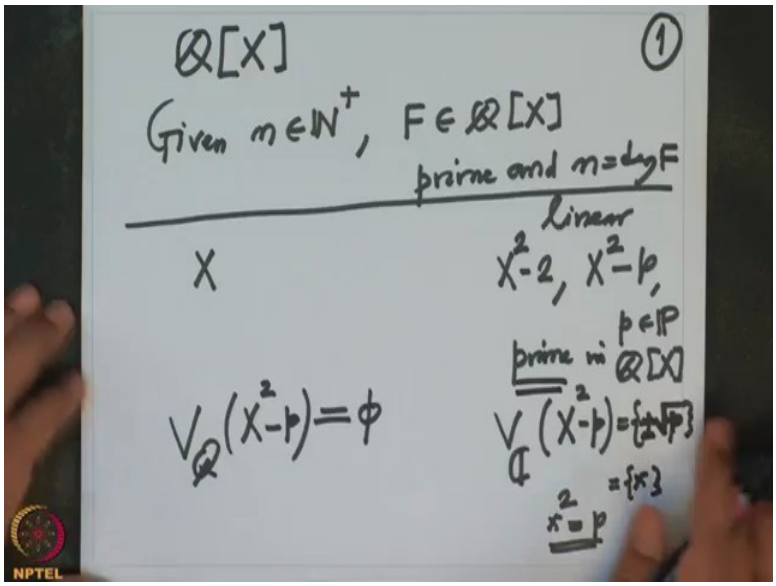
Galois Theory
Professor Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 10
Gauss's Theorem (Uniqueness of factorization)

Let us continue discussion about the polynomials, we have seen in the last part that if you want to list all prime polynomials (in) with real coefficients then they are only two kinds one is linear one and the other is a polynomials which are degree 2 and their discriminant should be negative these are the only two possibilities for a prime polynomial in real numbers.

(Refer Slide Time: 1:08)



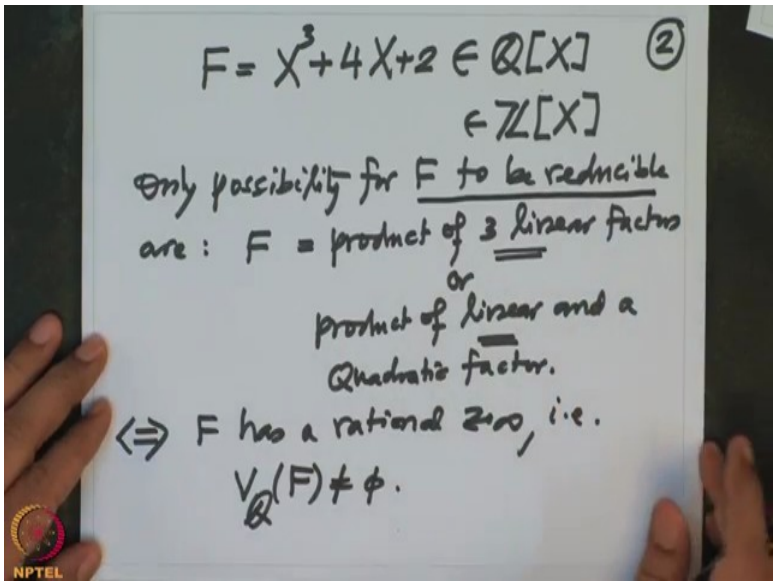
Now let us try to do this thing similarly for what about field $\mathbb{Q}$ what about $\mathbb{Q}[X]$? I want to find the possibility for two things, number one whether is there any given any degree n, given n any natural number I want to produce polynomial F with rational coefficients which is prime and the degree is n, n positive. So this will show that in contrast to the real numbers here polynomials can be of arbitrary degree, there are prime polynomials of arbitrary degree.

So first let us this is what I want to show. So first let us consider the polynomial of course you can write down many polynomials of degree linear ones of course exist there are many linear polynomials which are prime and many quadratic also degree 2 also for example X square minus 2 or more generally X square minus p they are all degree 2 polynomials these are as p varies in prime numbers these are all degree 2 and they are prime polynomials over $\mathbb{Q}$ in $\mathbb{Q}[X]$ prime in $\mathbb{Q}[X]$ simply because we know what are the zeros of these

polynomials in complex numbers, zeros of this polynomial for example $V_{\mathbb{C}}(X^2-p)$ this is square root of p with a plus sign or minus sign, these are the zeros - p here no (plus p) root p plus p and square root can have two signs either plus or minus.

It is better to write that as small x, where x^2 is p and (these are non so) these are non-real no they could be real, they are non-rational complex numbers. So therefore none of them is in $V_{\mathbb{Q}}$ of this polynomial is empty set. So it does not have a linear factor, so therefore they are prime polynomials.

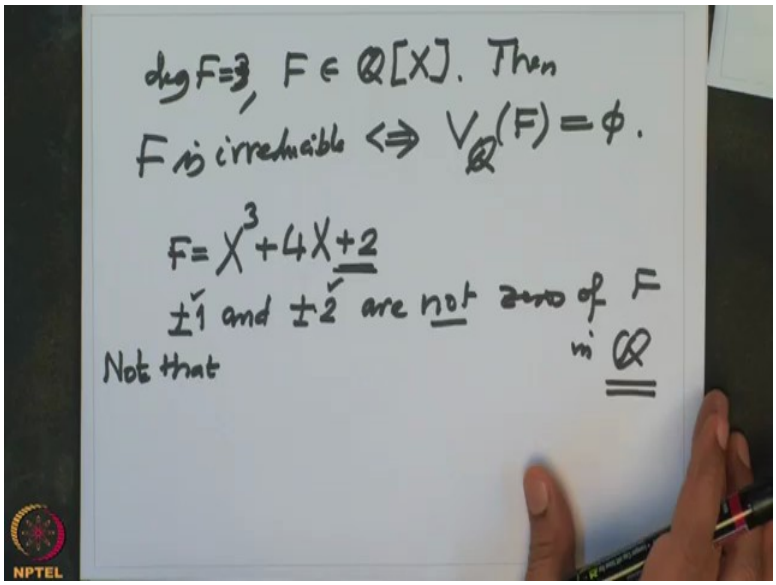
(Refer Slide Time: 4:32)



Now at least one cubic polynomial and just a method and then I will write down the formal criterion, how do you test rational polynomials are prime or not? So first let us look at the polynomial F equal to X^3+4X+2 this is a polynomial with rational coefficients, actually this polynomial has an integer coefficients and I want to analyse whether F is reducible or not. So if F is reducible the only possibility is it has linear all the 3 linear factors or one linear and one quadratic these are the only two possibilities.

So only possibility for F to be reducible are F is a product of linear product of 3 linear factors or product of a linear and a quadratic factor or in both the cases the linear as we have seen factors corresponds to the rational zero, so in both the cases one linear factor is there or equivalently F has a rational zero, again that means in our notation $V_{\mathbb{Q}}(F)$ is non-empty that is equivalent to saying that F is reducible. So when can F be reducible negation of that, so F is reducible if and only if $V_{\mathbb{Q}}(F)$ is empty set.

(Refer Slide Time: 6:52)



So in other words if degree of F is 3 and F is in $\mathbb{Q}[X]$. Then F is irreducible if and only if $V_{\mathbb{Q}}(F)$ is empty set. So to test whether the given polynomial X^3+4X+2 I want if I want to check it is reducible I should check whether this is empty set or not and how do I check that? So that is in general it is easy to see that the only possibility for a zero to be ± 1 and ± 2 are not zeros of this F.

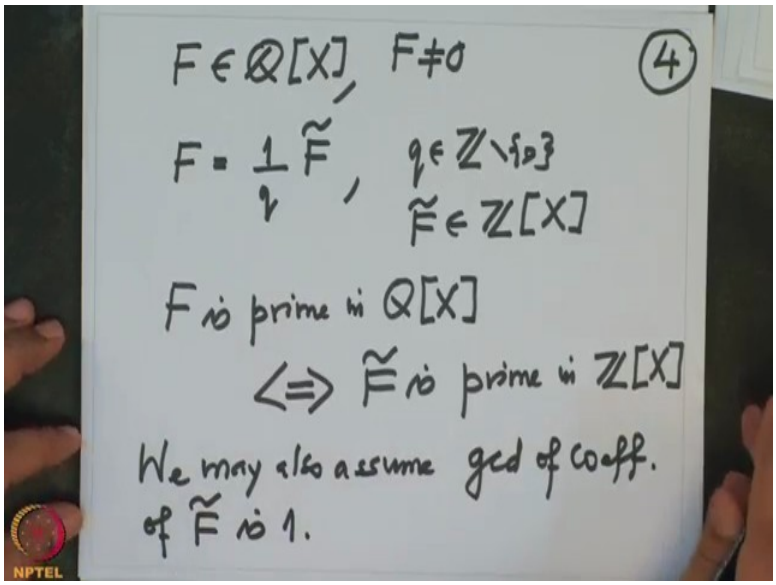
Note that $+1,-1,+2,-2$ they are not zeros of F in $\mathbb{Q}$. Let us test that, that is I just have to plug it in X equal to 1 then this is 1 + 4 + 2, so a positive thing will not work clearly, if you have put -1 this is -1-4+2 is -3 is not 0, so this we have checked. Similarly this we checked that plugging X=2 don't give a zero and how do I know that I only have to test this that is because look at the constant term, the constant terms factors are plus 1 minus 1, plus 2 minus 2.

So in general if somebody has a zero that is speciality about $\mathbb{Q}$, then these are the only two this will become clear when I write more general statement soon and the earlier statement that if I have a degree 3 polynomial over $\mathbb{Q}$ then we know that it is irreducible if and only if this at least one no zero in $\mathbb{Q}$ this statement is true for any field because degree 3 polynomial how can it factor over any field? That either one factor is linear and one factor is quadratic or 3 linear factors, in any case one linear factor occurs for arbitrary field, so this statement is for arbitrary field, the I only thing I use rational numbers here that it is enough to test that the

divisors of the constant term with integers integer divisors of the constant term should not be zero of that F then F will be irreducible over $\mathbb{Q}$.

Okay, so in general you have realized that in general it is not easy to test even for $\mathbb{Q}$, whether the polynomial is irreducible or not.

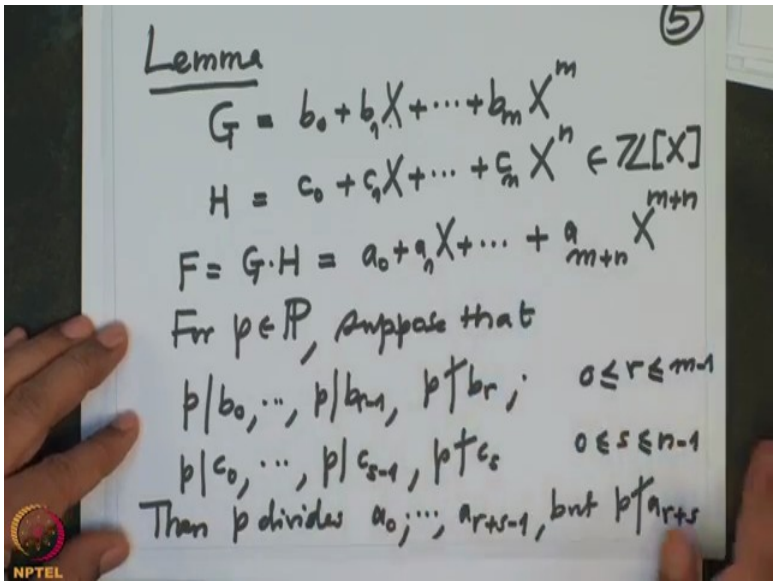
(Refer Slide Time: 10:28)



So now I am working now we are we want to check whether we can give some better way to test rational polynomials are reducible or not? So I am preparing for that now. For example you start with the polynomial F in $\mathbb{Q}[X]$ and let us assume F is non-zero. Now the first step is you write this F as take out the common denomenator see F has rational coefficients so each coefficient has canonical representation that is a integer by integer. So from each coefficient I am going to make the common denominator by supplying up and down by in multiplying the so I will write this as 1 by $\mathbb{Q}$ F tilde, where this $\mathbb{Q}$ is a non-zero integer and F tilde is actually has integer coefficients because 1 by $\mathbb{Q}$ is a common denominator.

So if I want to decide about reducibility or irreducibility of F in $\mathbb{Q}[X]$ it is enough to decide for F tilde. So F is prime in $\mathbb{Q}[X]$ if and only if (F tilde is prime in $\mathbb{Q}[X]$) F tilde is prime in $\mathbb{Z}[X]$ because now F tilde is a polynomial with integer coefficients. So more over I will also assume that all the coefficients of F tilde they may have some common factor, so we may also assume gcd of coefficients of F tilde is 1 remember gcd when we say gcd of integers it is always a positive integer. So gcd of the coefficient so such the gcd is also called the content sometimes but I will not use it now until sometime.

(Refer Slide Time: 13:36)

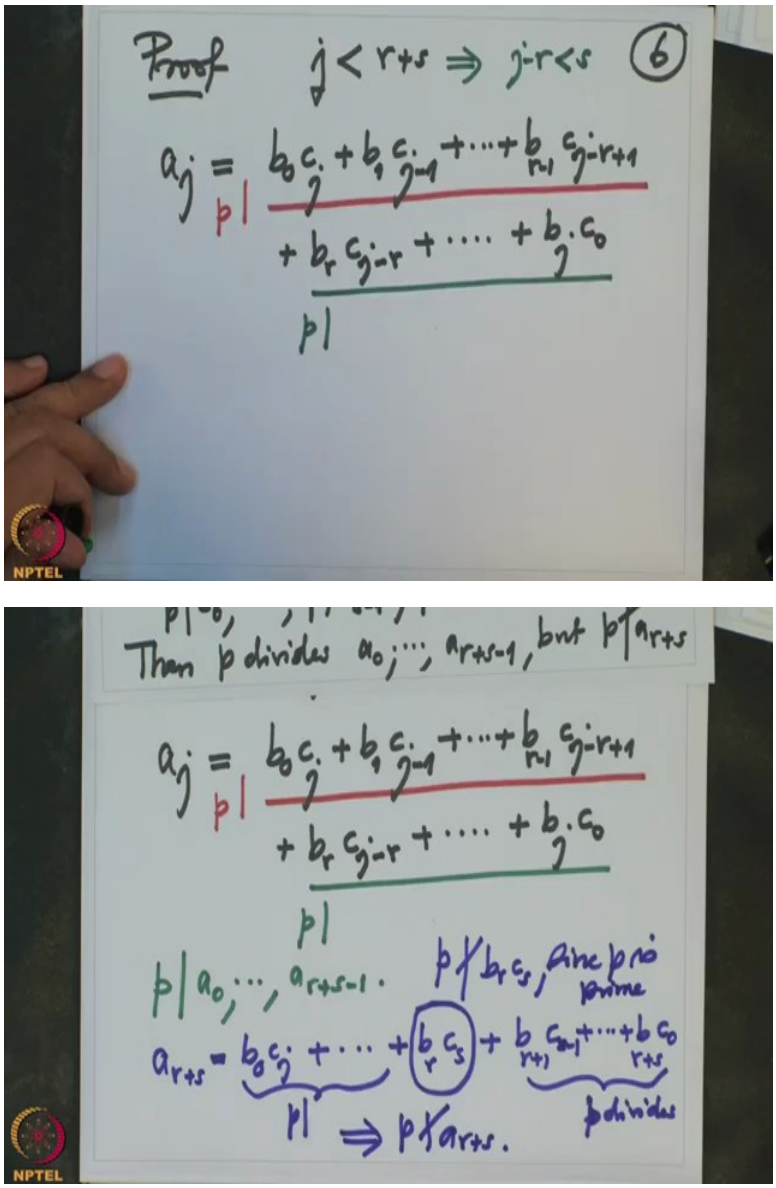


So therefore without loss we want to find a criterion for integer polynomials to be irreducible and for that I can also assume it is not necessary but I can also assume the polynomials are monic, but I will not do so. So page number 5, so this is the very important lemma this lemma is important for this, so I have two polynomials G and H, so G is written as $b_0 + b_1 X + \ldots + b_m X^m$ and H is $c_0 + c_1 X + \ldots + c_n X^n$ these are two polynomials in $\mathbb{Z}[X]$ and I want to call their product is $F = GH$.

So by definition F is reducible, G and H are proper factors if (m and n are not) m and n are at least 1, okay. So this product I have written it as $a_0 + a_1 X + \ldots + a_{m+n} X^{m+n}$, so G is of degree m, H is of degree n and then F is of degree $m+n$. Okay, for a prime number p suppose that p divides these coefficients upto some place p divides b_0 ,..., p divides b_{r-1} and p does not divide the next one b_r , where r is in between 0 and $m-1$.

Similarly for c's that is p divides c_0 , p divides c_{s-1} and p does not divides c_s , $0 \leqslant s \leqslant n-1$. You start looking at the coefficients the moment it does not divides p does not divides that stop there, earlier all coefficients are divisible by p, similarly here okay then if that is the case then what is the statement? Then p divides the coefficients p divides a_0 upto a_{r+s-1} , but p does not divide the next one a_{r+s} let us proof this, this is very useful fact. See p divides upto some place, p does not, p divides upto some place, p does not divide, then the same thing here happens.

(Refer Slide Time: 17:38)



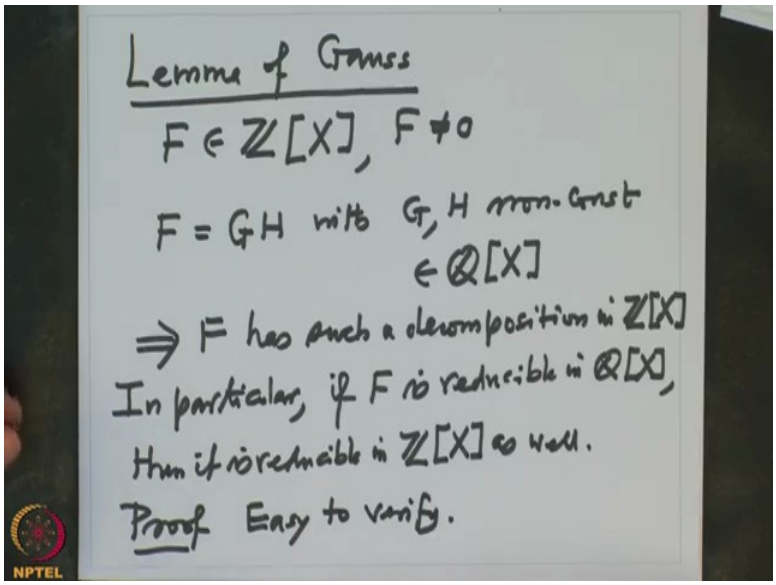
Okay, let us proof this and then we will deduce the consequences. So let us compute the coefficient I want to write down a formula for a_j . So take any coefficient a_j , so for proof if j is smaller than $r+s$ then what is a_j ? a_j is $b_0 c_j + b_1 c_{j-1} + \ldots + b_{r-1} c_{j-r+1}$ and then I cannot go on to the so the next one is $b_r c_{j-r} + \ldots + b_j c_0$ I can go on upto I can descend the index of c to 0, the index of c is descending and index of b is increasing so this is a_j .

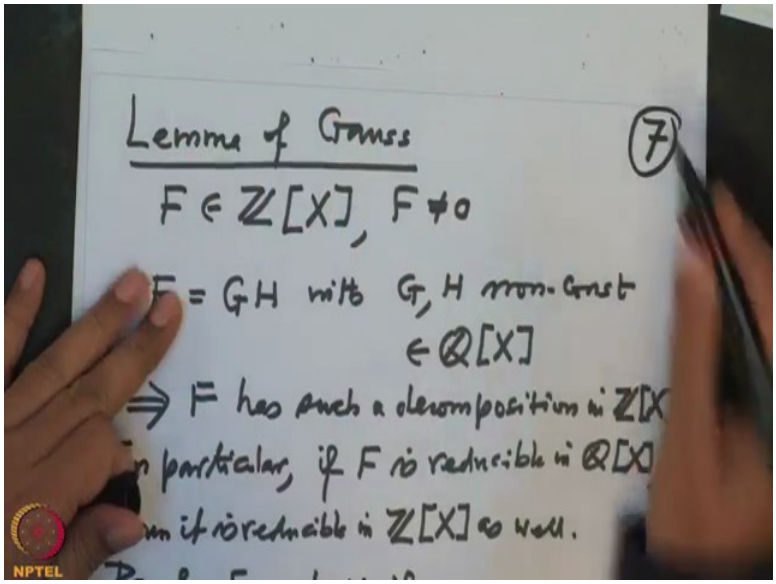
So in this p divides b_0 , p divides b_1 , p divides b_{r-1} , so this sum is divisible by p, this sum p divides p divides this sum. Similarly now I do not look at b's I look at c's (c_0) p divides c_0 , p divides c_1 , p divides c of this one because this one is $j-r$ is smaller

than s because of this $j-r$ is smaller than s, so therefore this sum p divides this so all together p divides this, so that proves the first part all this p all this p divides all these guys that is what we proved. So what we have proved is p divides a_0 to a_{r+s-1} .

Now I have to show that p does not divide the $r+s$ the next one, so what is that coefficient? So just write a_{r+s} this will be again $b_0 c_j$ and now it will go on till b_r what will be the coefficient of b_r ? That will be c should and plus $b_{r+1} c_{s-1}$ and it descend, so this is $b_{r+s} c_0$. See this term is extra and all these terms are divisible by p, this is also divisible by p, p divides and this one? p neither divides b_r nor p divides c_s . So therefore because p is prime p does not divide $b_r c_s$ because since p is prime, therefore p cannot divide that proves p does not divide a_{r+s} , that is what it proves the lemma.

(Refer Slide Time: 21:08)



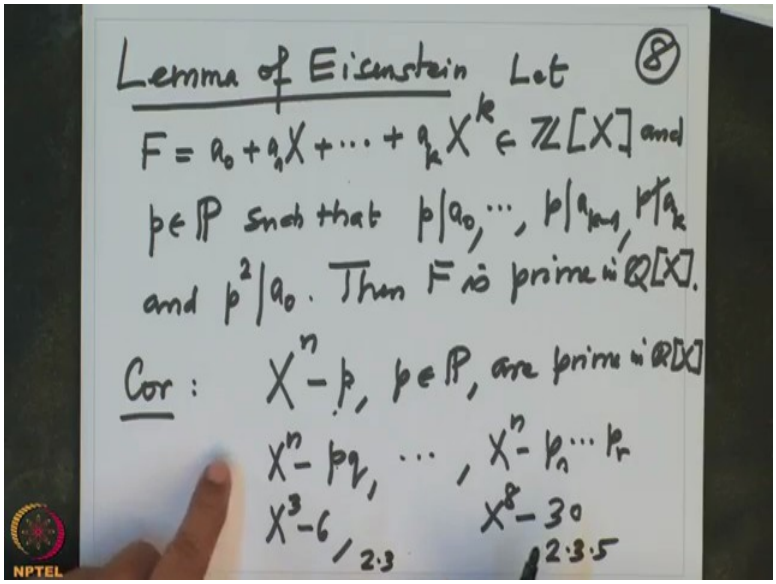


So remember this (we will) I will immediately use it to proof some nice things. So this is Lemma of Gauss, okay we have polynomial F in $\mathbb{Z}[X]$ integer coefficients, F is non-zero and suppose of course suppose F is of the form G times H with G and H non-constant polynomials with rational coefficients G and H are rational coefficients and F is this, then F has such a decomposition in $\mathbb{Z}[X]$ also.

So that means so in particular if F is reducible in $\mathbb{Q}[X]$, then it is reducible in $\mathbb{Z}[X]$ also, okay and proof I will just say easy to verify that will saving couple of minutes. So this is where you are using very important property of ring of integers which says that the ring of integers has that fundamental theorem of arithmetic that is that in the modern language it is said that the ring of integers is a unique factorization domain that means factorization exist, factorization into prime numbers exist and it is unique essentially unique upto order.

So such a theorem is called fundamental theorem of arithmetic, so arithmetic we are calling it because we were the school days arithmetic was done with the integers only and rational numbers. Now as we go to college and when we start studying integral domain then one calls them as a unique factorization domain that means it is an integral domain where the corresponding property holds and this fundamental theorem of arithmetic or prime decomposition of the polynomial K X that is the corresponding theorem.

(Refer Slide Time: 24:36)

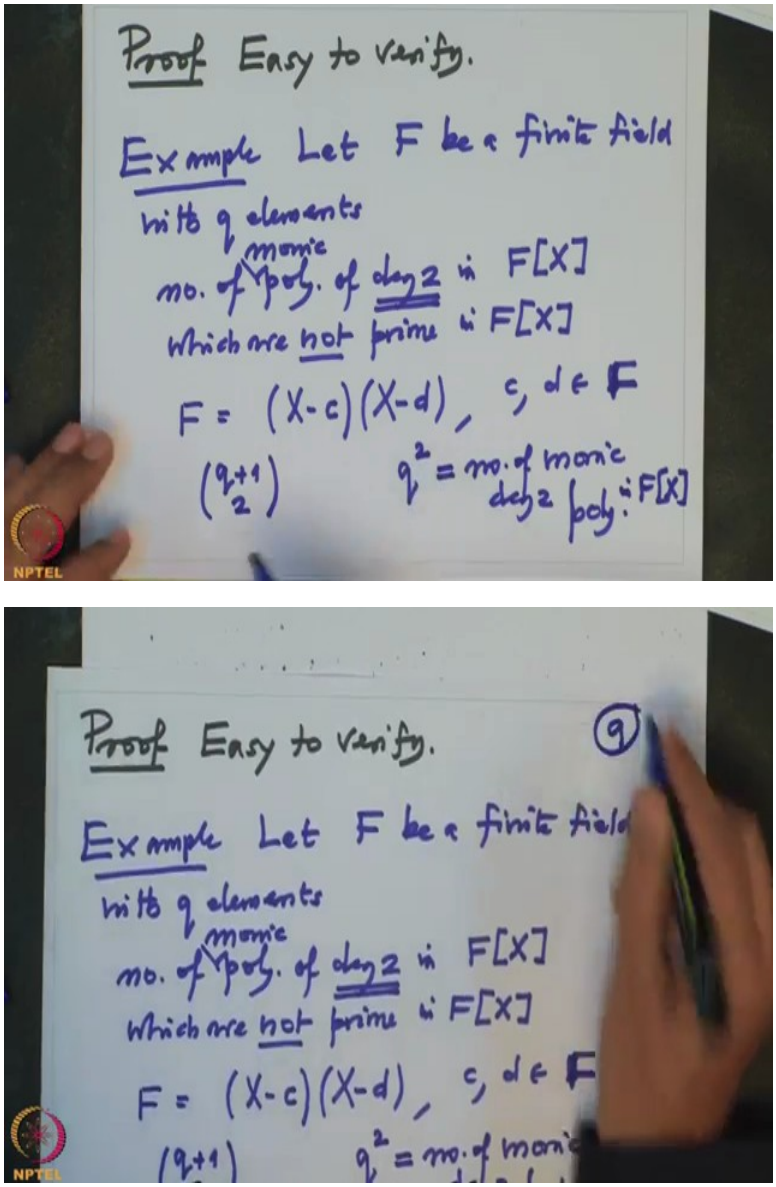


So the continuing that now I want to state very important lemma which is used very very often that is called (the little) so to produce or to check given polynomial in $\mathbb{Q}[X]$ is reducible or not, the following lemma is very very useful used very often Lemma of Eisenstein, what does it say? It says that suppose I have polynomial $F = a_0 + a_1 X + ... + a_k X^k$ this is degree k polynomial in integers and p be a prime number so I should have said let this and p be a prime number such that p divides a 0 upto p divides a_{k-1} the leading coefficient is a k, so p does not divide a_k , p divides all other but p does not divide the leading coefficient of F.

And in addition to this p square should not divide a 0. Then F is prime polynomial in $\mathbb{Q}[X]$. So before I proof this proof is very easy, before I proof this I just have to say that immediate corollary is if I take any $X^n - p$, p prime, these polynomials are prime in $\mathbb{Q}[X]$, simply because the leading term is 1, so I can take this p does not divide the leading term leading coefficient and the constant term is divisible by p, but not p^2 therefore we can apply Eisenstein criterion and say this polynomial is prime in $\mathbb{Q}[X]$, not only one prime we can take two at a time because then I can choose any you can apply Eisenstein lemma to either p or $\mathbb{Q}$ we can choose and nothing special about two, we can go on till $X^n - p_1 ... p_r$.

So for example $X^3 - 6$, or $X^8 - 30$ these polynomials are prime in $\mathbb{Q}[X]$ because here I took 2 into 3 into 5 these are prime number, here 2 into 3 and so on. So this will give lots of examples of prime polynomials in $\mathbb{Q}[X]$.

(Refer Slide Time: 28:05)



Now just let us finish the proof. So proof of that actually okay so the proof is essentially what we have done it in earlier case that if it factors then write down the equations and then you will realize that you will get a contradiction or you can also do it. So you write down and then check all coefficients are not divisible by p and then again choose r and s like earlier lemma. So I would just say easy to write down the proof easy to verify.

Please do this, now just last couple of minutes I will make some remarks about a finite field so let me write this as an example. So let F be a finite field with q elements we have not proved such a construction but we will do it next time we will do it sometime. So now I want to count the number of polynomials of degree 2 in $F[X]$ which are not prime in $F[X]$.

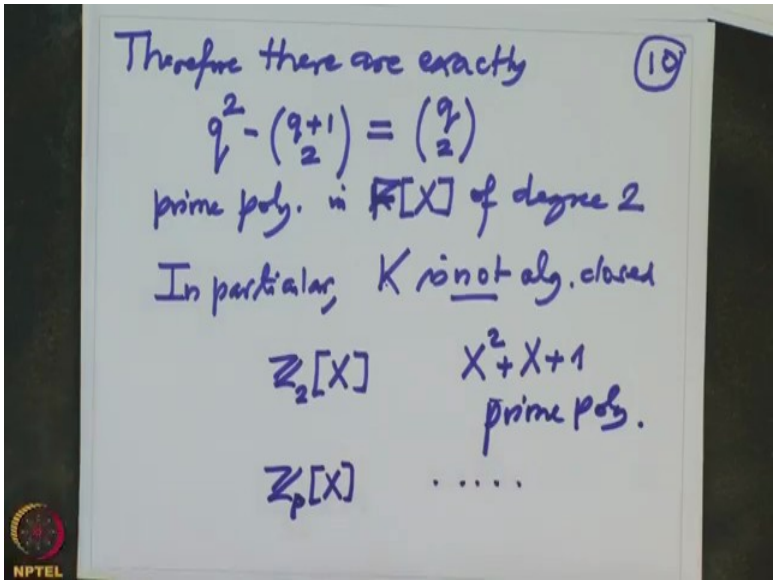
So how do I count that? Because it is degree 2 how can and let us say number of monic polynomials.

So how can a degree 2 monic polynomial will not be prime? The only possibility is it splits into two linear factors linear factors may be repeated or non-repeated, so that is only it can happen when (X is of the) F is of the type $(X-c)(X-d)$, where c and d are two elements in F and we just have to count them, how many?

So that means c and d varying in F, so we have to choose two elements so they are how many? They are they can be repeated so they are precisely $(q+1)C_2$, they are precisely so many polynomials because I am counting repeated also and how many monic polynomials are there all together? All together there are q^2 monic polynomials, q^2 is the number of monic degree 2 polynomials in $F[X]$ because monic so the degree X square coefficient is 1 and now only we have to count the coefficient of X and coefficient of constant term.

So there are two positions and in field they are setQ elements therefore we will have setQ square elements. So how many will be prime among them? These are the non-primes and the primes will be therefore the difference.

(Refer Slide Time: 32:14)



So the difference so what we know therefore is therefore there are exactly $q^2-(q+1)C_2$ there are exactly so many prime polynomials monic is included you know definition, prime polynomials in (K[X]) F[X] of degree 2 and what is this number? This number is nothing but

qC_2 , so what did we checked? We actually found out how many prime polynomials are there of degree 2 in F[X] in a finite field with q elements.

So in particular, K is not algebraically closed because if it were algebraically closed then there will be only linear polynomials, but these are the number of polynomials which are prime polynomials and this number is at least 1. So the only prime polynomial have degree 2 in $\mathbb{Z}_2[X]$ it is X^2+X+1 because q is 2 in that case, qC_2 is 1 so this is the only prime polynomial.

If I take $\mathbb{Z}_p$, then there will be more and then you can list them, this information is very very useful when you are applying these things to the practical use like designing bank cards and ATM cards and pins and so on. So that we will deal it sometime (in the) when we deal with concrete applications to summarize this lecture in the last we have given examples of fields which are non-algebraically closed that means there are polynomials which are not they are polynomials which are not linear ones and they are prime polynomials.

And we have explicitly given examples of such polynomials over many fields like rational numbers, real numbers and finite fields, whereas the only field which we have stated to be algebraically closed is the field of complex numbers and this theorem I will prove it in the coming lectures and also give a general construction of an algebraically closure of a field, so this will also be in the coming lectures, thank you very much we will continue in the next time.