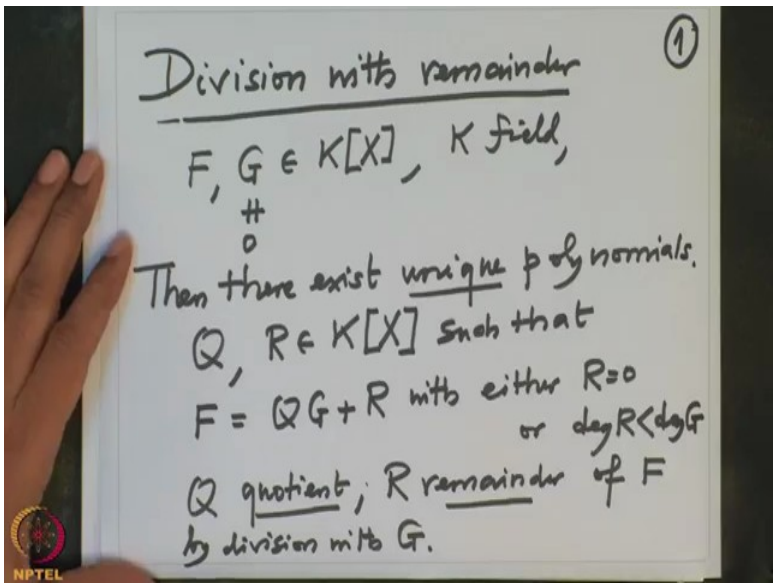
Galois Theory
Professor Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 6
Division with remainder and prime factorization

Let us continue our study of polynomials over a field and one of the most important thing which I will state now is about the division. So we already study such property of integers in the school, so I will not recall what is called division.

(Refer Slide Time: 0:54)

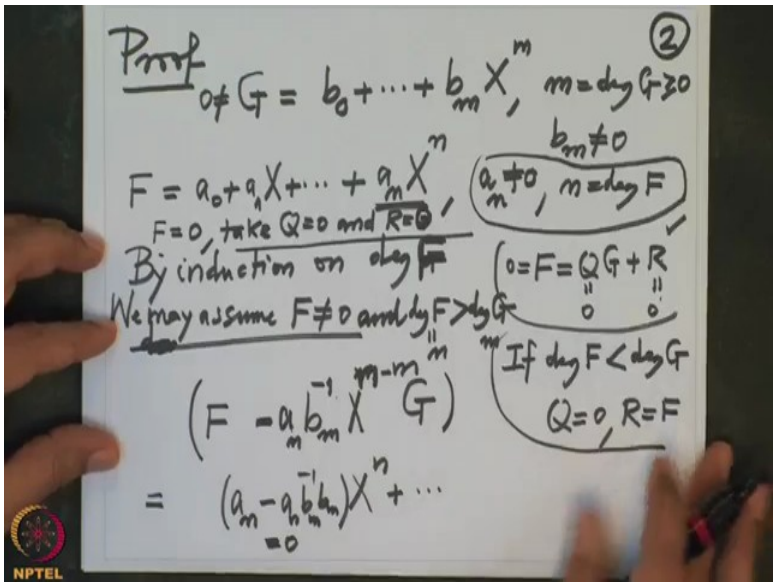


What I am trying to call now is division with remainder. So we have two polynomials F and G with coefficients in the field K and let us assume G is a non-zero polynomial, I want to remind you again that we have not defined degree of zero polynomial, so degree of a zero polynomial is not defined. Now we are given two polynomials and G is non-zero polynomial then I want to divide F by G and look at the quotient and remainder.

So then the assertion is there exist unique polynomials Q and R coefficients in K again such that $F=QG+R$ with either R is 0 or degree of R is strictly less than degree of G and once we prove this uniqueness, (we will take) because of uniqueness, Q is called quotient and R is called remainder of F by division with G, we will proof this statement but before we prove I just want to remind you this is what we studied in school. If you remember given two integers or, studied with a natural number, given two natural numbers one of them non-zero then we could divide the other natural number by a non-zero natural number to get a quotient and remainder and the remainder the role of the degree is played by the modulus.

So the magnitude of the natural number, so either the remainder should be less than that the dividend or it is 0 and this is a similar thing what we want to prove it instead of integers we want to prove it for the polynomials and you will see the proof is very easy.

(Refer Slide Time: 4:38)



So let me indicate the proof. So we are given F and G, so let us first write G, G is $b_0+...+b_m X^m$, m is the degree of G which is this b_m is non-zero therefore and this is G non-zero polynomial, so degree is bigger equal to 0 and define bigger equal to 0 and F is $a_0+...+a_n X^n$, where a_n is non-zero and n is the degree of F (when F is) I can write this only when F is non-zero remember that otherwise I have no information if F is 0 and we are looking for Q and R.

So I am going to prove the assertion by induction on the degree of G, I cannot say induction on the degree of F, degree of F may not be defined when F is 0, so induction on the degree G. So induction will starting the beginning of induction should be at. So let us look at degree of F. So before I have started with this if F is 0 then there is nothing to proof because if F is 0 you take Q equal to 0 and R equal to G, now (R equal to) Q is 0 and R is also 0 because let us write the equation what we want to satisfy (Q) F should be equal to QG plus R, so if this was 0. So obviously this equation is satisfied Q and there is no condition on Q and there is a condition on R that is R is either 0 or the degree of R is strictly less than degree of G that is also satisfied.

So if F equal to 0 then there is nothing to prove it is very easy. So we may assume F is non-zero and now we will prove our assertion by induction on the degree of F, so this sentence I

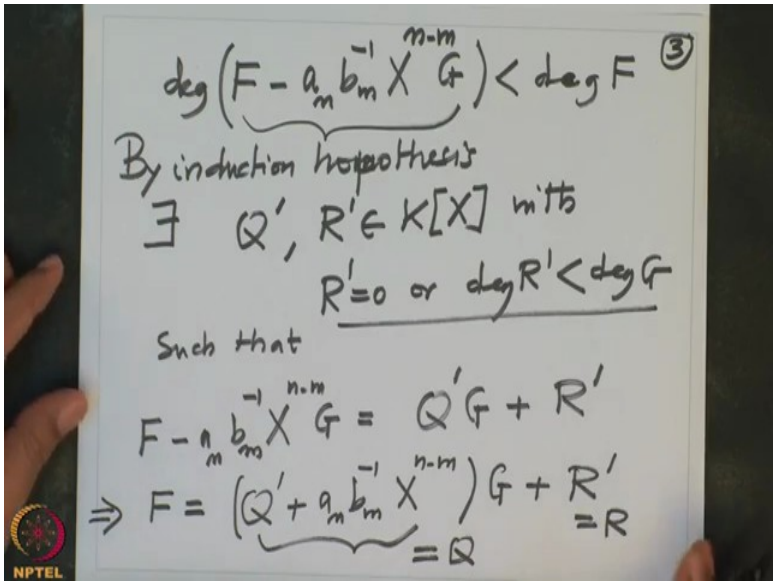
should have said it here so by induction on degree of F so F is now like this and what do I want? I assume now the statement for the smaller degree polynomial than F and then prove it for degree F, so that means I want to reduce the degree of F by using the polynomial G, so what do I do?

(Take) so I want to cancel this coefficient and fortunately over a field, so what do you do? You make multiply G by b_m^{-1} which exists because K is a field and b_m is a non-zero element of the field so this exist and then I want to cancel this n, so I will multiply this by X^{n-m} look at this polynomial G, first of all I also I have again forgot to make a comment that if n the degree of F is n if degree of F is smaller than degree of G so I will write in the side if degree of F is smaller than degree of G then again I will take Q equal to 0 and R equal to F then also this equation is satisfied, so therefore without loss I would have assume F is non-zero and degree of F is strictly bigger than degree of G should assume that.

So now we are trying to cancel the top degree coefficient of F, so what do I do? I consider this you remember what did I do with this, now G as leading coefficient b m and I multiply by b_m^{-1} this become 1 and I multiply by this X^{n-m} , now that is allowed because we are assuming we are assuming this is n and this is m, so we are assuming n strictly bigger than m, so this is (some positive) some natural number so this what is the leading coefficient of this is precisely X^n because the leading coefficient got cancelled and then this power became X power m, so leading coefficient is 1 here and you can multiply by a_n now minus a_n and then subtract this quantity from F what do I get?

Let us look from the top degree that is this is $a_n X^n$ I want to compute the coefficient of X^n plus lower degree term so from here it is coming a_n , from here it is coming $a_n b_m^{-1}$ and b_m so that is $a_n b_m^{-1}$ b_m but then this is 0 so therefore the degree of this quantity.

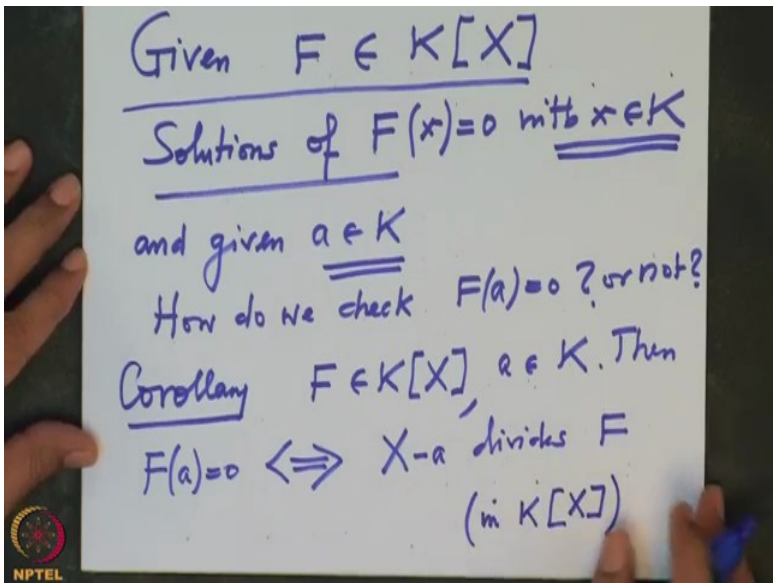
(Refer Slide Time: 11:48)



So let me write the result the degree of this polynomial $F - a_n b_m^{-1} X^{n-m} G$ this degree of this new polynomial strictly smaller than (degree of G) degree of F. Therefore by induction hypothesis I can apply the induction hypothesis to this polynomial this degree smaller so by induction hypothesis there exist Q' and R' two polynomials with either R' is 0 or degree of R' is strictly smaller than degree of G such that this polynomial $F - a_n b_m^{-1} X^{n-m} G$ this is equal to $Q'G + R'$ this is induction hypothesis.

Now I simply what do I do? I simply shift this term to the other side, so that will imply so therefore F will be equal to shift this to the other side and take G common. So $Q' + a_n b_m^{-1} X^{n-m} G + R'$, so this is my Q the one I am looking for and this is my R and so this condition remains same and on Q there is no condition, so we have found a polynomial Q and polynomial R with the required conditions. So this is division algorithm this is very very important you will see in a minute that I want to check now.

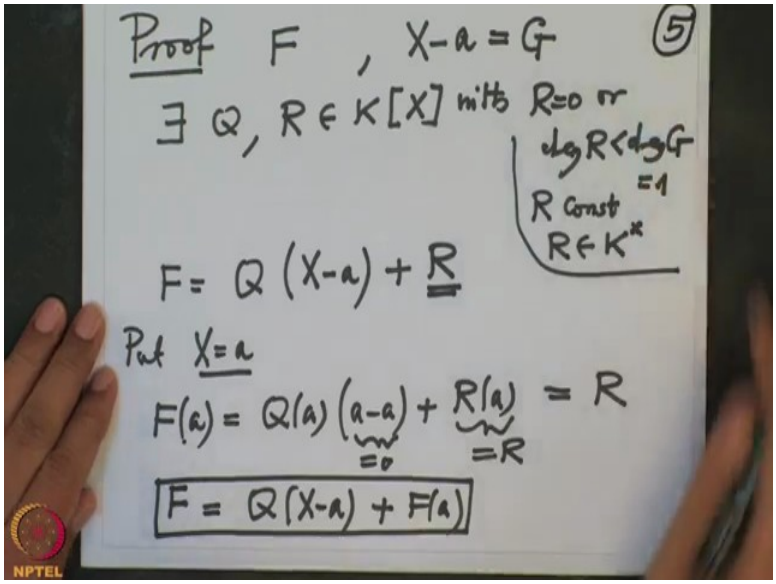
(Refer Slide Time: 14:26)



For example our problem let me remind you our problem was what? Our problem was given a polynomial so given a polynomial F with coefficients in a field, we are looking for the solutions, so solutions of F in K let us say. So solutions of $F(x)=0$ with $x\in K$ this is what we are looking. So that means we want to decide how do you check for a given polynomial so given F and given an element a in K, how do you check that this a is a solution of F? That means how do we check how do we check F of a is 0 or not?

So that is we will use now we will use now a division algorithm, (how do you) division with remainder so that is so let us write in the form of corollary. So we are going to apply to this given F, so F is a polynomial in K[X], a is a given element in K, then F of a is 0 if and only if the linear polynomial X minus a divides F, but again when you say divides F we should better write in K[X]. So let us proof this, this is very easy (I wrote it on this page is pe likh diya maine)

(Refer Slide Time: 17:58)

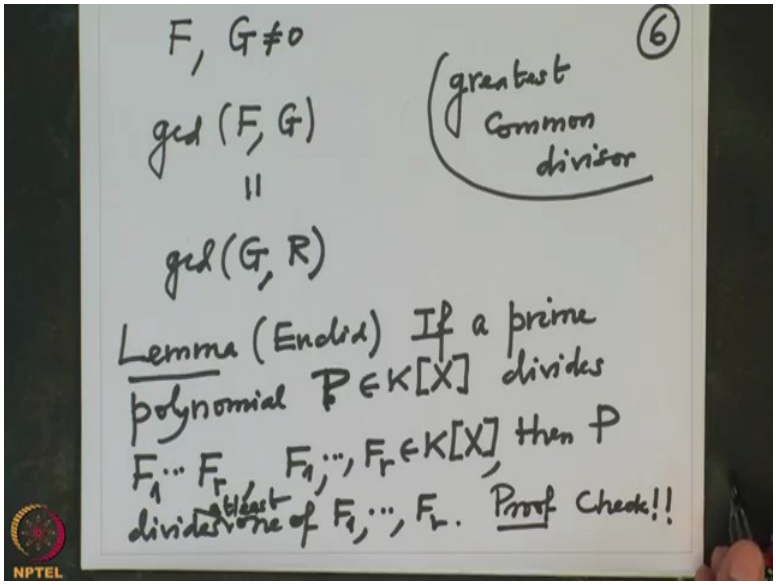


Okay, so let us continue with the proof, so we have now given F and also we have given this linear polynomial and this is my G now I am going to apply division with remainder by dividing by F by dividing by G then what do we get? There exist Q and R in the polynomials again with either R is 0 or degree of R is strictly smaller than degree of G, but degree of G is 1, so this R has to have the only possibility is R is the constant polynomial or R is 0, so this whole thing means R is constant that means R is an element in K^x actually strictly speaking so that is information.

So we have written F as $Q(X-a)+R$, but now I want to find what is R? Now in this equation this is equation about polynomial and I am going to put X equal to a, what do I get? This side I will get F(a), the other side I will get $Q(a-a)+R(a)$, but R(a) is R itself because it is a constant polynomial and this is 0, so all together it is R, so this R we have found in terms of F and a that is F of a.

So that proves that F equal that proves the formula F equal to $Q(X-a)+F(a)$, this is what it proves. So when will X minus a will divide F, precisely then there is $F(a)$ is 0, so that was the content of this corollary. So division with remainder then when we apply it again and again then we lead to what is called Euclidean algorithm, so that is one way to find a gcd one way to compute a gcd.

(Refer Slide Time: 20:49)



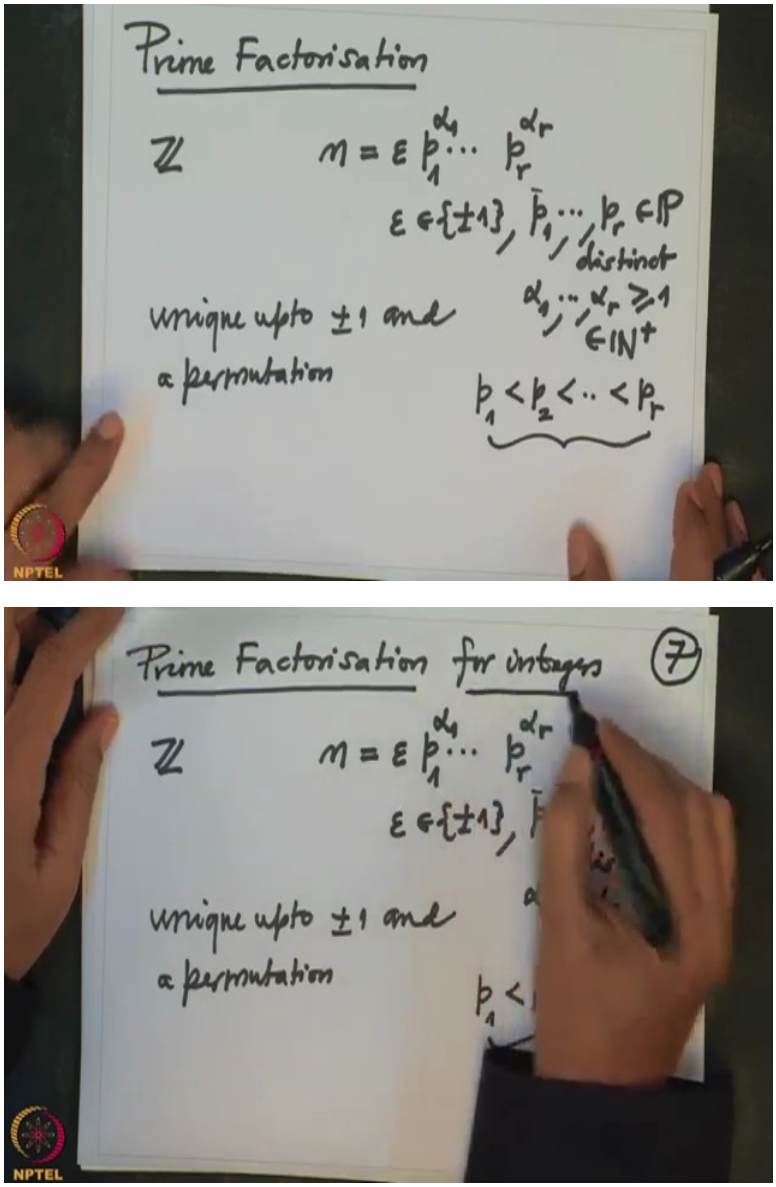
If I have given two polynomials F and G, how do you compute a gcd of F and G? Okay, now when we talk about gcd, gcd means first of all remember the long form greatest common divisor, so why should it exist? We have seen in case of integers it exist and the method to find a gcd was to apply divisional algorithm again and again, so only one step we have to prove it.

So prove that this is I will put this as an exercise for you, so check that gcd of F and G, let us say (F is) G is non-zero this is same as gcd of G and R. So you keep checking it like this so you are reducing the problem to the smaller degree polynomial in this, okay so I will not go much into this because otherwise we will not have enough time to do the do our course justification.

I will also note here one important lemma which is the analogue of the Euclid's lemma what we just mentioned for the integers that says that if a prime polynomial P, capital P is a prime polynomial that means P is a polynomial over K over a field K and it is a prime polynomial that means the only divisors are of the form a times P, where a is constant non-zero constant.

If a prime polynomial P divides the product $F_1 \ldots F_r$ this is the product, where $F_1 \ldots F_r$ are polynomials in K, then P divides one of them P divides one of $F_1 \ldots F_r$, atleast one of $F_1 \ldots F_r$ atleast I should write atleast one of $F_1 \ldots F_r$. This is also very easy to proof so I will not proof this, proof check. If you get stuck you should recall your proof for integers that is like going back to the school, alright.

(Refer Slide Time: 24:41)



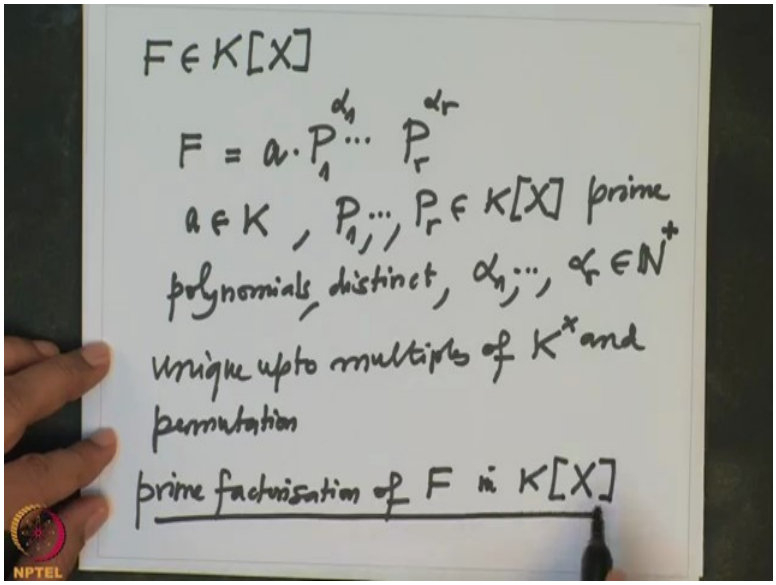
So next fact I want to again mention that this is analogue again with the integers that is the prime factorization. So recall over the ring of integers in the ring of integers any natural number n, we can write it as either +/- that is this sign and product of prime numbers $\epsilon p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, where this ϵ is ± 1 and this p_1 to p_r are distinct prime numbers distinct and this α_1 to α_r are non-zero natural numbers bigger equal to 1 there in $\mathbb{N}$ + I will write that notation $\mathbb{N}$ + is non-zero natural numbers.

So this we have been thought in the school that every number we can divide or we can write it as a product of prime numbers and when you collect the powers of the same prime number that is alpha 1 and so on and it is upto a sign and this factorization is also unique upto a

permutation unique upto plus minus 1 and a permutation of unique upto a permutation that means what?

If I have another prime factorization then first of all the number of the distinct primes is same, sign is same and the prime numbers they will differ only upto a permutation and to avoid that we can also put a condition that p_1 less than p_2, etc etc less than p_r then obviously it will be unique because then there is no question of permuting. So this is a prime factorization for integers. Similarly, we have a prime factorization for polynomials.

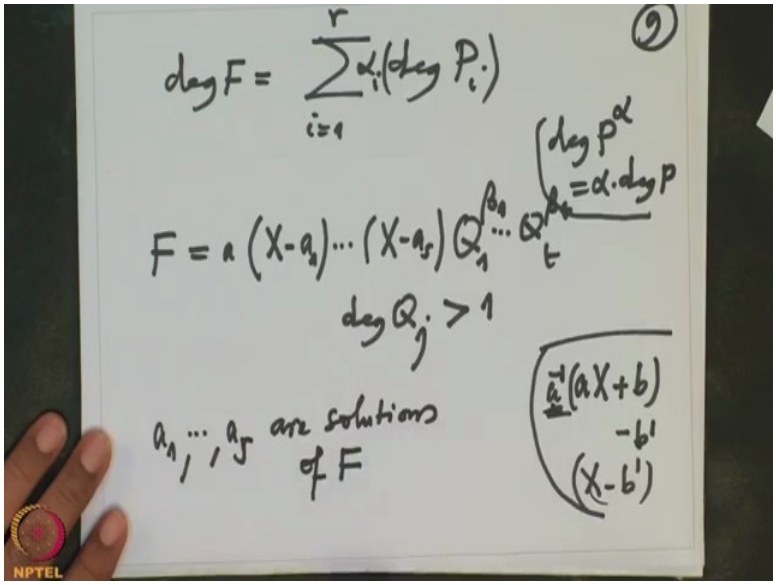
(Refer Slide Time: 27:18)



So for polynomials, for polynomials what do we do? So now we are taking a polynomial F over a field then I want to write this F, now that sign remember that now come as a constant a, where a is in a field and then product of prime polynomials $P_1^{\alpha_1} \ldots P_r^{\alpha_r}$, where this P_1 to P_r are prime polynomials in K[X] prime polynomials, distinct and α_1 to α_r are non-zero natural numbers.

And again such a factorization is unique, unique upto what? Unique upto now the elements of K^x and now there is no way that we can say P_1 less than P_2 and so on, we have to just say that it is unique upto multiples of K^x and permutation. So this is called a prime factorization of F in K[X] and we know that every polynomial has a prime factorization that I am going to assume that, but please go back and check all these things, best way to check is recall your proof or ring of integers and then write the analogues of the polynomials in one variable.

(Refer Slide Time: 30:02)



Now the next step is clear what I am going to do is among these prime factors I will look at the degrees and I will order them according to the degrees degree 1, degree 2, degree 3 and so on and therefore what will I do? Among them I will write the linear ones first, first of all before I write that we have already also information about the degree so degree of F will be equal to sum of degrees of the P_i 's, i is from 1 to r and also the α_i 's you have to multiply by α_i 's because the degree of P^{α} in general equal to α times degree P and then the degree of the product you apply repeatedly that will be this formula.

Now among the P_i 's I want to take out the linear ones first. So F will look like then a and first I will like few linear ones, so that is $a(X-a_1)\ldots(X-a_s)\ldots Q_1^{\beta_1}\ldots Q_t^{\beta_t}$, where now degree of Q_j is strictly bigger than 1, linear polynomials they will look may be they will have coefficient of X here, but I am going to multiply all the inverses and I will absorbe in this new a.

So what I am saying is following, if the linear polynomial looks like this and I want to make it in this form, then I am going to multiply this polynomial by a inverse and change the write this b as minus b prime and then absorbe this a prime a^{-1} also here, so these all together will become $X-b'$, so all the linear polynomials I can write in this form and all this inverse they will get absorbed in this way then the some other letters, right.

So therefore in any case I will reform given F into this one and these are the degree 2 or more polynomials. So obviously now what we know is all these a_i 's all these a_1 to a_r

they are precisely the solutions (s) are solutions of F and these Q's they will not have because I try to take possible. So let me just summarize what we have done in this lecture today at the end given polynomial F with coefficients in a field we have decomposed into prime polynomials, some of them are linear, some of them are non-linear and the linear polynomials we will precisely give the solutions of F equal to 0 in the field K.

So next time we will starting from here we will go on to study solutions of a given polynomial over a given field into a larger field. So this is a big project and we will slowly get into the subject, how do we find all solutions and whether is it possible to have formulas for them or not that is our main concern, thank you very much.