square plus 1 whole square is in fact a root of X square plus 1 also, but we know very well that there are no rational roots or real roots of the polynomials X square plus 1, but yet, X square plus 1 whole square is reducible over Q or R, because of course, the way it is defined already shows that it is reducible, it has a factorization, this has degree 4, the whole polynomial and it is written as a product of 2 degree 2 polynomials.

(Refer Slide Time: 4:55)



yet, $(X^2+1)^2$ is reducible over $\mathbb{Q}$ or $\mathbb{R}$.

Gauss lemma: $f \in \mathbb{Z}[X]$ is "primitive" if the gcd of all its coefficients is 1. Eg: $\begin{cases} 3x^2-6x+9 \text{ is not primitive} \\ 3x^2-6x+10 \text{ is primitive} \end{cases}$

→ If $f, g \in \mathbb{Z}[X]$ are primitive, then so is their product.

Applications:

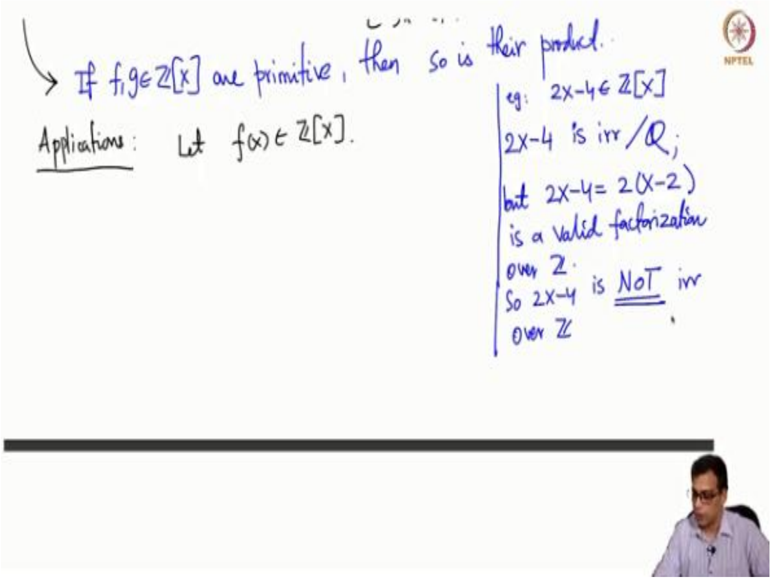
So, degree 4 or higher, you have to do more refined analysis to figure out irreducibility and in this process, a very important lemma result is called Gauss lemma. And this is in fact, one of the most important top results you learn in ring theory. It is, in fact very easy to prove this, but it is of, it has very, very important applications.

So, to state lemma, let me define what is a primitive polynomial, what is, when we say an integer polynomial is primitive. So let us say an integer polynomial f is given to you, it is called primitive if the gcd, the greatest common divisor of all its coefficients is 1 so, very simple concept. So example, 3x square minus 6x plus 9 is not primitive, because 3 divides all the coefficients, the coefficients here are 3, minus 6, and 9 and 3 divides all of them.

Whereas 3x square minus 6x plus 10 is primitive, there is no common factor other than 1 for all the coefficients. So this is the notion and the Gauss lemma now says if f and g are two integer polynomials or primitive, then so is their product. The proof is fairly simple, it involves just going modulo certain primes, but it is simple yet very important statement. It has important applications.

So, if you take two primitive polynomials, the product is also primitive. So, as I said the interest, I mean, on the face of it, the statement does not seem to have anything to do with irreducibility, but it does have important applications to the irreducibility question.

(Refer Slide Time: 6:58)



→ If $f, g \in \mathbb{Z}[x]$ are primitive, then so is their product.

Applications: Let $f(x) \in \mathbb{Z}[x]$.

eg: $2x-4 \in \mathbb{Z}[x]$

$2x-4$ is irr $/\mathbb{Q}$;

but $2x-4 = 2(x-2)$

is a valid factorization

over $\mathbb{Z}$.

So $2x-4$ is NOT irr

over $\mathbb{Z}$

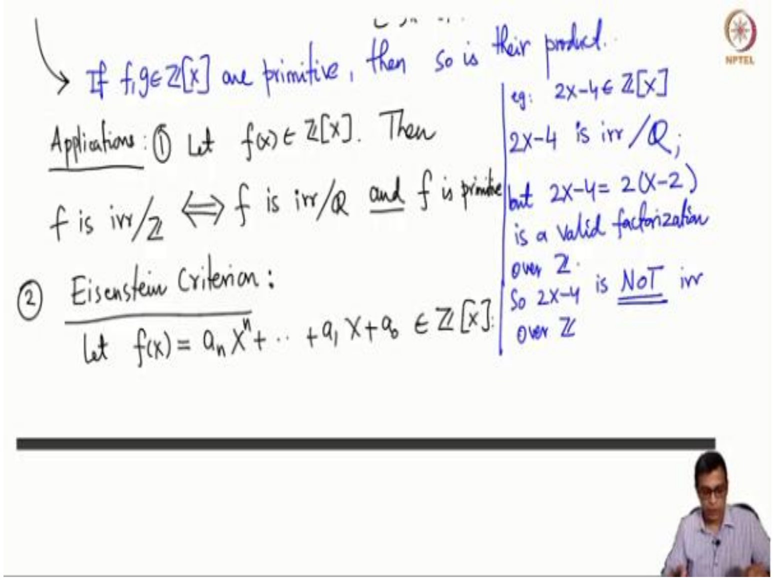
So, I want to highlight this in this form we may not directly use this, but let me state it as it is. Let f be an integer polynomials, so I want to highlight this following phenomenon. So in Galois theory, we will often encounter the situation we have an integer polynomial. So hence, it is a rational polynomial, we would like to establish whether it is irreducible over Q or not, but often it will be easier to establish whether it is irreducible over Z or not. And using that, we want to conclude irreducible to Q and of, I mean, these are independent phenomenon.

As an example we see this example. So take this example of 2x minus 4. So I claim that 2x minus 4 is irreducible over Q. So, any degree 1 polynomial over a field is irreducible, because you cannot factor this as a product of two smaller degree polynomials because any smaller degree polynomial, any degree 0 polynomials field is a unit, so you cannot that is not a valid factorization.

Whereas, you can have a factorization over Z is a valid factorization over Z. Note that 2 is a unit in Q, it is not a unit in Z. So, this is a valid factorization in Zx. So, 2x minus 4 is not irreducible over Z, it is irreducible over Q but not in Z. So, if something is irreducible over Z you may not be able to conclude that it is irreducible over Q right away.

So, here is where Gauss lemma plays a role. The problem here is that the polynomial is primitive. So, the point is a polynomial can be reducible over Z, but irreducible over Q, so you cannot use some information about Z to conclude information about Q, except when the polynomials is primitive, in this polynomial, the problem is that it is not primitive, because 2 is a common factor of all the coefficients. So the main application of Gauss lemma for us is that if you have a.

(Refer Slide Time: 9:30)



→ If $f, g \in \mathbb{Z}[x]$ are primitive, then so is their product.

Applications: ① Let $f(x) \in \mathbb{Z}[x]$. Then

f is irr$/\mathbb{Z}$ $\Longleftrightarrow$ f is irr$/\mathbb{Q}$ and f is primitive

② Eisenstein Criterion:

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$.

eg: $2x-4 \in \mathbb{Z}[x]$

$2x-4$ is irr $/\mathbb{Q}$;

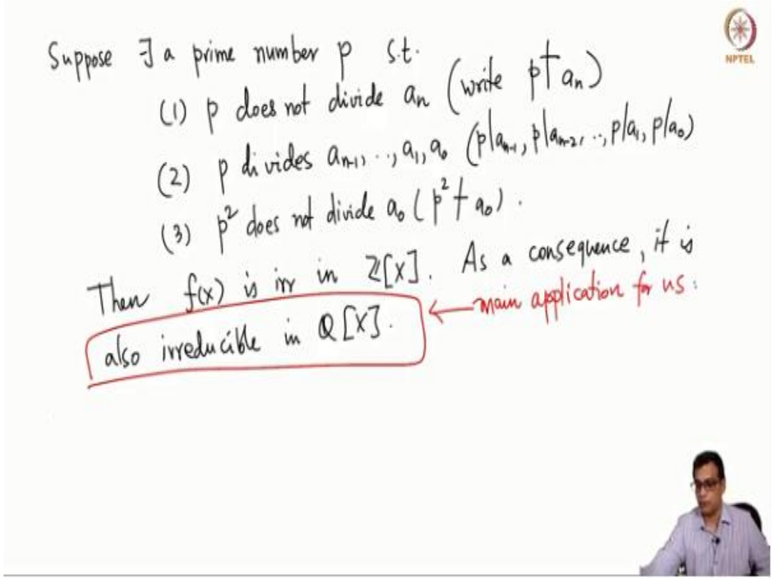
but $2x-4 = 2(x-2)$ is a valid factorization over $\mathbb{Z}$.

So $2x-4$ is NOT irr over $\mathbb{Z}$

So, let me write one, here. If f is a integer polynomials, then f is irreducible over Z if and only if f is irreducible over Q and f is primitive. So if you are working with a primitive polynomial, irreducibility in Z is equal to irreducibility in Q, if not, if f is not primitive it cannot be irreducible over Z so, that is the application of Gauss lemma.

So, using this you have certain very important irreducibility criteria, in fact the most important part is called Eisenstein criterion. Often this is the most important thing that you will see Eisenstein use in practice so, what does it say? Let, pay close attention to the way I am stating this. So, let us take a an integer polynomial.

(Refer Slide Time: 10:49)



Suppose $\exists$ a prime number p s.t.

(1) p does not divide a_n (write $p \nmid a_n$)

(2) p divides $a_{n-1}, \ldots, a_1, a_0$ $(p \mid a_{n-1}, p \mid a_{n-2}, \ldots, p \mid a_1, p \mid a_0)$

(3) p^2 does not divide a_0 $(p^2 \nmid a_0)$.

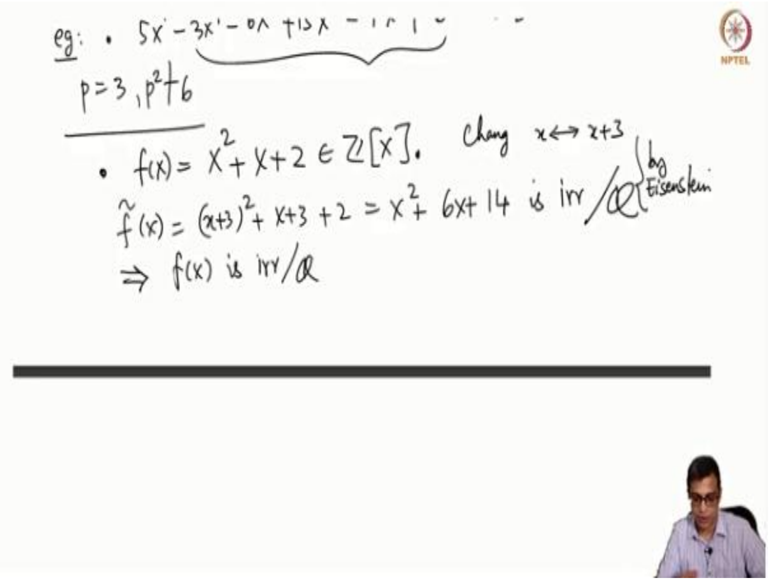
Then $f(x)$ is irr in $\mathbb{Z}[X]$. As a consequence, it is also irreducible in $\mathbb{Q}[X]$. $\leftarrow$ main application for us:

So, let us take an integer polynomial that is important for me. Suppose so, let me write it here, suppose there exists a prime number p such that, three things happen. So, this is of course, a n is not zero, it is a degree n polynomial. Every time I write a polynomials like this of course, I mean, the leading coefficient is not zero.

So, such that p divides, I will say p does not divide a n the leading coefficient and in short, we always write like this, this vertical bar represents divides. So cross means it does not divide. Two, p divides all the other coefficients a n minus 1 up to a1 to a0. So, p divides a n minus 1, p divides a n and minus 2, p divides a1, p divides a0 and finally, p square does not divide a0. So, p square does not divide a0, then the conclusion that you can easily make is that this is irreducible over Zx.

As a consequence, it is also by the earlier result one, which is an application of Gauss lemma it is also irreducible in, so, when I say over should say Z, so, I cannot say over Zx, it is irreducible in Zx and as a consequence it is irreducible in Qx so, the most important application for us is this. This is the main application for us, we do not really care about irreducibility over Z. So, we often will be interested in irreducibility over Q.

(Refer Slide Time: 12:59)



eg: • $5x - \underbrace{3x - 6x + 15x - \cdots}$ [illegible]

$p = 3,\ p^2 \nmid 6$

• $f(x) = x^2 + x + 2 \in \mathbb{Z}[x]$. Chang $x \leftrightarrow x+3$

$\tilde{f}(x) = (x+3)^2 + x+3+2 = x^2 + 6x + 14$ is irr $/\mathbb{Q}$ $\Big\{$ by Eisenstein

$\Rightarrow f(x)$ is irr$/\mathbb{Q}$

So, some easy cases of this a theorem criterion, for example, 5x 10 minus 3x 7 minus 6x square, this is 6x cube plus 15x square minus 9x plus 6 this is an integer polynomial is irreducible over Q. So, this is somewhat of, like a magical formula, because this is degree 10.

So, you cannot use this business with roots even if you know that there are no roots, which of course itself is not easy to establish, but we can immediately conclude that 3 does not take p equal to 3 in the Eisenstein criterion, p does not divide 5, but it divides all the other coefficients, p squared does not divide 6, the constant coefficient. So, this is irreducible, so, this is magical.

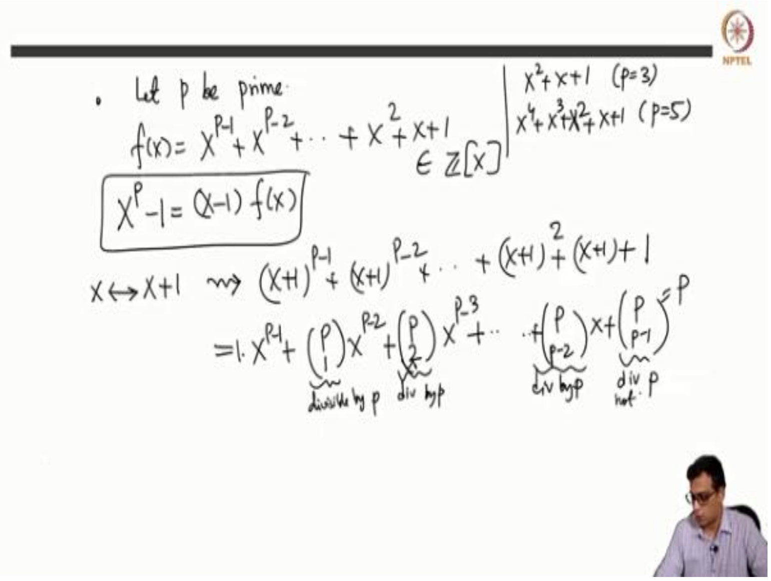
In fact, it becomes even more interesting, when you directly cannot say but sometimes small manipulation can give you interesting statements, for example, if you take this so, this is degree 2 so, one can also check the roots and do but which is not difficult in this case, but I want to illustrate how Eisenstein criterion can be applied even if it does not look like it can be applied. Here, of course, there is no prime, right? Because one of the coefficient is 1 so, you cannot choose any prime, which satisfies the Eisenstein criterion.

Remember, Eisenstein criterion is a very special case, most of the time you cannot apply this, so in which case you cannot conclude anything about irreducibility. If you are lucky that there is a p like this, you can conclude any irreducibility. Sometimes it may look like there is no p but a change of variables can do the trick for us. So, change x to x plus 3 okay, then what happens?

So you get f tilde of x is x plus 3 whole square plus x plus 3 plus 2 and if you work this out, you get x squared plus 6x plus 14 so this is now Eisenstein criterion can be used, because you can take 2 as a prime, 2 divide 6, 2 divides 14 and 2 square, which is 4 does not divide 14. So this is irreducible by Eisenstein.

And now simple homomorphism sub groups will tell you that this implies f itself is irreducible over Q because f were to break up as a factor of, as a product of g and h, by simply changing x to x plus 3, you can break f tilde also as g tilde times h tilde, which you cannot do. So this is irreducible.

(Refer Slide Time: 15:56)



- Let p be prime.

$f(x) = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1 \in \mathbb{Z}[X]$

$X^2 + X + 1 \quad (p=3)$

$X^4 + X^3 + X^2 + X + 1 \quad (p=5)$

$\boxed{X^p - 1 = (X-1) f(x)}$

$X \leftrightarrow X+1 \rightsquigarrow (X+1)^{p-1} + (X+1)^{p-2} + \cdots + (X+1)^2 + (X+1) + 1$

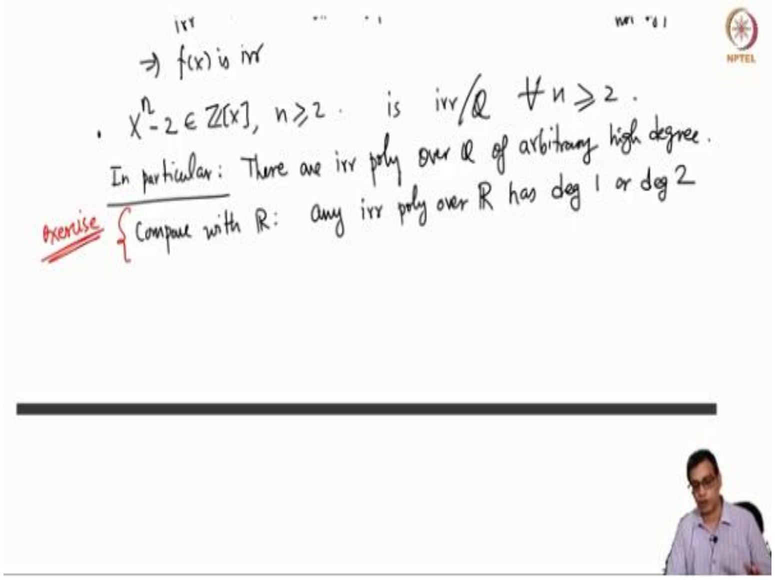
$= 1 \cdot X^{p-1} + \underbrace{\binom{p}{1}}_{\text{divisible by } p} X^{p-2} + \underbrace{\binom{p}{2}}_{\text{div by } p} X^{p-3} + \cdots + \underbrace{\binom{p}{p-2}}_{\text{div by } p} X + \underbrace{\binom{p}{p-1}}_{\substack{\text{div } p \\ \text{not}}} = p$

A more interesting example is something we will encounter later in the course, is this. So let us say p is a prime, a prime number, then let us take fx to be X power p minus 1 plus X power p minus 2 plus x square plus x plus 1, for example, you can take x square plus x plus 1 for p equal to 3, you can get x4 plus x plus 1, p equal to 5 and the reason that this will come up later is this is the factorization of X power p minus 1.

So, fx is that polynomials and now again, to determine the irreducibility of f, you cannot directly apply Eisenstein because there is no prime which divides all the coefficients, in fact all the coefficients are 1, but now you change the variable x to x plus 1, I think okay. So, in that case, what you get is so, in this case, if you, you have to work this out carefully, but if you do this, so, then what you get actually is X power p minus 1 plus p choose 1, X power p minus 2, so, there will be p many terms. So, that is p choose 1, p choose 2 X power p minus 3 plus p choose p minus 2x plus p choose p minus 1 this is a simple calculation.

So, now, this is divisible by p because the leading coefficient is 1 here, p does not divide it whereas, this is divisible by p, this is divisible by p, and this is divisible by p, this is in fact p so, but it is not divisible by p square.

(Refer Slide Time: 18:20)



irr

$\Rightarrow f(x)$ is irr

- $X^n - 2 \in \mathbb{Z}[x]$, $n \geq 2$. is irr$/\mathbb{Q}$ $\forall n \geq 2$.

In particular: There are irr poly over $\mathbb{Q}$ of arbitrary high degree.

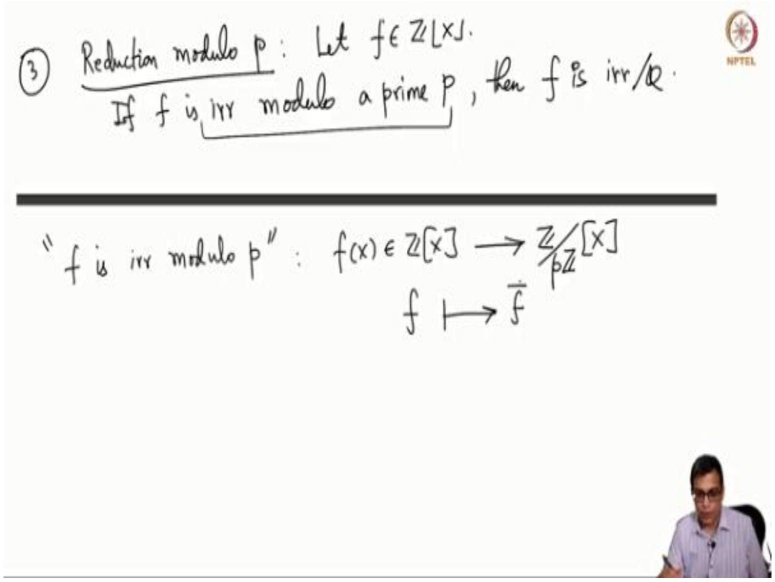
Exercise $\{$ Compare with $\mathbb{R}$: any irr poly over $\mathbb{R}$ has deg 1 or deg 2

So, this is irreducible in fact f itself is irreducible so, Eisenstein criterion is quite powerful tool in determining irreducibility. So, one final example of Eisenstein criterion I will give you, you take X power n minus 2 in Zx and I assume n is at least 2, I claim that this is irreducible for all Q, sorry for all n, this is irreducible over Q for all n at least two, because Eisenstein criterion will apply with p equal to 2 to give you the result.

This in particular says that a simple fact but it is the first time we are proving this, there are irreducible polynomials over Q of arbitrary high degree, because n can be taken to be any integer, there are irreducible polynomials of over Q of arbitrary high degree and note that this is not true, compare with R any irreducible polynomial over Q, sorry over R has degree 1 or degree 2.

So, in R this is a nice exercise in field theory. So, at some point we might do this, but over R there are only two possible degrees for irreducible polynomials, over Q you can have irreducible polynomials of arbitrary degree. So, this is an aside but it is a statement. So as I said Eisenstein criterion is our primary tool to determine irreducibility.

(Refer Slide Time: 20:26)

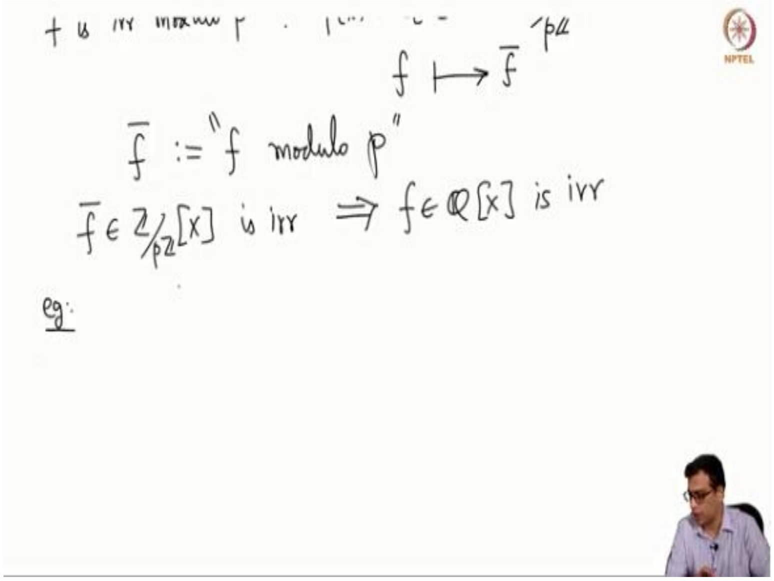


③ Reduction modulo p: Let $f \in \mathbb{Z}[x]$.

If f is irr modulo a prime p, then f is irr/$\mathbb{Q}$.

"f is irr modulo p" : $f(x) \in \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x]$

$$f \longmapsto \bar{f}$$



f is irr modulo p . . . /pℤ

$f \longmapsto \bar{f}$

$\bar{f}$:= "f modulo p"

$\bar{f} \in \mathbb{Z}/p\mathbb{Z}[x]$ is irr $\Rightarrow f \in \mathbb{Q}[x]$ is irr

eg:

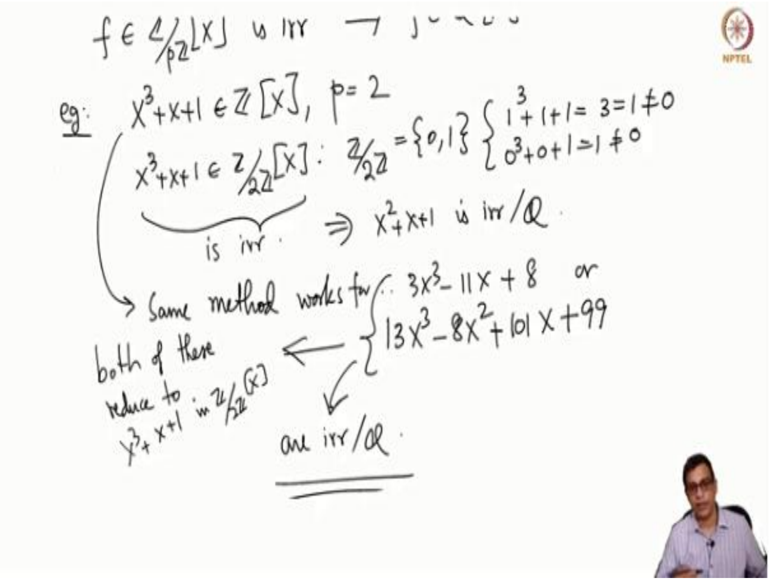
One other, so I do not remembering so Gauss lemma, one application is that, two is the Eisenstein criterion. So I want to give one final thing, which is not always useful, in fact, often it is not applicable, but it is good to keep this in mind, Reduction Modulo p. This is also an application of Gauss lemma really.

So here, the statement is that, let f be an integer polynomial, if f is irreducible modulo a prime p, so I will explain this. Okay, so again, I will skip the intermediate step which is that it is irreducible over Z and as a consequence, it is irreducible over Q, but I will again write only the conclusion which is important to us, it is irreducible over Q, but what is the meaning of this, irreducible over Q mean, modulo p mean?

f is irreducible modulo p means so, fx is in Zx and Zx there is a natural map from Z to Z mod p Z, so, there is a natural map from Z X to Z mod p Zx. So here f goes to f bar. So you reduce all the coefficients modulo p.

Now, check for irreducibility in f bar, so f bar is referred to as f modulo p, so if f bar is irreducible, so the statement is that if f bar over in Z p, Z mod Zp x is irreducible, implies f in Qx is irreducible. Okay, this is also sometimes useful, though again, it is most useful when degree is 2 or 3 because irreducibility over Z mod pZ is not easy to determine, the most easy case is when you have small degree, so you can check directly for roots.

(Refer Slide Time: 22:18)



$f \in \mathbb{Z}/p\mathbb{Z}[x]$ is irr $\rightarrow$ ...

eg: $x^3+x+1 \in \mathbb{Z}[x]$, $p=2$

$\underbrace{x^3+x+1 \in \mathbb{Z}/2\mathbb{Z}[x]}_{\text{is irr}}$: $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$ $\begin{cases} 1^3+1+1 = 3 = 1 \neq 0 \\ 0^3+0+1 = 1 \neq 0 \end{cases}$

$\Rightarrow x^2+x+1$ is irr/$\mathbb{Q}$.

Same method works for $\begin{cases} 3x^3-11x+8 \quad \text{or} \\ 13x^3-8x^2+101x+99 \end{cases}$

both of these reduce to x^3+x+1 in $\mathbb{Z}/2\mathbb{Z}[x]$

are irr/$\mathbb{Q}$.

For example, if you take X cube plus x plus 1, and you take p to be let us say 2 so here, you take x square plus x cube plus x plus 1 in Z mod 2Z x. And remember our first method to check for irreducibility in degree 2 and 3, you simply check for roots. If you want to do that checking for roots in Zx, it is difficult because Z has infinitely many elements. So who knows which one has a root though analysis will tell you, but over Z mod 2Z it is even easier, because Z mod 2Z has only two element, three elements, sorry two elements. So check for both of them.

So, 0 cube plus 1 plus 1 is sorry, 1 cube plus 1 plus 1 is 3, which is, which is actually equal to 1 not 0. Similarly, check for 0, 0 cube plus 0 plus 1 equals 1 not 0. So, this is irreducible and hence, by the third criteria that I am giving, it is irreducible over Q directly we can say.

And this in fact, works not just for this, same method for lots of polynomials, for example, all you need is that the coefficients of x cube x and 1 are odd or you can have 13x cube minus 8x square plus 101x plus 99, because if you go modulo two what you get is x cube 13 is 1, 8 is 0 so x square term will vanish, 101 will give x, 99 will give 1.

So, both of these reduced to x cube plus x plus 1 in Z mod 2Z, so that we have checked already is irreducible. So these are irreducible, these both are irreducible over Q, so that is the main techniques that I wanted to give you. There are some other things called rational root test and so on, but whenever we discuss this in detail, and we need to use those and I will recall them, but for now these will suffice.

So, these are interesting and useful techniques to check for irreducibility. And very soon in the course you will see why these are useful for us. So, I will stop the video here. In the next video we will start a revision of the field theory that we will use in the course. Thank you.