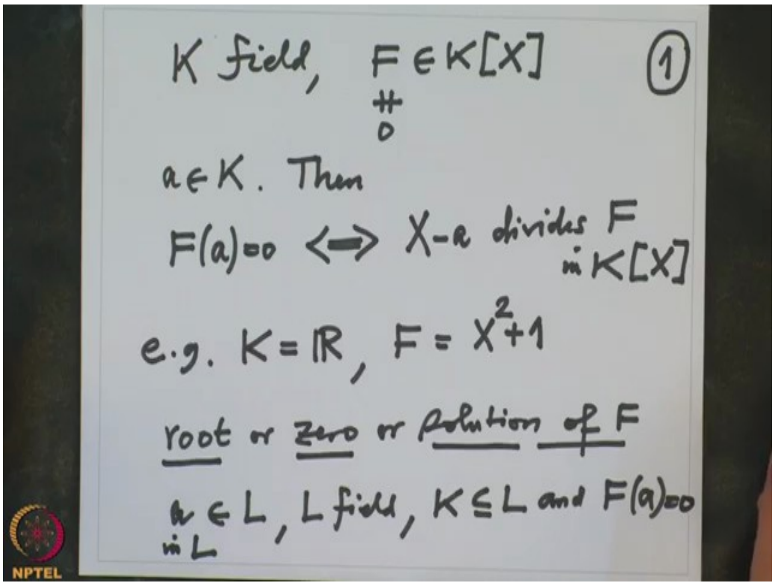
Galois Theory
Professor Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 7
Zeroes of polynomials

In the last lecture we started our study of polynomials over a field and what we saw was we use division with remainder to decide whether a given element of the field is a zero of that polynomial or not.

(Refer Slide Time: 0:56)



K field, $\underset{\neq 0}{F} \in K[X]$ ①

$a \in K$. Then

$F(a) = 0 \iff X - a$ divides F in $K[X]$

e.g. $K = \mathbb{R}$, $F = X^2 + 1$

root or zero or solution of F

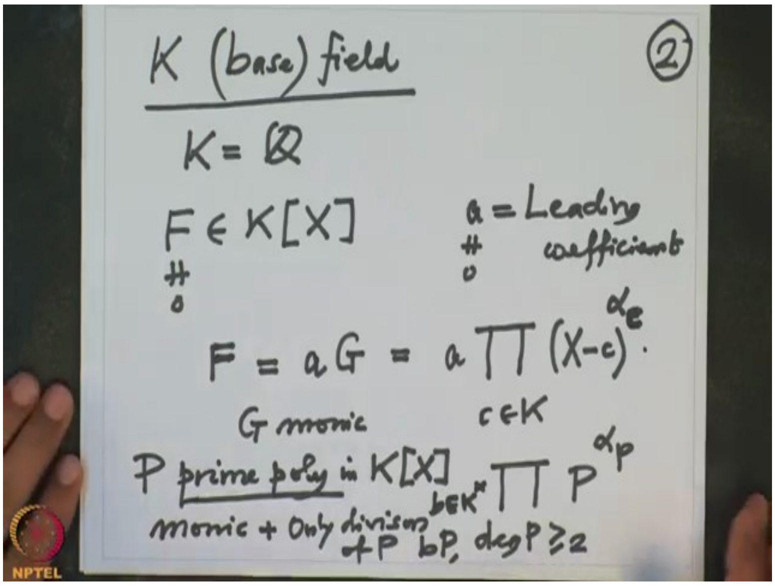
$a \in L$, L field, $K \subseteq L$ and $F(a) = 0$ in L

So let me recall briefly what we did, so K is a (field) arbitrary field and F is a polynomial with coefficients in K and let us assume F is non-zero, then we have noted as a consequence of division with remainder that if I have an element a in K then F of a is zero, if and only if the linear polynomial X minus a divides F in the polynomial ring K[X]. So we are interested in finding out remember our main aim is in this course is to find roots or zeros of the polynomial and this information is useful only when the roots or solutions or zeros they are in the field K, but it may happen that your polynomial may not have any zero in K.

For example, if I take K equal to $\mathbb{R}$ and F equal to X^2+1 then this polynomial F does not have any zero or solution or root in the field $\mathbb{R}$. So remember henceforth, I will use the words like root or zero or a solution is are of same meaning of F means an element a somewhere (may not be in F) may not be in K but may be in a bigger field than K in some L, where L is a field which contain K and F of a is 0, such a thing is called root or zero or a solution of F and when should specify in L, where L is a given bigger field.

And in formal days the people, researchers they were working in a special field rational numbers and definitely they knew that inside the complex numbers all polynomials have zeros, this was precisely so called fundament theorem of algebra which we will also prove it, but I am gathering the information or gathering the vocabulary and then we will start proving things so that we will have less and less confusion.

(Refer Slide Time: 4:20)



K (base) field ②

$K = \mathbb{Q}$

$F \in K[X]$, $F \neq 0$ $\quad$ a = Leading coefficient, $a \neq 0$

$$F = aG = a \prod_{c \in K} (X-c)^{\alpha_c} \cdot$$

G monic

P prime poly in K[X] $\quad \prod_{b \in K^{\times}} P^{\alpha_P}$

monic + Only divisors of P bP, $\deg P \geq 2$

Okay, so what did we decide in the last lecture? An element in a and that given field K, I will keep calling a base field. So this K the field we start always that is called a base field. In formal days that was usually K = $\mathbb{Q}$ field of rational numbers because that is the smallest field that we got it from natural numbers, from natural numbers we got integers and from integers we got rational numbers that is the field and that is the smallest field. Nowadays because of the applications one also considers finite field, so in general now I will keep arbitrary K is arbitrary base field and this $\mathbb{Q}$ will be the classical case and arbitrary other fields will also be very important for the applications.

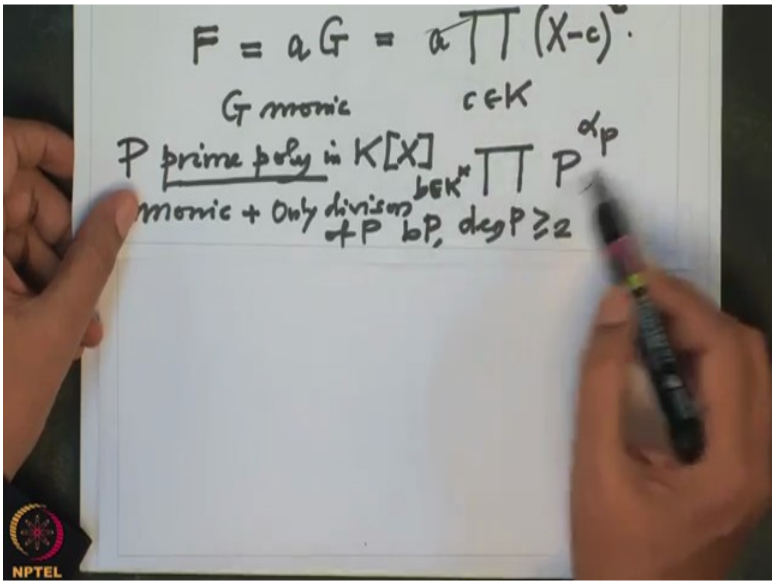
So we have proved last time in the last lecture we have proved that every polynomial F in K[X] has a factorization like this F is non-zero and this F definitely I can factor it as, first of all this F will have a leading coefficient so I want to call that a to be the leading coefficient of F. So if I take out because I am in a field and this a is non-zero because F is a non-zero polynomial this leading coefficient is non-zero. So I can always take out a common factor that I can do it that is among to saying that you are multiplying by the inverse.

So that means this F, I can definitely write it as a times some G, where the G is another polynomial. Now G is monic this I can always do it because a is non-zero, just multiply F by a inverse and you get G, so G is monic and then this one we try to see whether some elements of K is 0 of G or not and that will be then the linear factor of G. So this G definitely I can write it as a times product this product is varying over $c \in K$ such that $X - c$ and may be some this $X - c$ may be repeated factor so that the multiplicities are alpha c times now the other factors.

So that will be unfortunately I cannot write here so I will write it down there times product. Now this product will run over degree P bigger equal to 2 and P^{α_P} , where only finitely many factors occur here this product is finitely many that is only finitely many linear factors are there these are the multiplicities. Similarly, these P are prime polynomials in K[X], remember prime polynomials in K[X] means this is we defined last time.

So it means two things, first of all P is monic and the only divisors of P in K[X] are either only divisors of P are of the form some bP, where this b is actually a unit in K that means it is in K^{x} that is the only divisors in K[X]. So these are also some books you will see these are also called irreducible polynomials but when a irreducible polynomial is monic I call it a prime polynomial because they are analogue of the prime numbers. So prime numbers are the one which do not have divisors other than 1 and itself in natural numbers, so the same philosophy so therefore we have written.

(Refer Slide Time: 9:14)

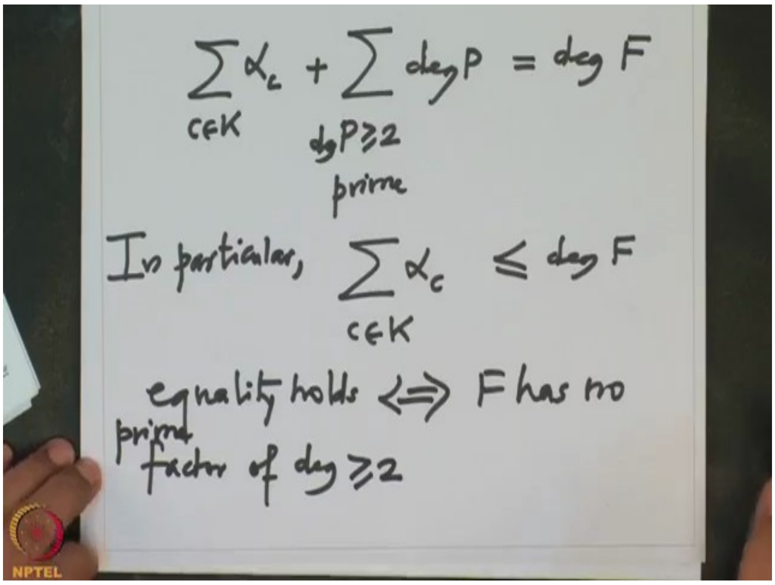


$$F = aG = a\prod_{c\in K}(X-c)\cdot\prod P^{\alpha_P}$$

G monic

P prime poly in K[X]

monic + only divisors of P b, bP, $b\in K^{\times}$ deg P ≥ 2



$$\sum_{c\in K}\alpha_c + \sum_{\substack{\deg P\geq 2\\ \text{prime}}}\deg P = \deg F$$

In particular, $\sum_{c\in K}\alpha_c \leq \deg F$

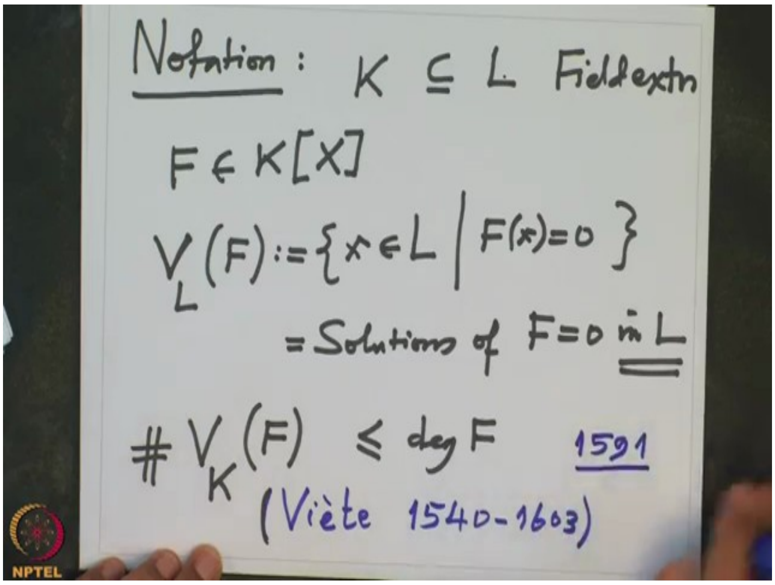
equality holds $\Longleftrightarrow$ F has no prime factor of deg ≥ 2

Now immediately from this because we are over a field when you compare the degrees on both sides we will get the formula that if I take all these alphas. So that is summation α_c, c varies in that K and only finitely when you see this sum is only finitely many plus the degree of P, where P varies in that product, P degree P bigger equal to 2 and prime polynomial this degree is on the degree of the right side.

See this degree is I am comparing the degrees. So this is does not fit in one line this degree here is the degree of this the degree of this is for each factor it is this, so it is a sum. Similarly here it is sum alpha P and the other side is degree F so this is equal to degree F, this is the degree for me now because we are over a field so the sum of the degree is of the factors in the product equal to degree of the product that is what we are used for this.

So in particular what did you inform, in particular we have proved that the summation $\alpha_c, c \in K$ this is less equal to degree F and when can equality hold here? Equality will hold here that means when F has no factor of degree 2 or more. So equality holds if and only if F has no factor of degree bigger equal to 2, no prime factor I should write so that means this part is absent actually this was for a long time so in particular.

(Refer Slide Time: 11:34)



Notation: $K \subseteq L$ Fieldextn

$F \in K[X]$

$V_L(F) := \{x \in L \mid F(x) = 0\}$

= Solutions of $F = 0$ in L

$\# V_K(F) \leq \deg F$ 1591

(Viète 1540-1603)

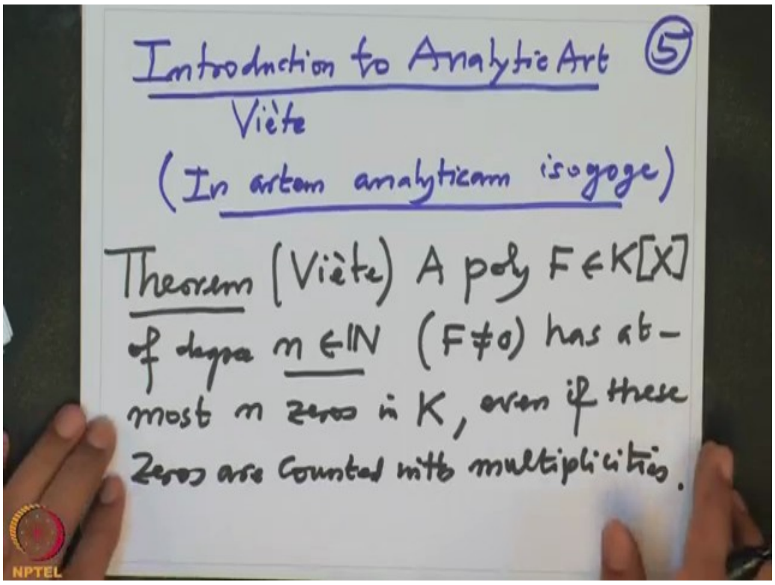
So now let me before I write down further in particular case, let me introduce a notation here now. So this we will use it throughout the course, this is very very important. So suppose I have a field K and I have a bigger field L, so this one means that the operations are same that means the addition and multiplication in K is induced from the addition and multiplication in L in particular the 0 element in K, 0 element in L are same, 1 in K and 1 in L are same thing that is assumed. So such a thing I will call field extension, these are fields and one is contained in the other or this is K is a sub field of L or L is a bigger field than K.

Now and if you have a polynomial F given in with coefficients in K, then I will write here V suffix L of F, this means all elements (x in) small x in capital L here such that F of x is 0 that means small x, so this is also one can say this is the solutions of F equal to 0 in L, right (so) and this is what we want to study and whether our main problem is can you find given a polynomial F, can you find L so that all the solutions are in L and whether the solutions have close formulas in terms of the coefficients of F that means using addition, multiplication, subtraction, division and extracting this K root that is the problem of the Galois theory, this is Galois theory centres around studying this problem so this is.

And what we proved above is the cardinality of $V_K(F)$ is less equal to degree of F, this is what we studied this is what follows from that, in fact little bit more, what more? That each element in $V_K(F)$ we attach a multiplicity and not only the distinct points but if you count each point with the corresponding multiplicity then also the sum is less equal to degree, actually this was proved by I wanted to make that comment this was proved by Viete I will write here in the bracket this is very important observation this was for a long time it did not people did not know so this is Viete the French mathematician who lived between 1540 to 1603 and he has observed this around 1591.

Actually the notation about capital X to denote capital X the variable in a polynomial also this polynomial ring that notation is also due to Viete and in fact (it is) he has written a book, okay.

(Refer Slide Time: 15:30)



Introduction to Analytic Art 5

Viète

(In artem analyticam isogoge)

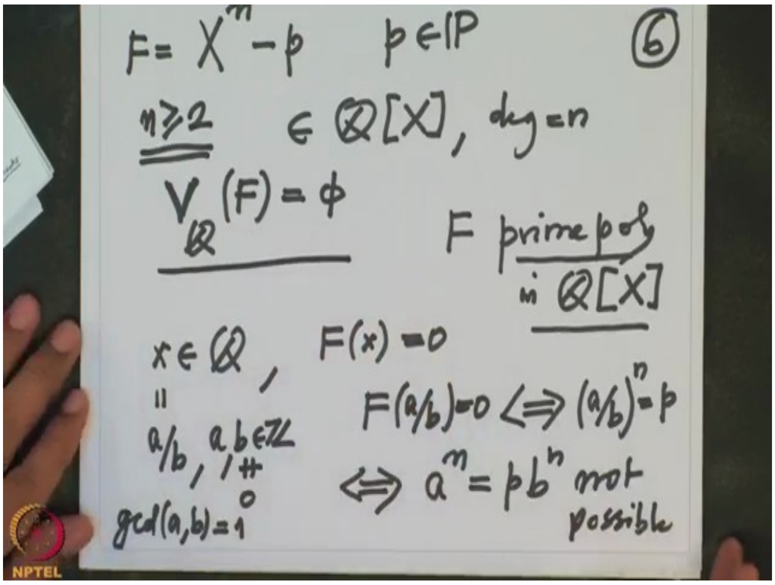
Theorem (Viète) A poly $F \in K[X]$ of degree $n \in \mathbb{N}$ $(F \neq 0)$ has at-most n zeros in K, even if these zeros are counted with multiplicities.

So the book I just mention it, it is interesting, it is called introduction to analytic art this is Viete, he also gave methods to solve degree 4 equations in a trigonometric way anyway. So this was see those days the language was not English, the language was Latin and in that this tittle I have translated in English, but in Latin it is in artem (analytic) analyticam isogoge this was what the tittle was, so there you will find this theorem.

So let me state now what we proved what this observation as a theorem so that we can refer. So this is theorem this is Viete a polynomial F with coefficients in a field K of degree n, where n is natural number remember this assumption means that F is non-zero because once this is a polynomial of degree n that means F cannot be 0, we have defined degree only for non-zero polynomials and degree can be 0 constant polynomial have precisely degree 0.

So a polynomial of degree n has atmost n zeros in K, even if these zeros are counted with multiplicities this is what we have proved here so that is summation of α_c is less equal to the degree F very important. So we know there cannot be more, (but this also says) this also shows not all can be in the base field or none can be also. So for example I gave example X square plus 1 that real numbers it has no zero, degree is 2 but it has no real zero.

(Refer Slide Time: 18:34)



$F = X^n - p \quad p \in \mathbb{P}$ ⑥

$\underline{\underline{n \geq 2}} \quad \in \mathbb{Q}[X], \ \deg = n$

$\underline{V_{\mathbb{Q}}(F) = \phi}$ $\quad$ F $\underline{\text{prime poly in } \mathbb{Q}[X]}$

$x \in \mathbb{Q}, \quad F(x) = 0$

$\| \quad\quad F(a/b) = 0 \iff (a/b)^n = p$

$a/b, \ a, b \in \mathbb{Z}, \ b \neq 0 \quad \iff a^n = p b^n$ not possible

$\gcd(a,b) = 1$

Similarly if I take polynomial $X^n - p$, where p is a prime number p is a prime number think of this is a polynomial in $\mathbb{Q}[X]$, the degree is n and it has no zero, this is F, F has V better to use this notation again and again so we will get $V_{\mathbb{Q}}(F)$ is empty say and our problem is to find all zero, that means you enlarge $\mathbb{Q}$ to $\mathbb{C}$ for example, $\mathbb{C}$ may be too big you may not need whole big $\mathbb{C}$.

So enlarge $\mathbb{Q}$ to big field so that all zeros of F are there and then say how do we write the formulas or is it possible to write formulas? So that is the problem, okay so this polynomial is actually this polynomial F is a prime polynomial F is prime polynomial in $\mathbb{Q}[X]$ this is not this is not immediately trivial but this we will prove it later, but right now we only want to say that there is no zero, so that is easier to prove if so let me just indicate this proof.

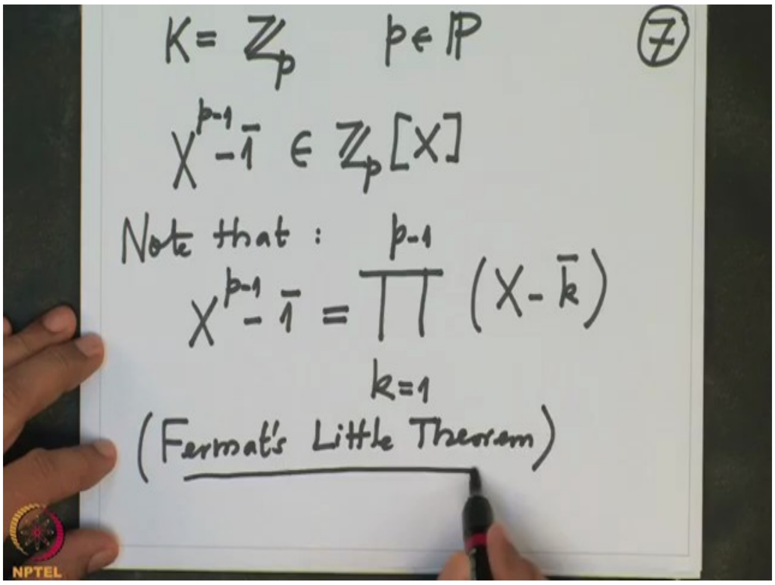
Suppose x is a rational number and suppose $F(x)=0$, I should get a contradiction because this is empty set. So x is a rational number, so x will be of the form $\frac{a}{b}$, where a, b are integers and b is non-zero so any rational number by definition like that and then I want to check that this cannot so I want to check that F of a, b cannot be 0.

So if F of a, b is 0 a by b is not 0 (not a, b) a by b is 0 that is equivalent to saying when I plug X equal to $\frac{a}{b}$ then it becomes 0, so $(\frac{a}{b})^n - p=0$, p is a prime number but that equation is equivalent to saying $a^n = p\,b^n$, okay to start with I could have written this fraction as the lowest fraction that means these integers a and b have gcd 1 that we can always do it because if they have a common factor up and down you can select and then this is usual trick what we have been learning in the school for so many years.

So gcd is 1, so that means a and b does not have any common factor in particular they do not even have common prime factor. So but you see this p divides the right hand side, so therefore p will divide a by a power n but p is a prime number, so if p divides a power n then p will divide a, but once p divides a, p power is the factor here and you cancel one of the factor and then the remaining n minus 1 so you need a condition n is atleast 2, so this is not possible, clear no?

Because if p divides a^n then p divides a, then this will divide the left hand side will be divisible by p^n but then you cancel one p, but p^{n-1} still divide the left hand side which is atleast 1, so p will divide b^n and therefore p will divide b and therefore gcd cannot be 1. So therefore what all together we have checked that we have checked that $V_{\mathbb{Q}}(F)$ is empty set, so there is no zero, so how do we find and where? So that problems we are doing that, okay.

(Refer Slide Time: 23:16)

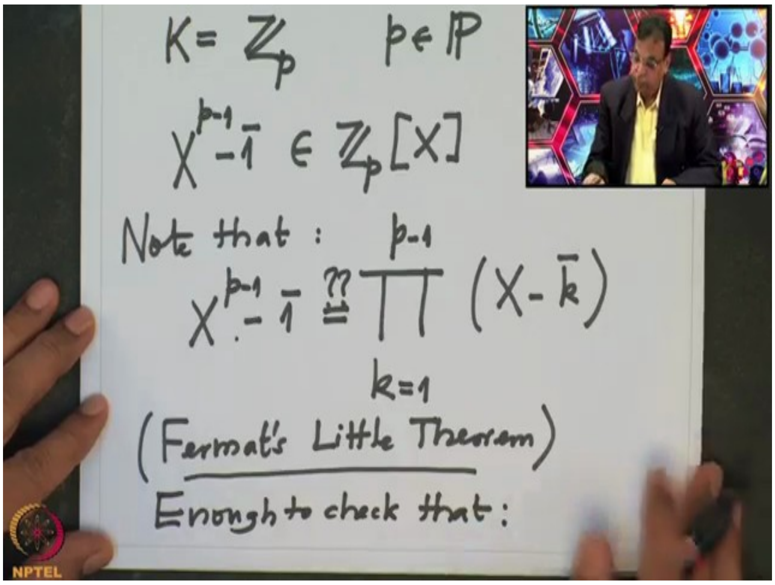


$K = \mathbb{Z}_p \quad p \in \mathbb{P}$ 7

$X^{p-1} - \bar{1} \in \mathbb{Z}_p[X]$

Note that: $X^{p-1} - \bar{1} = \prod_{k=1}^{p-1} (X - \bar{k})$

(Fermat's Little Theorem)



$K = \mathbb{Z}_p \quad p \in \mathbb{P}$

$X^{p-1} - \bar{1} \in \mathbb{Z}_p[X]$

Note that: $X^{p-1} - \bar{1} \overset{??}{=} \prod_{k=1}^{p-1} (X - \bar{k})$

(Fermat's Little Theorem)

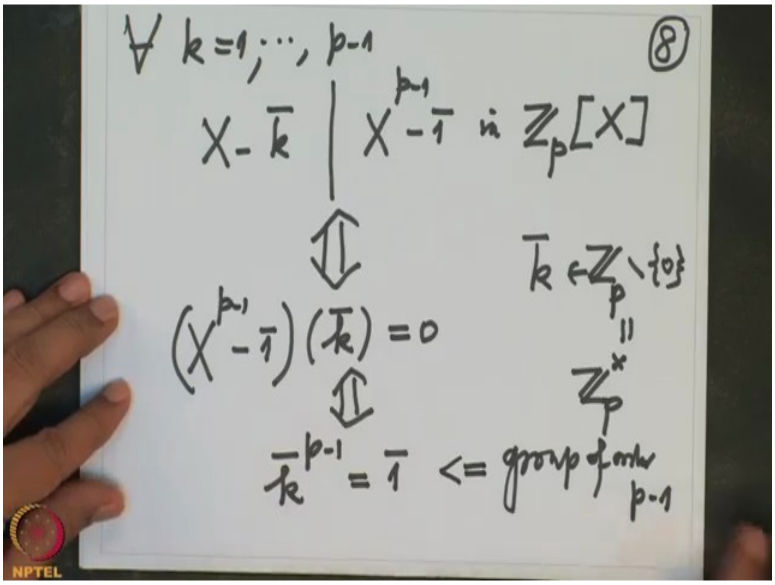
Enough to check that:

So now let me give one more application of that theorem of Vieta, so for example now I want to apply this to the polynomial I take first of all K to be $\mathbb{Z}_p$, p is a prime number and I take the field $\mathbb{Z}_p$ this is this field we have got it from integers by defining a congruence relation there and then taking the congruence classes and defining addition and multiplication there and it became a field this field.

And I am going to take the polynomial $X^{p-1}-1$, this is a polynomial with $\mathbb{Z}_p[X]$ this is a polynomial with coefficients in $\mathbb{Z}_p$. So one should really write this 1 as 1 bar, okay and then what do we want to apply what did we write? We want to find out first of all note that $X^{p-1}-1$ this (polynomial) this given polynomial is in fact the product of product is varying from k equal to 1 to p - 1, there cannot be more because this degree is p - 1 and X - k, I strictly speaking I should write k bar, this is I want to check this equality first.

So what do I have to check? I have to check that when I expand this side only two terms remain the degree term and the constant term, in between terms become 0 or I will have to check that this is I just want to say that this is precisely what is known as Fermat’s Little Theorem, what do I have to check that each one of them is a factor here, if I check that that is enough because each one is a factor here, therefore they are different factors the different prime polynomials and therefore they will divide all of them will divide this, therefore this product will divide this but on the other hand there cannot be anymore because this degree is p - 1, this is also p - 1 degree and both are monic. So once you proof that to check this enough to check to check that I will write on the next page.

(Refer Slide Time: 26:20)



8

$\forall\ k = 1, \cdots, p-1$

$X - \bar{k} \mid X^{p-1} - \bar{1}$ in $\mathbb{Z}_p[X]$

$\Updownarrow$ $\qquad \bar{k} \in \mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^{\times}$

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

$\Updownarrow$

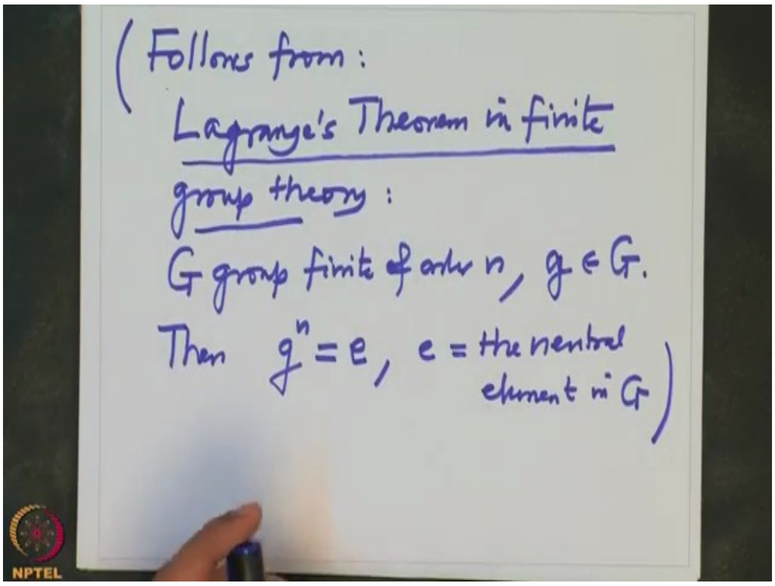
$\bar{k}^{p-1} = \bar{1} \Leftarrow$ group of order $p-1$

Enough to check that for each k from 1 to p - 1, $X-\bar{k}$ bar divides $X^{p-1}-1$ bar in this field in this polynomial ring, this is what I have to check. But just now we observed in the morning few minutes back that whenever you want to check somebody divide this it is enough to check this is enough to check that when I plug in $\bar{k}$ in this it should become 0.

So this is X power p minus 1 minus 1 bar this polynomial if I evaluate at $\bar{k}$ it should become 0 that means when I put X equal to $\bar{k}$ but that is equivalent to checking k bar power p minus 1 equal to 1 bar, but you see where is $\bar{k}$? $\bar{k}$ is an element in $\mathbb{Z}_p$ and $\bar{k}$ is not 0 and this is precisely what we have called it $\mathbb{Z}_p^x$ and $\mathbb{Z}_p$ is a field, therefore this is precisely the group of units and this is a group of then order group of order p - 1, so it is a finite group of what is p - 1 and this $\bar{k}$ is one element there.

So when I raise that element to the power of the order of the group you should get a trivial element in the group or identity element in the group, this group is with multiplication so the identity element in this group is precisely 1 bar. So therefore this follows this equation follows so this is also called what is called Lagrange's theorem it follows from Lagrange's theorem in group theory which also we will proof.

(Refer Slide Time: 28:34)



(Follows from:

<u>Lagrange's Theorem in finite group theory</u>:

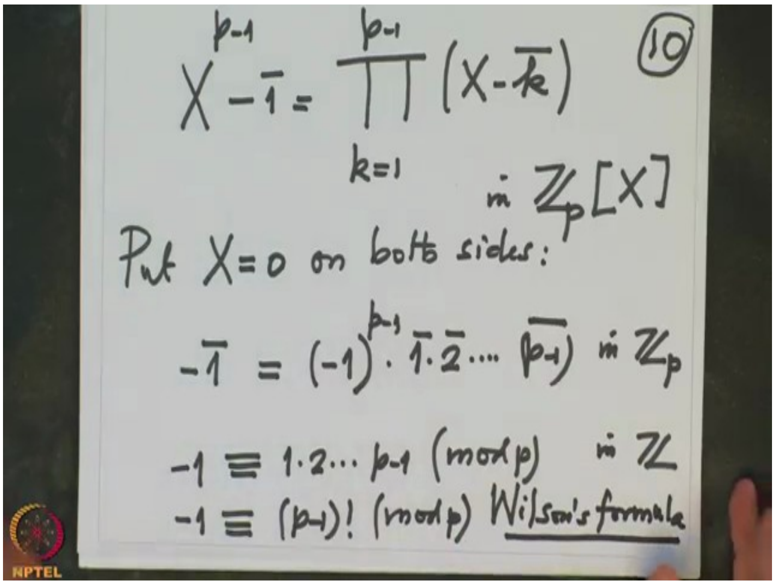
G group finite of order n, $g \in G$.

Then $g^n = e$, e = the neutral element in G)

So remember just remember we have used the fact that so I will write in the bracket this is this follows from Lagrange's theorem in finite group theory which says that if G is a group finite of order n and (a is) g is an element in G, then g power n is identity element e in g, where this e is the neutral element in G, this is also we will prove I will indicate when I prove more general than this, but right now we accept this.

That is what I mean by that is what I mean by when I said I will assume that the participants of this course are familiar with abstract algebra first level that means finite groups, also vector spaces, little bit of rings, little bit of fields and linear algebra, etc etc.

(Refer Slide Time: 30:22)



$X^{p-1} - \bar{1} = \prod_{k=1}^{p-1} (X - \bar{k})$ 10

in $\mathbb{Z}_p[X]$

Put $X = 0$ on both sides:

$-\bar{1} = (-1)^{p-1} \cdot \bar{1} \cdot \bar{2} \cdots \overline{p-1}$ in $\mathbb{Z}_p$

$-1 \equiv 1 \cdot 2 \cdots p-1 \pmod{p}$ in $\mathbb{Z}$

$-1 \equiv (p-1)! \pmod{p}$ Wilson's formula

So we have checked that we have checked that coming back here, what did we prove? We proved that we proved that we have proved such an equation $X^{p-1} - \bar{1} = \prod_{k=1}^{p-1} (X - \bar{k})$. So now that means what and this is in $\mathbb{Z}_p[X]$, so that means this polynomial factors actually into linear factors and we know also the zeros and we know they are precisely so in the base field they are actually all in base field so there is no need formula is clear.

So now I want to deduce one more fact from this equation now. In this equation I am going to put this is the equation, this side is polynomial, this side is polynomial so I can arbitrary put X equal to whatever values I like in this. So put X equal to 0 on both sides and what do we get? We get here minus 1 bar because X is 0 I am putting equal to X is 0 I am putting, so this will be minus sign how many times? p - 1 times and the product of this so what do we get?

Minus 1 I will take that out $(-1)^{p-1} \bar{1}\bar{2} \ldots \overline{p-1}$, right. But then this is equation in $\mathbb{Z}_p$, now I want to write the equation in $\mathbb{Z}_p[X]$. So there are two numbers they are equal in $\mathbb{Z}_p$ means they are modulo p they are equal that means so this minus 1 so I want to lift this equation to $\mathbb{Z}$. So minus 1 is congruent to and you see p is a prime number therefore p - 1 is even so therefore $(-1)^{p-1} 1$ and then instead of bars I have to write so 1 into 2 into upto p - 1 mod p that is the meaning of the above equation.

But this means -1 is congruent to (p – 1)! mod p this will remind you theorem which you might have proved in your college there this is called Wilson's formula, okay. So we will continue after the break our study of polynomials and the zeros, etc etc thank you.