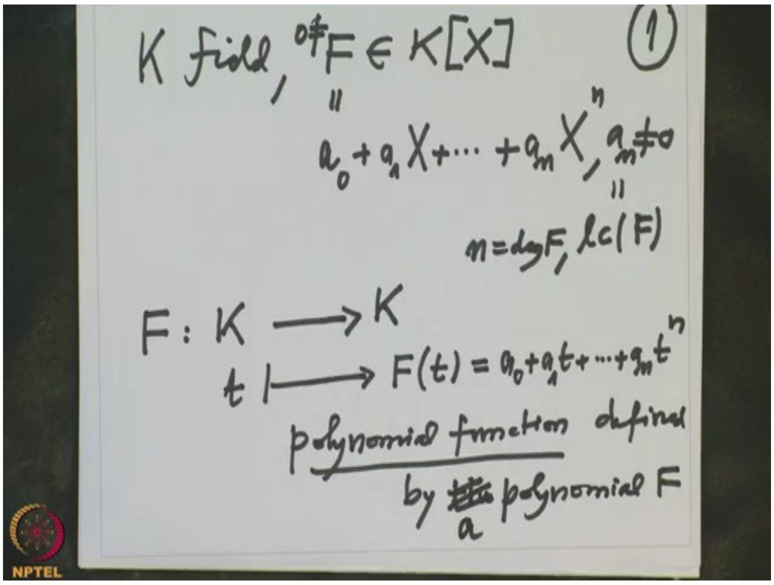
Galois Theory
Professor Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 8
Polynomial functions

Let us continue our study of polynomials over a field specially the zeros of the polynomial, their number, their multiplicities, etc etc this is last in the last half we have seen that if you take polynomial over a finite field $\mathbb{Z}_p$, special polynomial I showed you that it can split into linear factors completely and just from this identity we can also deduce nice formulas like Wilson formula, etc etc.

(Refer Slide Time: 1:10)



K field, of $F \in K[X]$ ①

$$F = a_0 + a_1 X + \cdots + a_n X^n,\quad \underset{\underset{lc(F)}{\|}}{a_n} \neq 0$$

$n = \deg F$, $lc(F)$

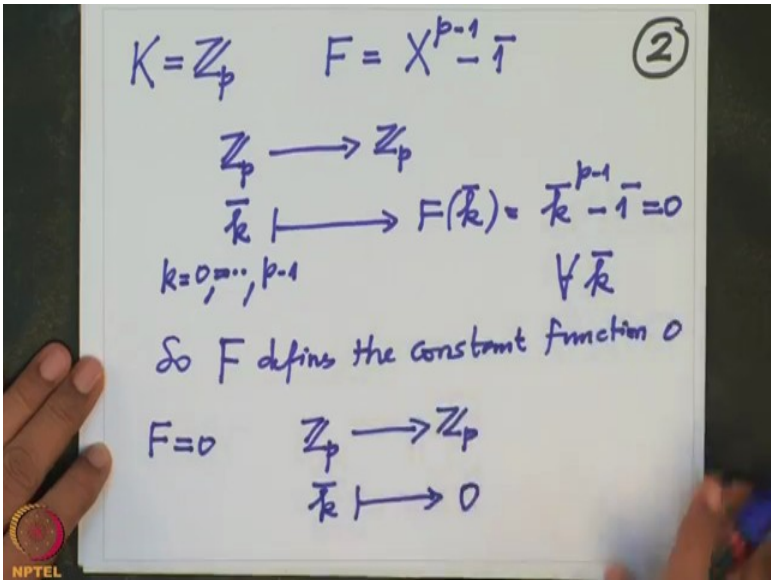
$$F : K \longrightarrow K$$
$$t \longmapsto F(t) = a_0 + a_1 t + \cdots + a_n t^n$$

polynomial function defined by ~~the~~ a polynomial F

Now I am going to take up the problem. So again we have K to be a base field and we have a polynomial F so this is this polynomial has the coefficients, so $a_0 + a_1 X + ... + a_n X^n$, a_n is non-zero, so if F is let us assume F is non-zero polynomial, F is 0 then we do not have to study anything, this a_n is called the leading coefficient of F and n is called the degree of F and we are always concern with zeros of the polynomial F somewhere may not be in K, may be in a bigger field and we have to find whether such a big field exist or not, all these questions are still hazy, we just began to study polynomials over a field, okay.

So this F also you can think as a function, F is a function, think of it is a function from K to K, (now what is how do you) so if I have a t an element in K then this will you want again an element in K so that is F of t, remember F of t is an element in K again because t is in K, this F of t is nothing but $a_0 + a_1 t + \ldots + a_n t^n$. So such a function this is called a polynomial function defined by defined by the polynomial F actually strictly speaking I should not use the word their defined by a polynomial F you will say in a minute.

(Refer Slide Time: 3:48)



$K = \mathbb{Z}_p \qquad F = X^{p-1} - \bar{1}$ 2

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$$

$$\bar{k} \longmapsto F(\bar{k}) = \bar{k}^{p-1} - \bar{1} = 0$$

$k = 0, \ldots, p-1 \qquad \forall \bar{k}$

So F defines the constant function 0

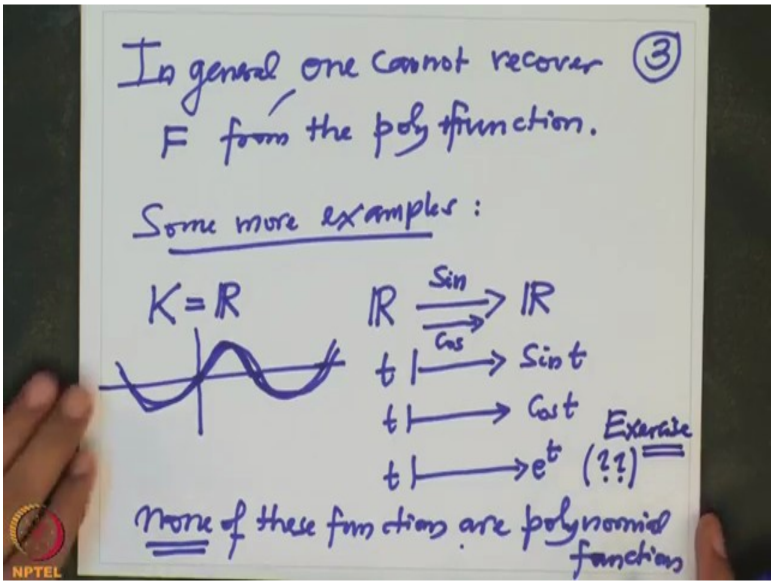
$$F = 0 \qquad \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$$

$$\bar{k} \longmapsto 0$$

Because two different polynomials can define the same function for example so for example let us take now K equal to $\mathbb{Z}_p$ and F equal to $X^{p-1} - \bar{1}$ the earlier polynomial then what is that function defined by F on $\mathbb{Z}_p$ to $\mathbb{Z}_p$. So any element here will look like $\bar{k}$, where (k is in between 0) and k is equal to 0 to p-1, so where does it go? It goes to F of $\bar{k}$, but F of $\bar{k}$ is $\overline{k^{p-1}} - \bar{1}$ but just above we saw that this is nothing but 0 for every $\bar{k}$. So that means this function the polynomial function defined by F is actually 0 function constant function 0.

So F defines the 0 function the constant function 0. So if I take F equal to 0 polynomial, then what is the function on $\mathbb{Z}_p$? That any $\bar{k}$ goes to take the polynomial and evaluate this at $\bar{k}$, but 0 is a polynomial and when you evaluate $\bar{k}$ there is no X there so therefore it goes to 0, so this is also the constant function 0. So this F and this F=0 will define the same function but they are different polynomials, so you cannot recover a polynomial from a functioning general.

(Refer Slide Time: 6:02)



In general, one cannot recover ③
F from the poly function.

Some more examples :

$K = \mathbb{R}$ $\qquad$ $\mathbb{R} \overset{\sin}{\underset{\cos}{\rightrightarrows}} \mathbb{R}$

$t \longmapsto \sin t$

$t \longmapsto \cos t$

$t \longmapsto e^t$ (??) Exercise

None of these functions are polynomial functions

So let me note this so this example shows that in general, one cannot recover F from (the function) the polynomial function. So also it is harder to see which functions are polynomial functions, when I say polynomial functions they are functions defined by polynomials and these polynomials are not unique therefore the coefficients are not uniquely determined (and so I want) therefore it needs to study some more examples.

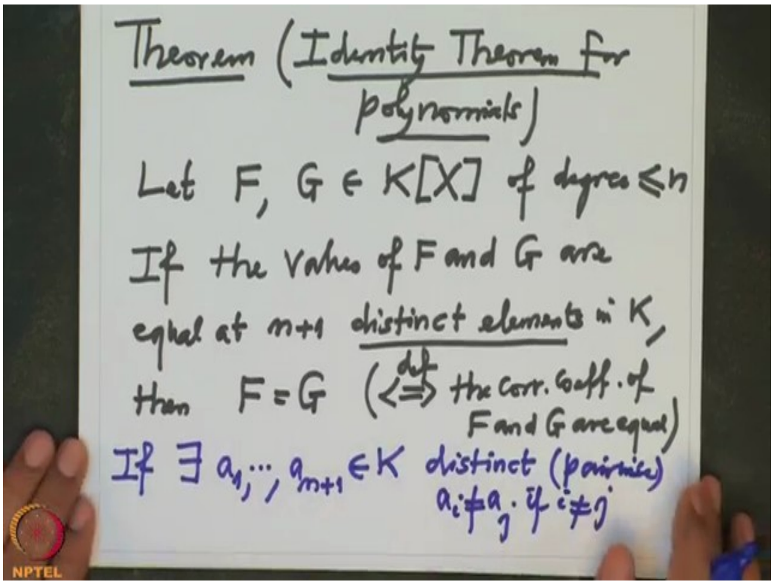
So some more examples, this time we do not take so let us take the classical example, so now I will take the field to be real numbers and let us take the example $\mathbb{R}$ to $\mathbb{R}$ function, t going to Sin t, this is a Sin function or you can take Cos or another function is Cos t, t goes to Cos t or another function is t goes to e^t , this is exponential function, these are trigonometric functions, none of these functions are polynomial functions none of these functions are polynomial functions, why? (none)

Simply because we have seen above that given a polynomial it can have only finitely many zeros with the (same field) same base field we have checked that if you are given a polynomial with coefficients in a field K then these polynomial can have only finitely many zeros in K or in any other field bigger field also because this number is bounded by the degree of that polynomial unless it is a 0 function everybody will be 0 that is the only case but your polynomial is non-zero then it can have only finitely many zeros, but these functions you know what is the graph of Sin X?

So if you try to draw a graph Sin 0 is 0 at $\frac{\pi}{2}$ it is so the graph will look like this, so every multiple of 2π it will keep hitting the X axis, right. So all these points are zeros of the Sin function and they are countably many in fact countably infinite. Similarly for Cos and for e^t , e^t there is no 0 actually so you still have to find a different argument for e power t that it cannot be polynomial function, I suggest that you think about it why does e power t is not a polynomial function.

So let me just put this as an exercise that the exponential function is not defined by a polynomial function, okay. So you see we are trying to understand the polynomials by the zeros etc etc.

(Refer Slide Time: 10:22)

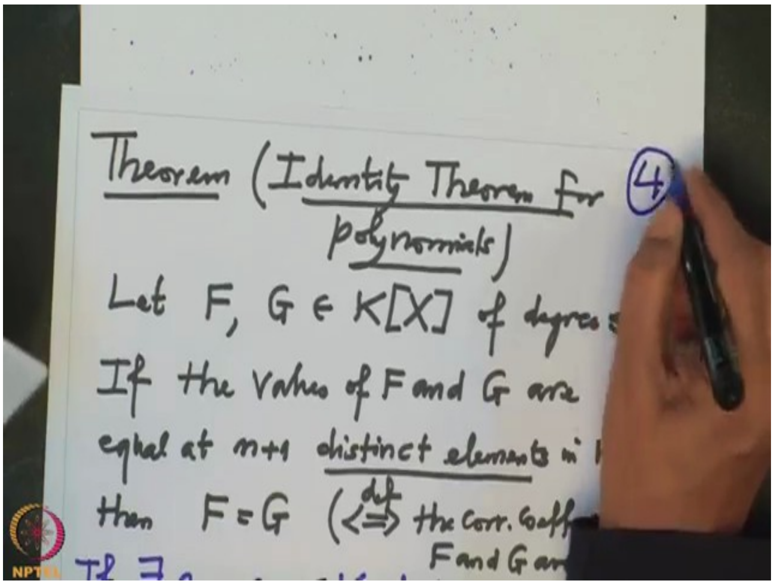


Theorem (Identity Theorem for polynomials)

Let $F, G \in K[X]$ of degree $\leq n$

If the values of F and G are equal at $n+1$ distinct elements in K, then $F = G$ ($\overset{\text{def}}{\Longleftrightarrow}$ the corr. coeff. of F and G are equal)

If $\exists\, a_1, \cdots, a_{n+1} \in K$ distinct (pairwise) $a_i \neq a_j$ if $i \neq j$



Theorem (Identity Theorem for polynomials) ④

Let F, G ∈ K[X] of degree

If the values of F and G are equal at n+1 distinct elements in

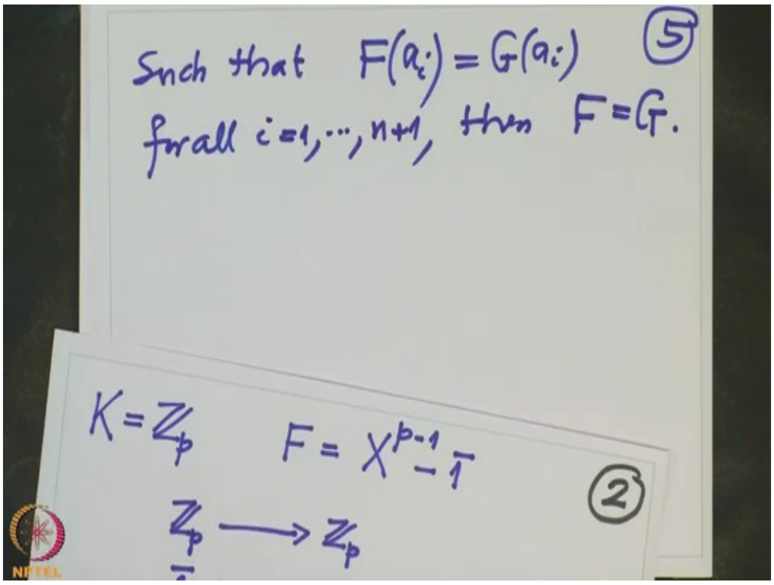
then $F = G$ ($\overset{\text{def}}{\Longleftrightarrow}$ the corr. coeff F and G ar

So I want to put therefore I want to prove a theorem which is very important theorem which one proves I do not know which subject you prove this but it should be proved in algebra or wherever. So this theorem actually it is called identity theorem for polynomials, so what does it say? It says that if I have two polynomials. So let F and G be two polynomials with coefficient in the field K of degree less equal to n both are of degree less equal to n.

Suppose if the values of F and G I will write into the words and then we will convert into notation, notation actually is always better but sometimes it is good to write in the words also. If the values of F and G are equal at $n+1$ distinct elements in K, then F must be equal to G and F must be equal to G, and F equal to G means what? That is by definition the corresponding coefficients are equal, so the corresponding coefficients of F and G are equal, what do I mean by corresponding coefficient? That means the coefficient of X^i here and coefficient of X^i, here if it is a i, that is also a i here, so that is what we need to prove.

Now do you write in terms of the notation? If the values of F and G are equal at $n+1$ distinct, distinct is also very important point. So now I am going to write this into the notation, so if will variable to prove soon, if there exist a 1 to a $n+1$ in the field K distinct they are distinct no two of them are equal, so better to write also distinct see this is also called pair wise distinct that means if you take a i and a j they should not be equal if i not equal to j.

(Refer Slide Time: 13:58)

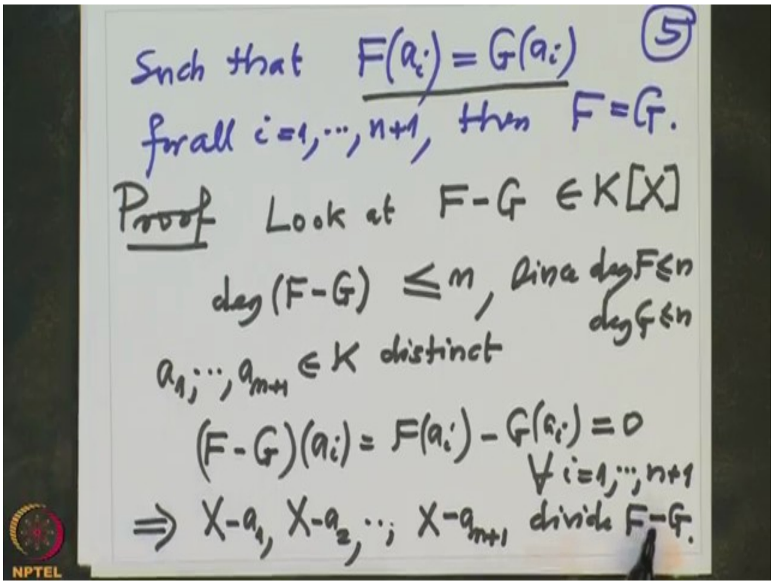


Such that $F(a_i) = G(a_i)$ 5

forall $i=1,\dots,n+1$, then $F=G$.

$K=\mathbb{Z}_p$ $F = X^{p-1}-1$ 2

$\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$



Such that $\underline{F(a_i) = G(a_i)}$ 5

forall $i=1,\dots,n+1$, then $F=G$.

Proof Look at $F-G \in K[X]$

$\deg(F-G) \leq n$, since $\deg F \leq n$, $\deg G \leq n$

$a_1,\dots,a_{n+1} \in K$ distinct

$(F-G)(a_i) = F(a_i) - G(a_i) = 0$ $\forall i=1,\dots,n+1$

$\Rightarrow X-a_1, X-a_2, \dots, X-a_{n+1}$ divide $F-G$.

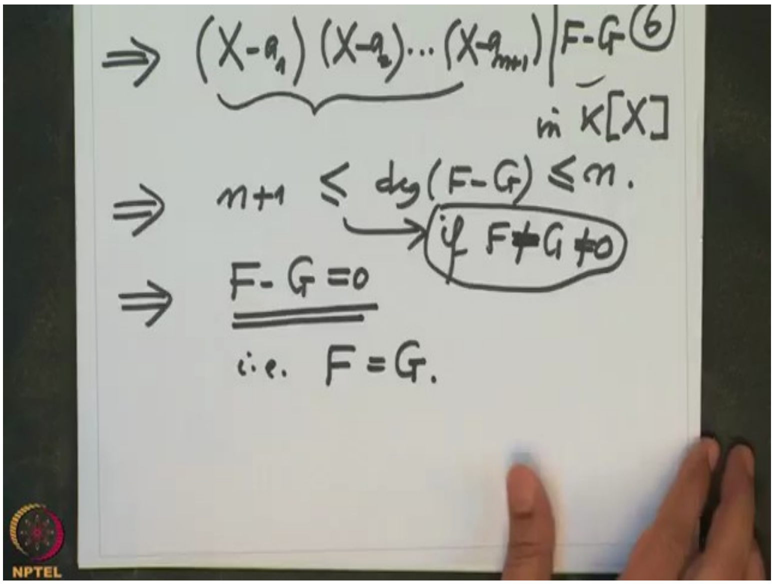
If there exist n distinct points in K elements in K such that there values of F and G are equal, F of a i equal to G of a i for all i from 1 to $n+1$, then F equal to G. So if you want to test F and G are equal then you find $n+1$ distinct points so their values are equal, okay let us proof this. So remember in the early example I just want to show you this example see this polynomial and the 0 polynomial the polynomial functions are equal but here the degree is $p-1$ and they are all together only $p-1$ elements in the field $\mathbb{Z}_p^x$, so therefore we cannot apply this theorem that is why F and that 0 polynomials are equal in that example, okay.

So let us proof this, proof so remember I want to proof F equal to G, okay. So how do we proof? Let us look at the difference, look at F minus G, F is a polynomial, G is a polynomial and we know we can add polynomial, subtract polynomial, multiply polynomials. So look at this, this is a new polynomial with coefficients in K, what is the degree of F minus G? Degree of F minus G cannot be more than n, because F has degree less equal to n, G has degree less equal to n, may be when the top degree term might also get cancelled in any case the degree of the difference will be less equal to n because since both degree F less equal to n and degree G is also less equal to n, so degree is less equal to n.

(And then) but I know that this there are a_1 to a_{n+1} distinct, this is given distinct such that F of a i equal to G of a i this is given to us, but then F minus G at any a i this is equal to F of a i minus G of a i but this is 0 for all i from 1 to $n+1$ that means this a_i is 0 of this F minus G and we have seen yesterday last lecture that if somebody is 0 of the polynomial then the linear factor should divide that polynomial F minus G.

So then all this $(X-a_1)(X-a_2)...(X-a_{n+1})$ all of them they divide F minus G, but they are all different linear factors you see none of them are equal because the a i's are different. So therefore all these guys are different prime elements in the polynomial ring, they are prime elements in the polynomial ring and they are different and each one of them divide this polynomial therefore their product will also divide (so 6).

(Refer Slide Time: 17:58)



$\Rightarrow \underbrace{(X-a_1)(X-a_2)\cdots(X-a_{n+1})} \mid F-G$ (6)

in K[X]

$\Rightarrow n+1 \leq \deg(F-G) \leq n.$ $\rightarrow$ $\boxed{\text{if } F \neq G \neq 0}$

$\Rightarrow \underline{\underline{F-G=0}}$

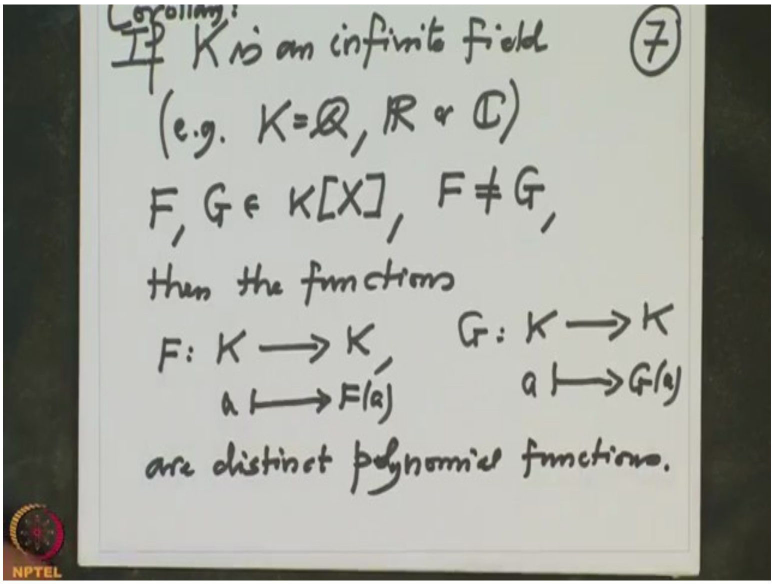
i.e. $F=G.$

So then the product $(X-a_1)(X-a_2)...(X-a_{n+1})$ divide F minus G, but if this polynomial and divide where in K[X], if this polynomial divide the polynomial F minus G then the degree of F minus G should be atleast this is a factor of F minus G so that should mean that $n+1$ which is the degree of this side should be less equal to degree of F minus G, but degree of F minus G is less equal to n by our assumption, so this cannot happen.

So the only chance is this F minus G is 0 polynomial because if it is a non-zero polynomial then only we know, remember that theorem has the theorem we proved in the morning that has an assumption that if you have a non-zero polynomial then it can have maximum degree number of zeros in the base field K or (why) every in every extension also the polynomial cannot have more zeros than the degree of that polynomial if it is non-zero.

So the only possibility is F minus G is a 0 polynomial, so this is if (F minus G is 0) F minus G is non-zero then only this inequality holds, okay. So that is the contradiction therefore only possibility F minus G is 0 that is F equal to G that is what we wanted to know. So it is very simple we are deducing this as a consequence from the what we proved it.

(Refer Slide Time: 20:02)



Corollary: (7)

If K is an infinite field

(e.g. $K = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$)

$F, G \in K[X]$, $F \neq G$,

then the functions

$F: K \longrightarrow K$, $G: K \longrightarrow K$

$a \longmapsto F(a)$ $\quad$ $a \longmapsto G(a)$

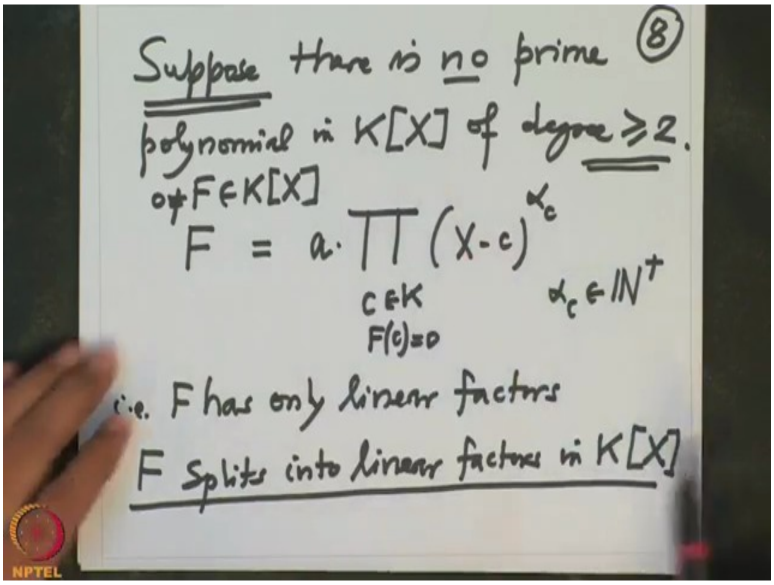
are distinct polynomial functions.

Okay, let us continue. So another consequence, now suppose for a moment our field was infinite. So if K is an infinite field that means K as a set is infinite, so for example K equal to $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$, so this is I am writing this should be corollary to the earlier statement and F and G are two polynomials with coefficients in K and suppose F is not equal to G, then the functions I will use the same letter for denoting the function which is from K to K and G is also function from K to K, this is a going to F of a and this is a going to G of a are distinct polynomial functions.

Because if they are equal functions that means they will agree at infinitely many points, they agree at every point in K their equal function means they agree at every point in K, but K has infinitely many points. So therefore they agree at more than definitely degree F and degree G are finite degree F and degree G both are bounded by some natural number, we know it. So by earlier theorem it will tell you F equal to G but that is not possible, so this is because K is infinite.

So over a field over a infinite field a polynomial function you can identify that polynomial functions are polynomials, there is no ambiguity in that but over a finite field one cannot do this, okay.

(Refer Slide Time: 22:48)



Suppose there is no prime polynomial in $K[X]$ of degree ≥ 2. 8

$0 \neq F \in K[X]$

$$F = a \cdot \prod_{\substack{c \in K \\ F(c)=0}} (X-c)^{\alpha_c} \qquad \alpha_c \in \mathbb{N}^+$$

i.e. F has only linear factors

F splits into linear factors in $K[X]$

So now I (am) want to analyse. So next topic I will introduce now it will come on its own after few minutes. So suppose I have a polynomial suppose there is no prime polynomial in K[X] of degree bigger equal to 2, suppose this is a big assumption prime once again let me say the prime polynomial means it is a polynomial monic polynomial and it has no proper factor when I say proper factor means the only factor is either itself or it is a unit multiple of that prime that polynomial, so that is the constant multiple non-zero constant multiple of that polynomial, so these are called improper factors.

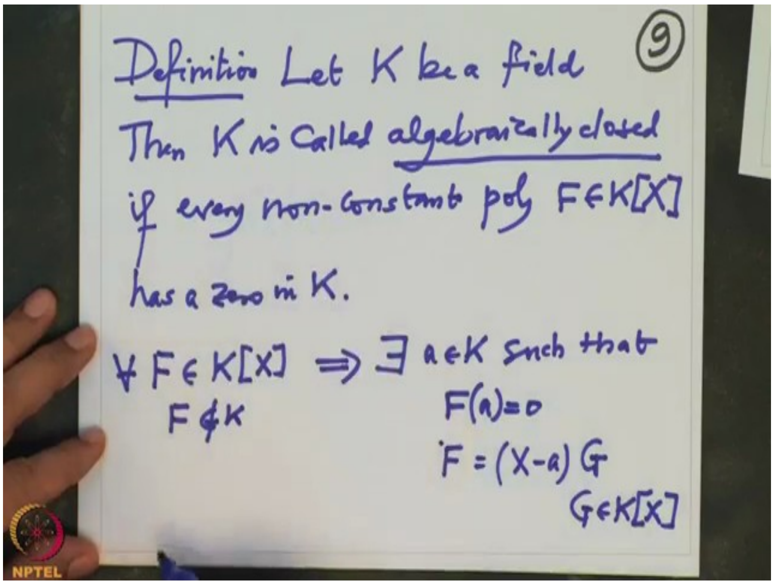
So like for example in case of integers suppose I take 6, (2 is a factor) 2 is a proper factor because 6 is 2 times 3, whereas minus 2 has which are the factors 1, minus 1 I am talking in Z now (1 minus 1, 2 minus 1) 1 minus 1, 2 minus 2, but all these are called improper factors because they are either units or they are unit multiples of the given integer. So in general a prime polynomial over a field means it is a monic polynomial first and the only factors are unit multiples of the given polynomial they are called prime polynomials.

Okay, so if it has no prime factor of degree bigger equal to 2, no prime factor. So that means what? What will that polynomial will look like? That means the polynomial F should look arbitrary polynomial, there is no prime polynomial of degree bigger equal to 2 in K[X], so given any F in K[X] non-zero F, how can you write? We just wrote that it has some linear factors and it has a prime factor of degree bigger equal to 2, but there is no prime polynomial of degree bigger equal to 2 in K[X] at all.

So this F will look like the leading coefficient of F times product X minus c power alpha c, this product is varying over c in K actually such that F of c is 0 so they are finitely many at most degree F times and this alpha c's are the non-zero natural numbers so this is how F will look like that means F has only linear factors. So that is F has only linear factors. In this case I will also write F splits into linear factors in K[X] this is what I will write.

So what did we observed that if there is no prime polynomial in K[X] of degree bigger equal to 2, then every non-zero polynomial in K[X] actually splits into linear factors and then we can count the zeros and all zeros are in K range, so this is very very special property of the field. So let me say you first atleast one field that we will proof that that has this property and we will proof also that any given any field we can always enlarge to such a field, where the bigger field has this property that there are no prime polynomials of degree bigger equal to 2 in a bigger field.

(Refer Slide Time: 27:24)



9

Definition Let K be a field

Then K is called algebraically closed if every non-constant poly $F \in K[X]$ has a zero in K.

$\forall\, F \in K[X] \Rightarrow \exists\, a \in K$ such that

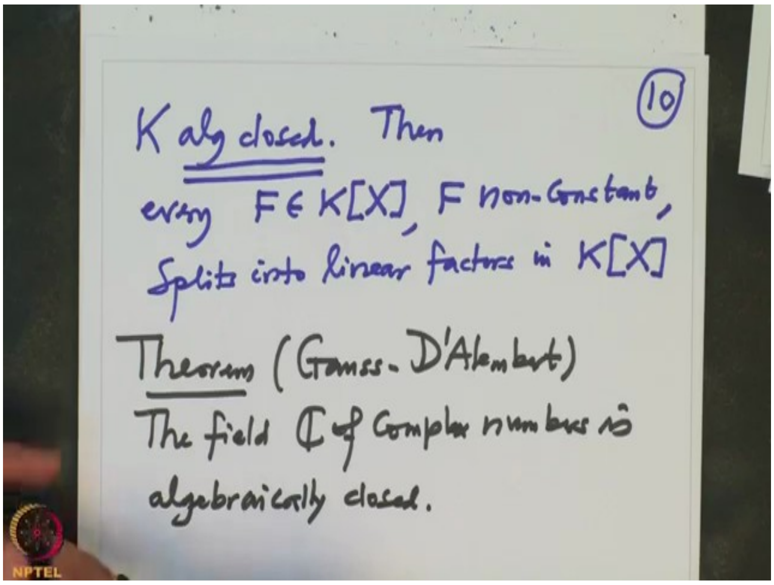
$F \notin K$ $\qquad F(a)=0$

$F = (X-a)\,G$

$G \in K[X]$

So for that convenient to make a following definition so definition let K be a field then we will call then K is called algebraically closed if every non-constant polynomial F in K[X] has a zero in K such a field is called algebraically closed. So what does this notation means? Given F in K[X], F non-constant means F is not in K, then there exist a in K such that F of a is 0, such as for every F we have this then we call that field to be algebraically closed and once we have this then we know that this X minus a is a factor of F times some other polynomial G, then this G is a new polynomial in K[X], if G is constant we stop here, if G is not constant again I apply the same that means G will have a linear factor again, so that will come out of this and collect the powers together and so on.

(Refer Slide Time: 29:32)



10

K alg closed. Then every $F \in K[X]$, F non-Constant, Splits into linear factors in $K[X]$

Theorem (Gauss-D'Alembert)
The field $\mathbb{C}$ of Complex numbers is algebraically closed.

So if K is algebraically closed I will just note it here, so K algebraically closed then every non-constant F every polynomial F with coefficients in K, F non-constant splits into linear factors in K[X]. So therefore our study if your field is algebraically closed our study is much easier. So I will just end this discussion by stating a theorem and which we will prove it. So first of all examples of such fields, so this is the theorem which has a big history and we will prove it sometime.

So this theorem this is called Gauss D'Alembert, which says the field $\mathbb{C}$ of complex numbers is algebraically closed, this is very very important theorem, remember former days like Vieta and even later Galois, Abel and so on they did not know the proof of this, but they somehow where convinced in their minds including Lagrange that the $\mathbb{C}$ has this property that every polynomial with coefficients in $\mathbb{C}$ factors into linear factors in $\mathbb{C}[X]$ and this what was implicitly used in their discussion about polynomials, zeros and further study Galva groups etc, etc this was used and this we will proof it sometime in the coming future.

So I would like to stop here and just remind you that what we have done is we have begun our study of polynomials over a field K and we want to study the zeros for example how many zeros the polynomial has we have seen that the number of zeros is always bounded by the degree, this is what we proved, also we have also mentioned that the polynomial functions polynomials we can also think about polynomial functions.

But in this thinking if your field is not infinite you may still lose some information that two polynomials might give the same polynomial functions, but over infinite field two distinct polynomials will define distinct polynomial functions and so on. Now next time also I will give some little more remarks about this theorem of Gauss D'Alembert and then we will continue our study of polynomials in general and then we will also now soon start studying field extensions, okay so I stop here, thank you very much.