Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 14
Examples

(Refer Slide Time 00:25)

So in the last couple of minutes we have seen the definition of algebraic elements over a field and

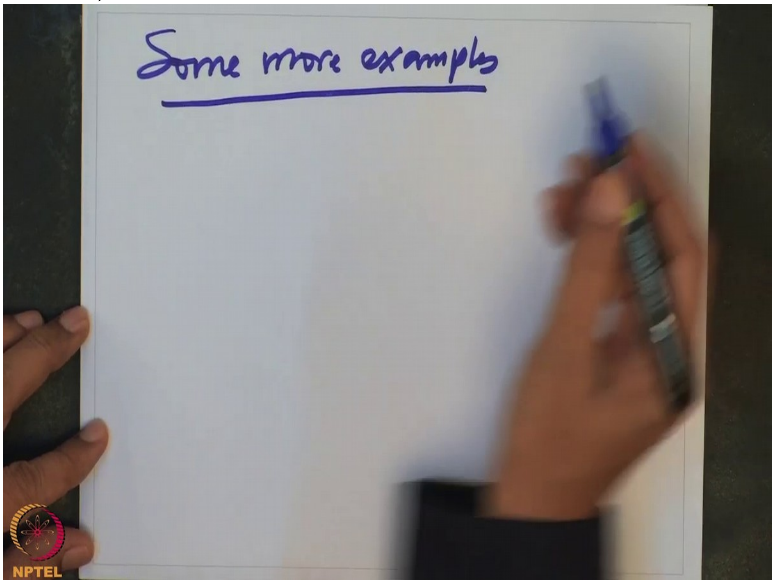
(Refer Slide Time 00:36)

remember that we did not only define algebraic elements in a field but in a general algebra, general K-algebra, we have defined the concept of algebraic elements.

And as a due course, we will see this is more generally, definition is also very important. Now before I go on to the characterization of algebraic elements that is how do you test economically some element in a given algebra is algebraic or not, to test this, we need some more concepts which I will develop on the way but before that I want to give examples of an element which are not algebraic.

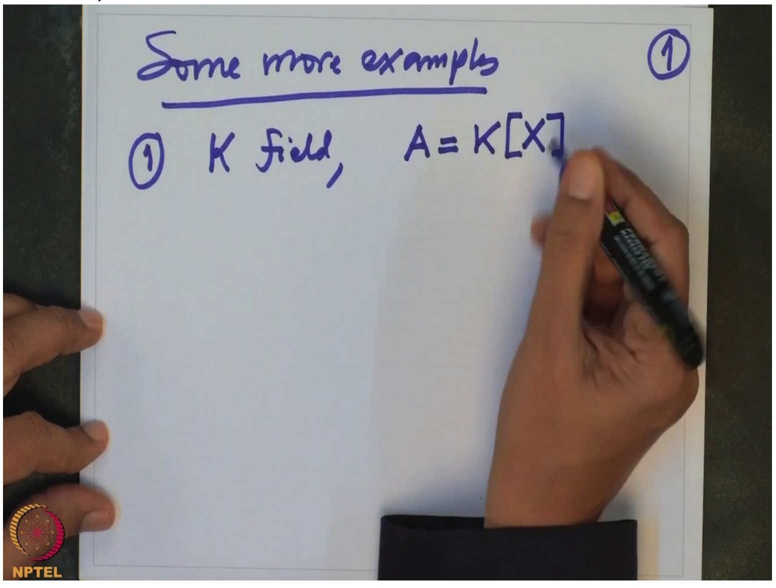
That means; examples of transcendental elements. So, some more examples.

(Refer Slide Time 01:40)



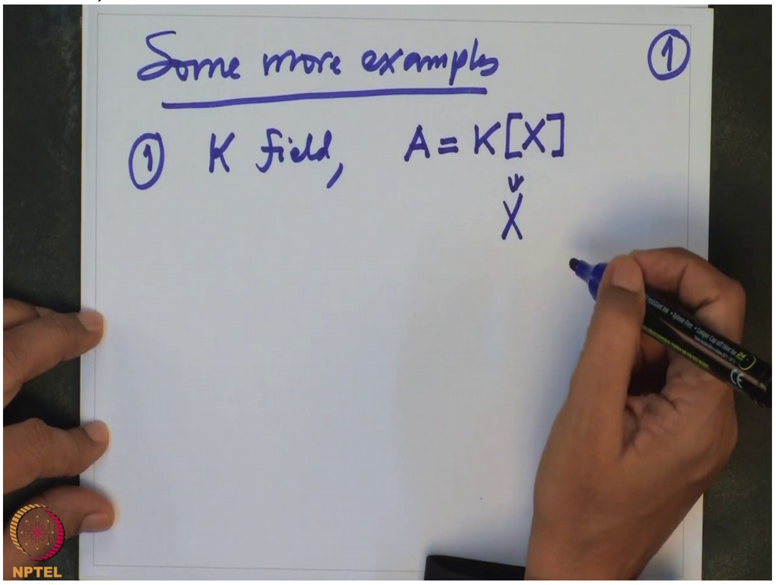
So first one is, now K is field, arbitrary field and let us, let me take my K-algebra A to be a polynomial algebra $K[X]$

(Refer Slide Time 01:58)



and the element there is capital X,

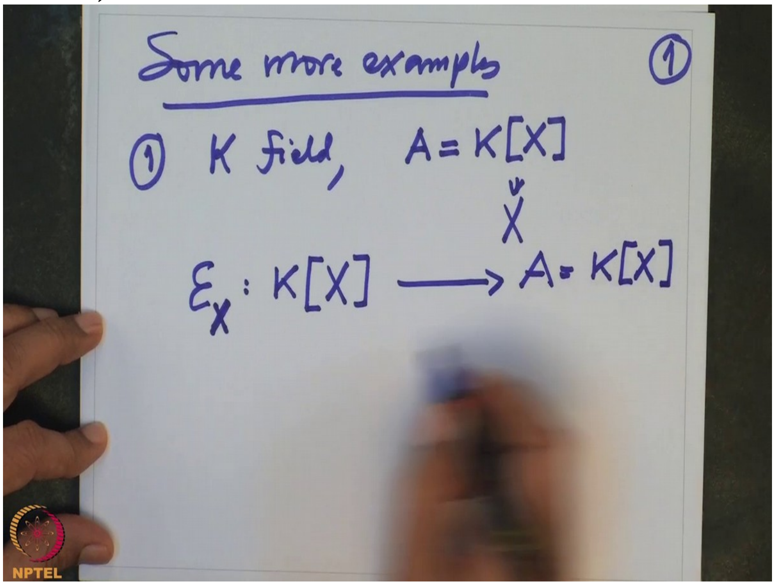
(Refer Slide Time 02:03)



Ok. Then in this case, what is the substitution homomorphism? epsilon capital X should be a K-algebra homomorphism from $K[X]$ to A. But A is also $K[X]$.

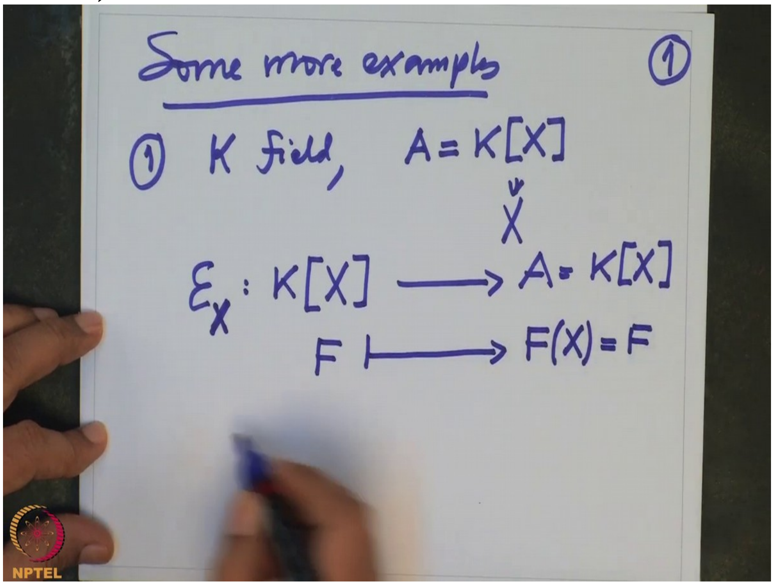
And what is the map?

(Refer Slide Time 02:23)



Any polynomial F got to be evaluated at capital X but that is same as F. So

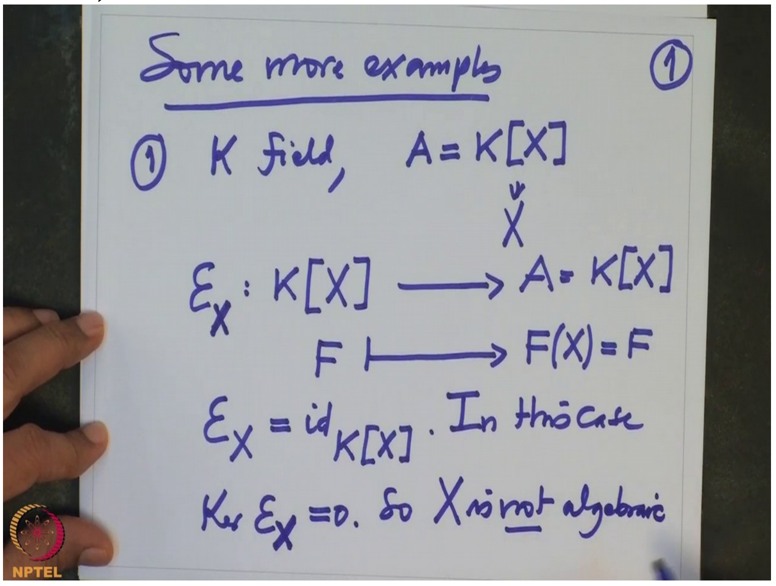
(Refer Slide Time 02:33)



that means in this case, this evaluation map or substitution map is identity map of the K-algebra $K[X]$. So it is identity map.

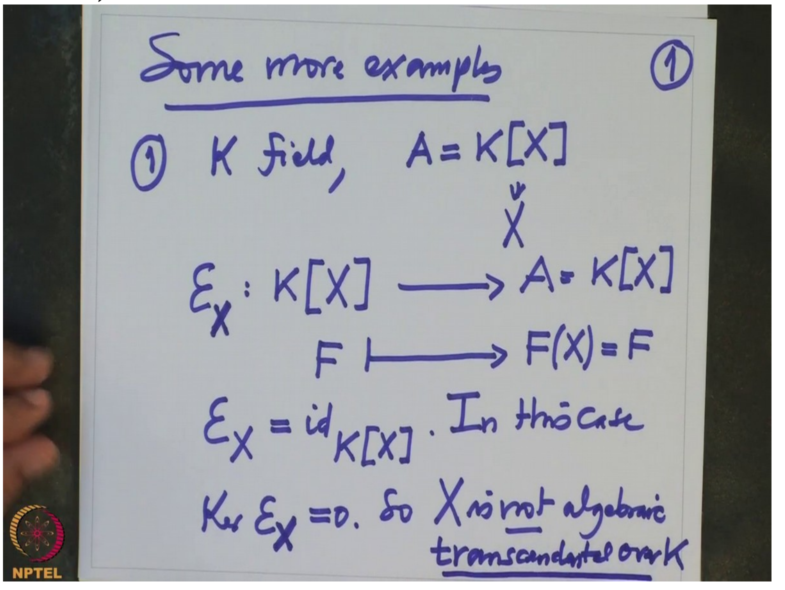
So kernel cannot be zero. So then in this case, in this case kernel of substitution homomorphism by X is 0. So X is not algebraic.

(Refer Slide Time 03:11)



So, therefore also it serves the right name that X is transcendental over K. So in other words the variables

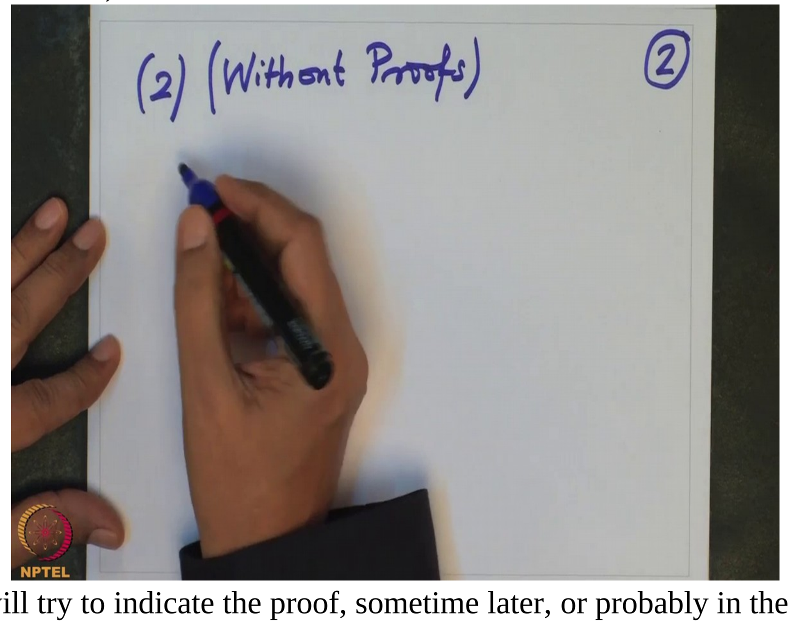
(Refer Slide Time 03:28)



we consider are always transcendental.

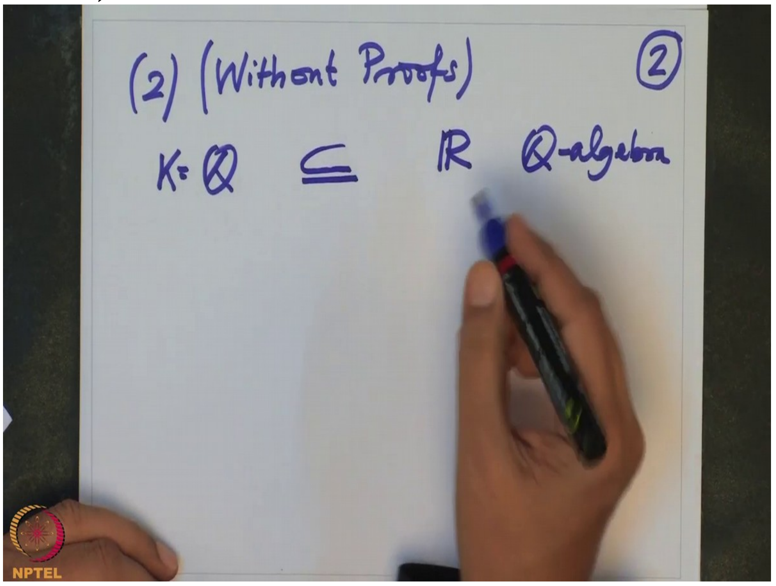
Ok, so another example, another examples proofs are not so easy. So 2, this, I am just noting these examples but without proof. So 2, without proof but eventually

(Refer Slide Time 03:55)



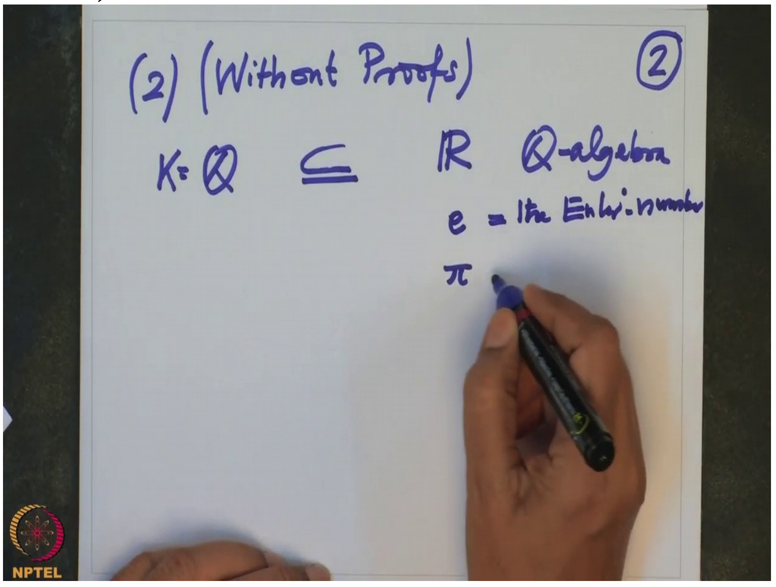
some time we will try to indicate the proof, sometime later, or probably in the exercises. So look at now $\mathbb{Q}$. Our base field is $\mathbb{Q}$. And $\mathbb{R}$ is the $\mathbb{Q}$ algebra. So this is our field extension.

(Refer Slide Time 04:23)



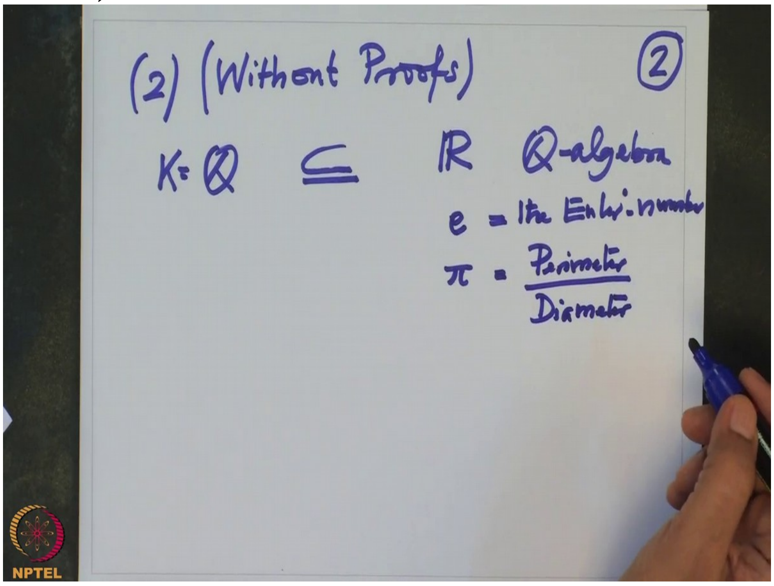
And look at the element there. They are elements called e and π . e is what is called the Euler number, Euler number and π is the,

(Refer Slide Time 04:44)



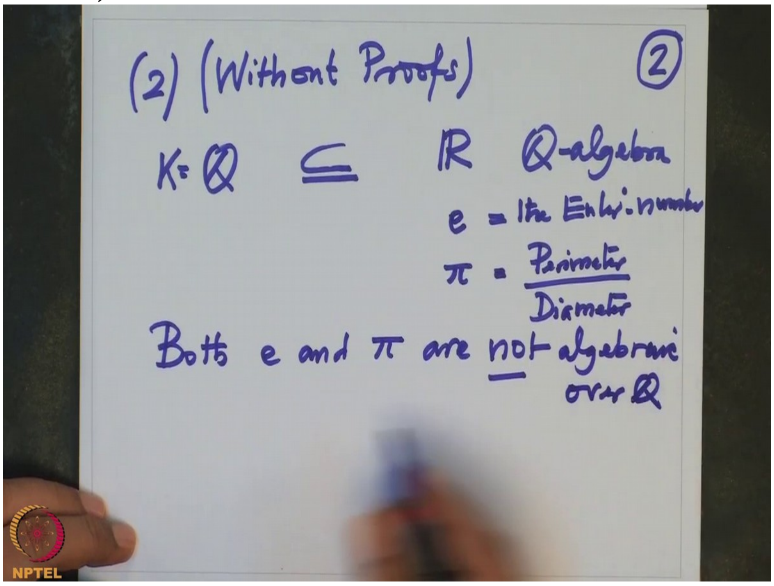
π is connected to the circle, right. This is the ratio of perimeter divided by diameter.

(Refer Slide Time 05:04)



Now there are lots of things to be checked. I am not going to go into the definitions of e and π but just mention that both e and π are not algebraic over Q.

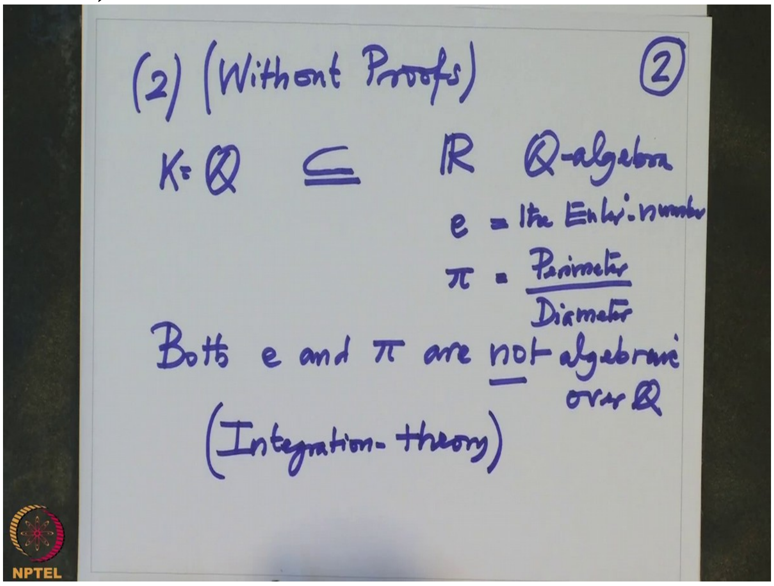
(Refer Slide Time 05:32)



This is not so easy to prove. Proof of e is relatively easier than the proof of π , but both of these needs integration theory.

And which we are not going to go

(Refer Slide Time 05:53)

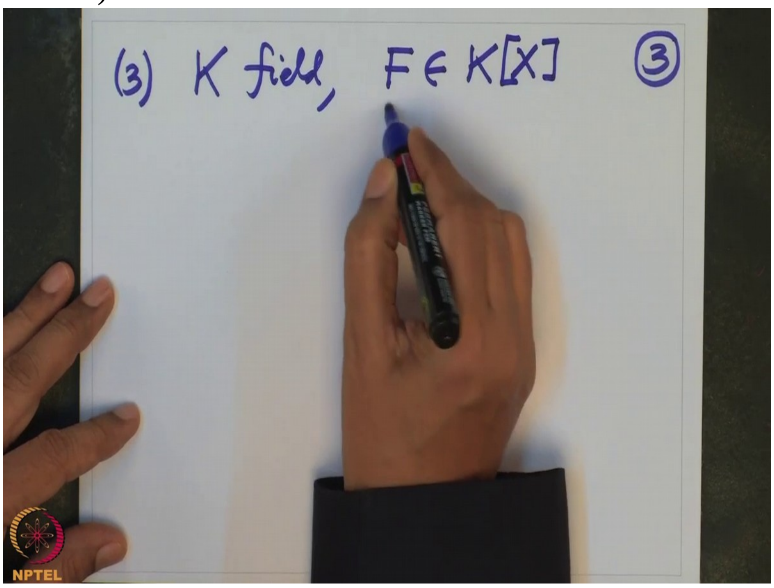


into this course but at least what we will actually show is that there are more real numbers which are not algebraic over $\mathbb{Q}$ than the real numbers which are algebraic over $\mathbb{Q}$.

This statement we will prove it in some course, some course of lecture, Ok. So the third, so these are 2 examples and, Ok so now we want to find a characterization of algebraic element. But before that again I want to give one more example that we will get acquainted with examples of K-algebra.

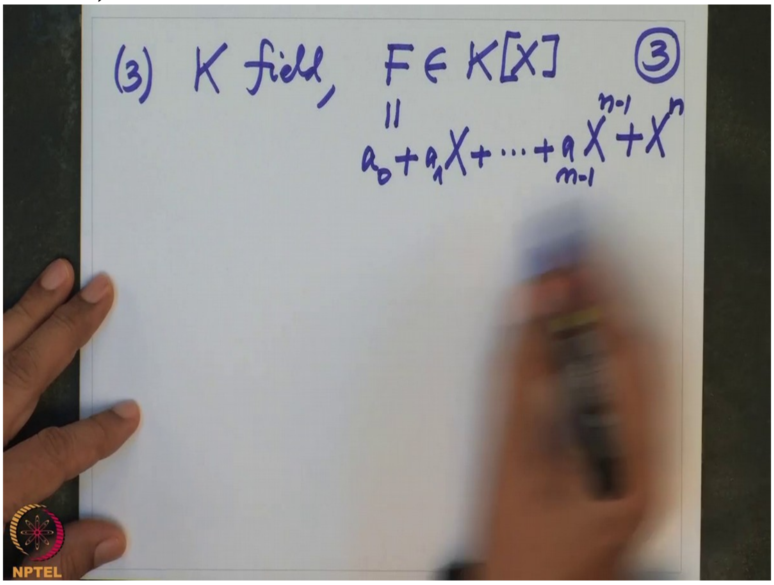
So third example, now I take K is our base field. And I fix a polynomial capital F. Capital F is a polynomial in $K[X]$, fixed polynomial

(Refer Slide Time 07:03)



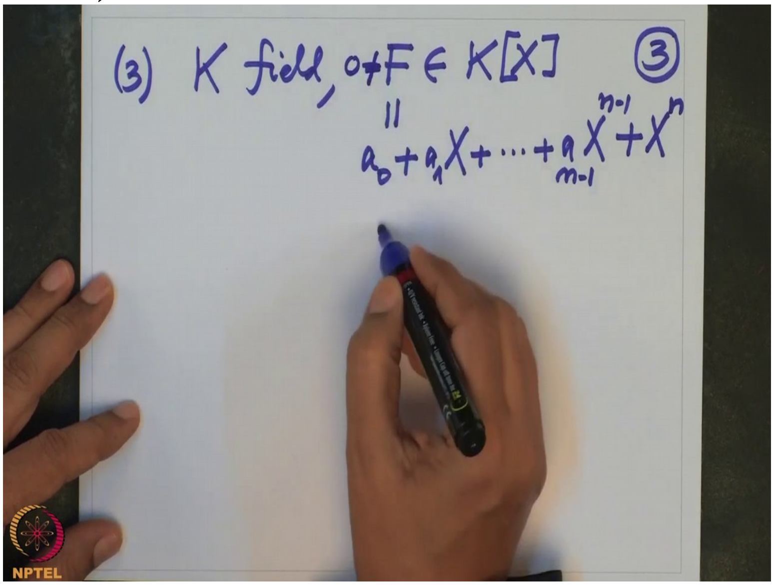
and non-zero polynomial... So and that I write it as like this. $a_0+a_1X+...+a_{n-1}X^{n-1}+X^n$. So it is a monic polynomial

(Refer Slide Time 07:20)



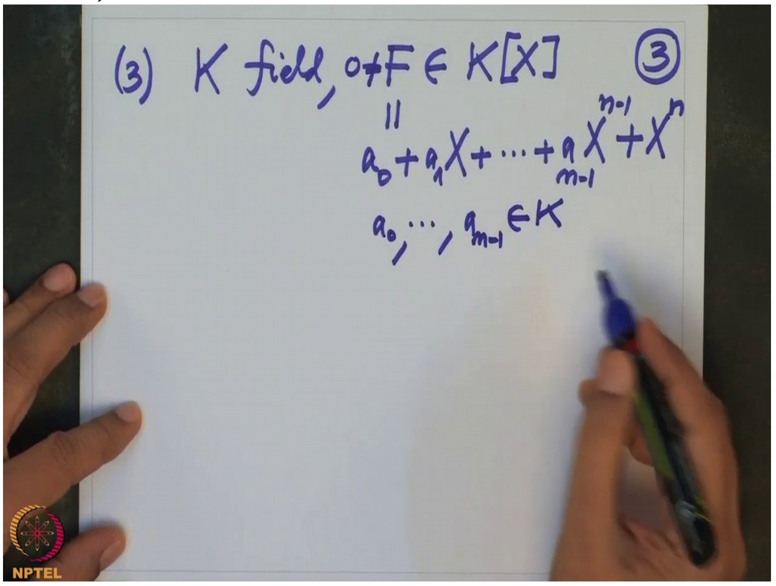
in $K[X]$. F is non-zero. So

(Refer Slide Time 07:27)



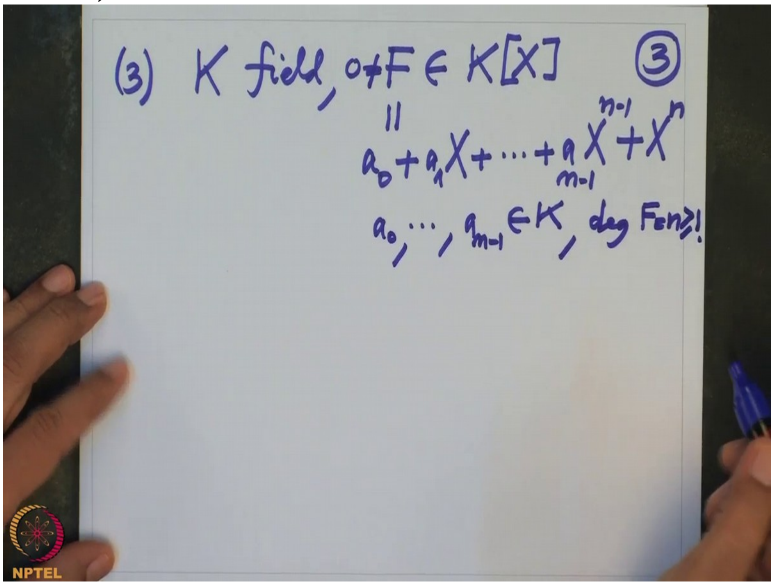
a_0 to a_{n-1} , they are elements in the field K.

(Refer Slide Time 07:34)



The degree of F is obviously n. And n is bigger equal to 1 let us assume.

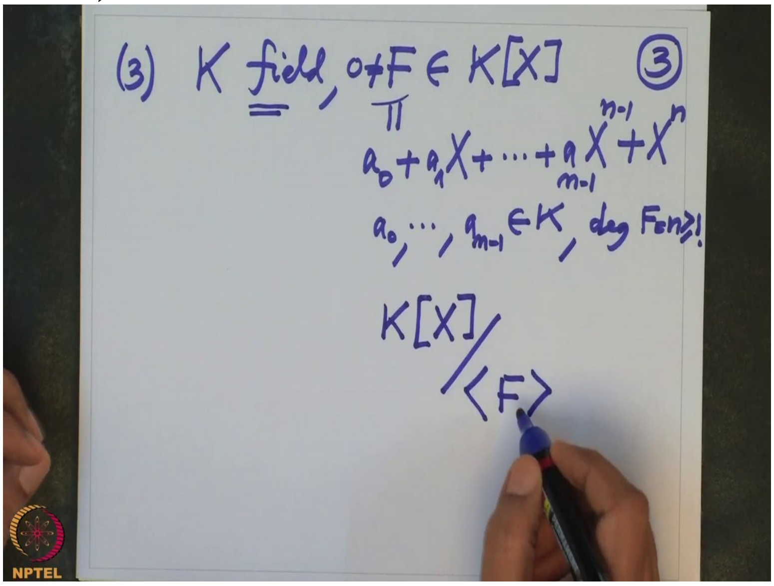
(Refer Slide Time 07:42)



So, by the way any polynomial you could have made it monic because we are in the case of field. So just if I say F is non-zero polynomial, that is enough. But only thing I have to say that the degree is bigger equal to 1.

So you get such a polynomial and then I have these operations modulo F, modulo F, $K[X]$ modulo ideal generated by F. So F is the principal ideal generated by F. That means we are taking all polynomial multiples of this given F.

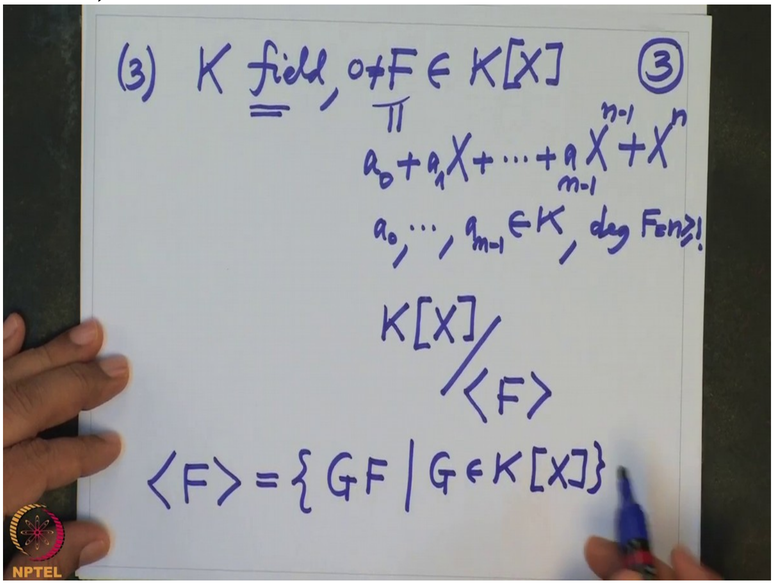
(Refer Slide Time 08:20)



So all these are all polynomials, ideal generated by F is by definition, all G times F where G is a polynomial in $K[X]$.

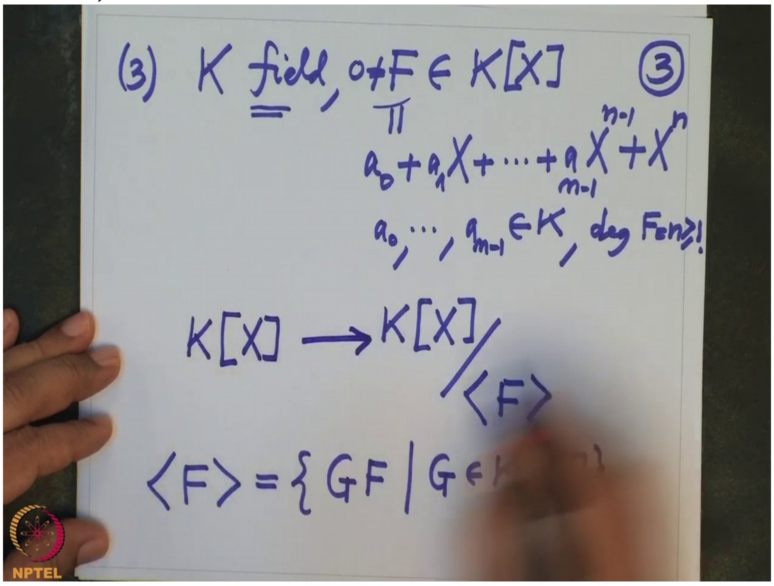
This is clearly an ideal and

(Refer Slide Time 08:36)



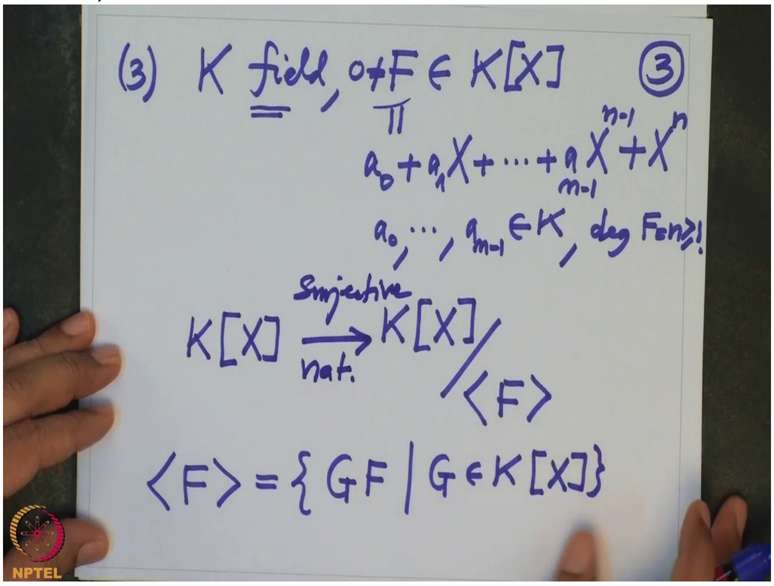
then we go modulo that ideal and then form a new ring. Actually this is also K-algebra. So just there is also, K-algebra homomorphism from $K[X]$ to this algebra. $K[X]$

(Refer Slide Time 08:55)



This is surjective, so this is a natural map. I just want to remind you

(Refer Slide Time 09:03)

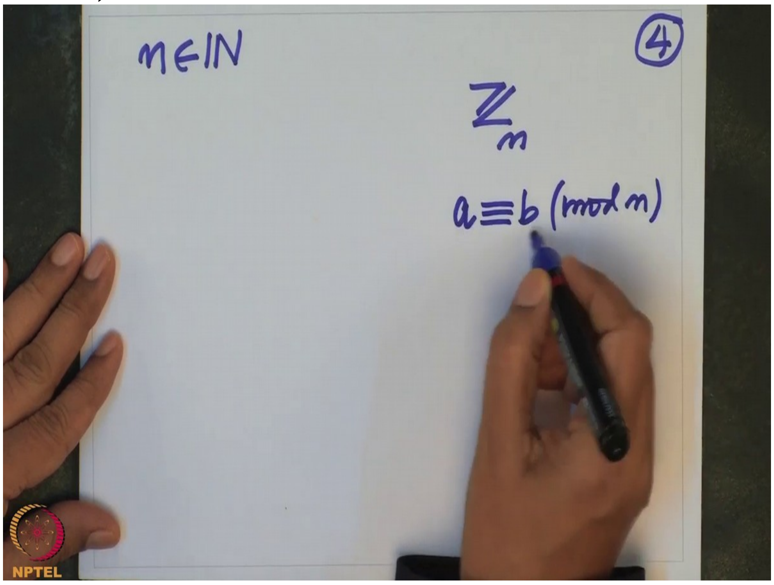


that this is similar to what we have studied for integers.

So this is similar to, remember any given natural number n, we have defined $\mathbb{Z}_n$, this is from the usual addition and multiplication we have defined two operations, addition modulo n and multiplication modulo n which made it a ring.

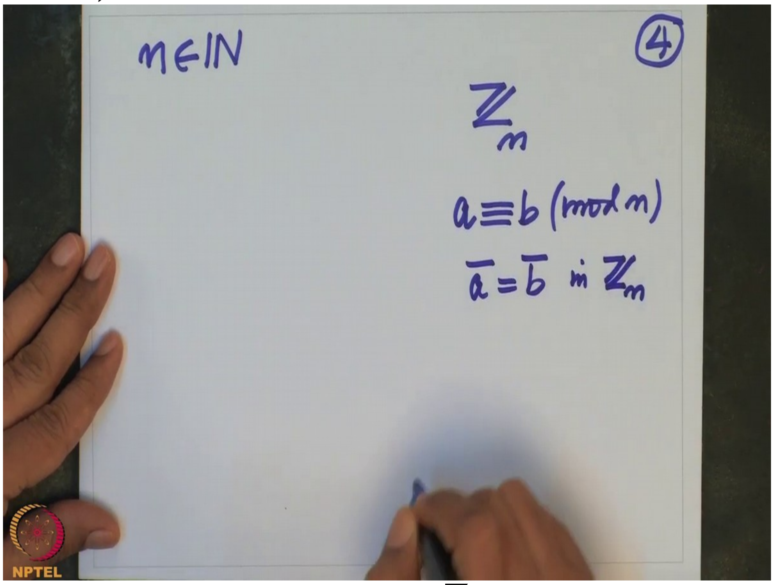
And how are they defined? The difference of the integers should be divisible by n and they are equal. So we started using this notation. a congruent to b mod n that means they are not equal

(Refer Slide Time 09:45)



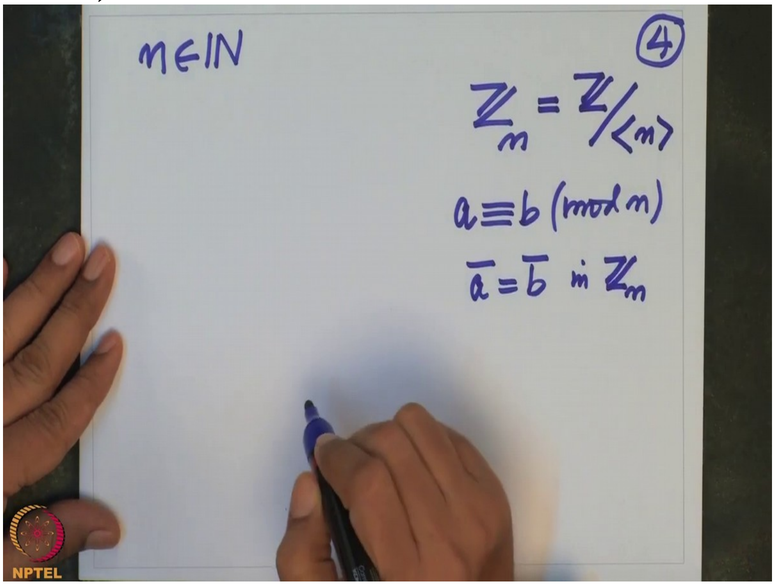
but they are in the same equivalence class. So here that this is same as writing a bar equal to b bar in $\mathbb{Z}_n$.

(Refer Slide Time 09:57)



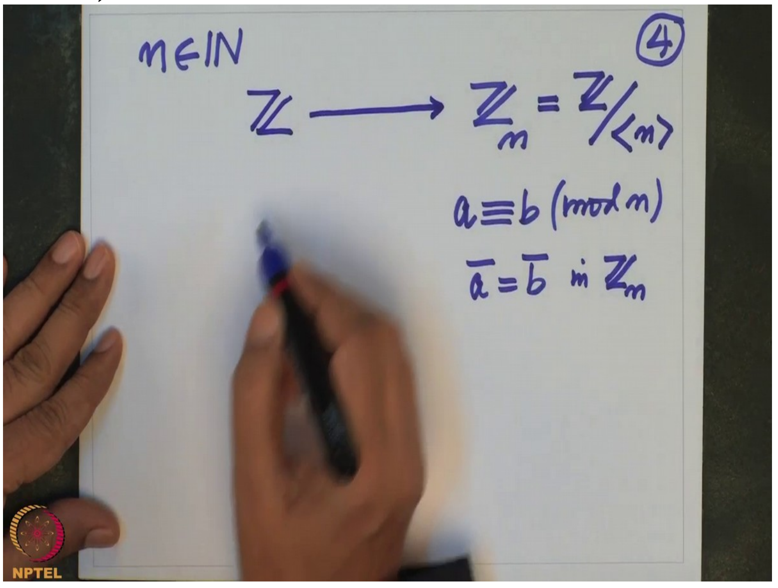
And actually $\mathbb{Z}_n$ you should think it is a ring $\frac{\mathbb{Z}}{\langle n\rangle}$.

(Refer Slide Time 10:06)



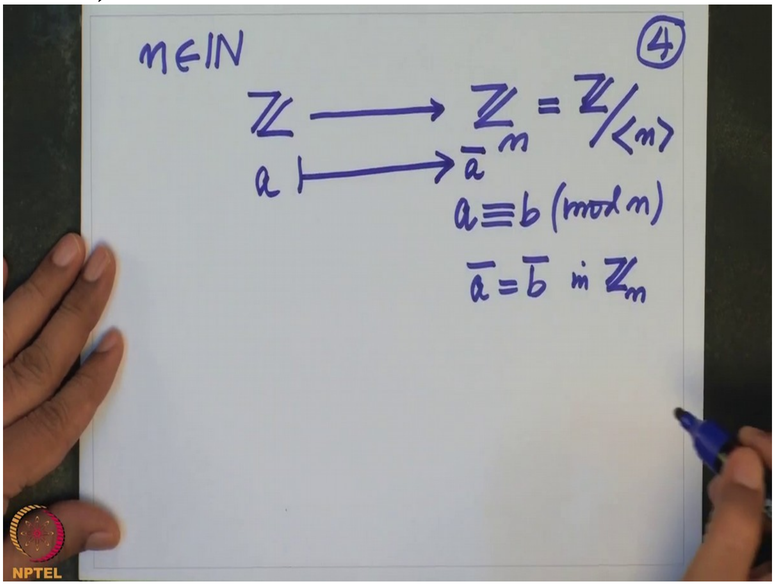
And then we have a natural map here. $\mathbb{Z}$ to this, this map is

(Refer Slide Time 10:11)



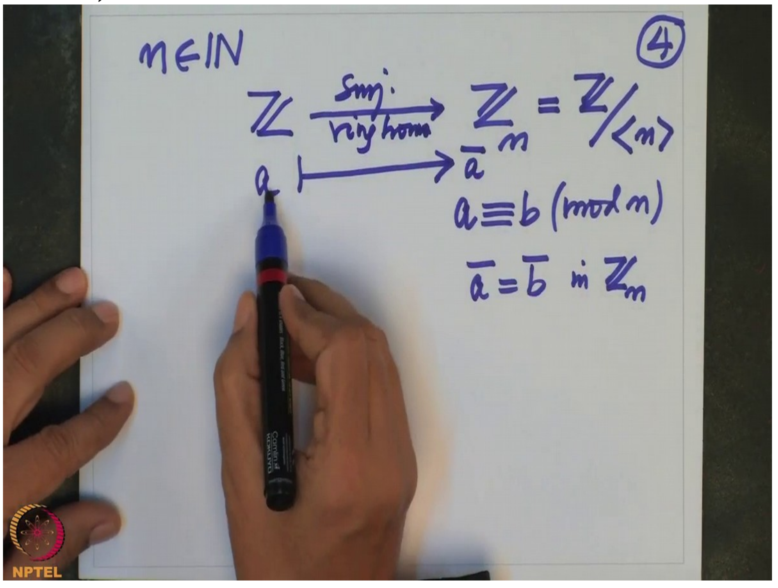
any a going to its residue class modulo n that is denoted by $\bar{a}$

(Refer Slide Time 10:16)



and this becomes a surjective ring homomorphism. And what is the kernel? Precisely

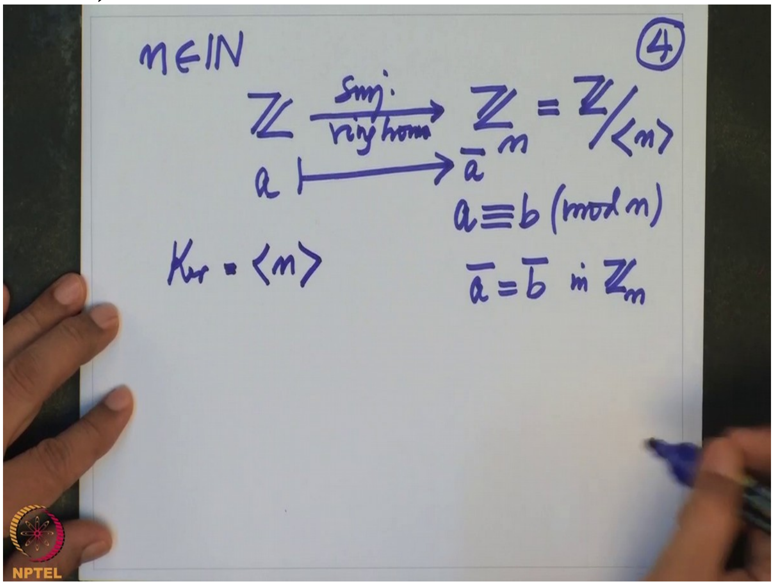
(Refer Slide Time 10:24)



all those elements which go to zero that means all those integers who, when I divide by n the remainder is zero.

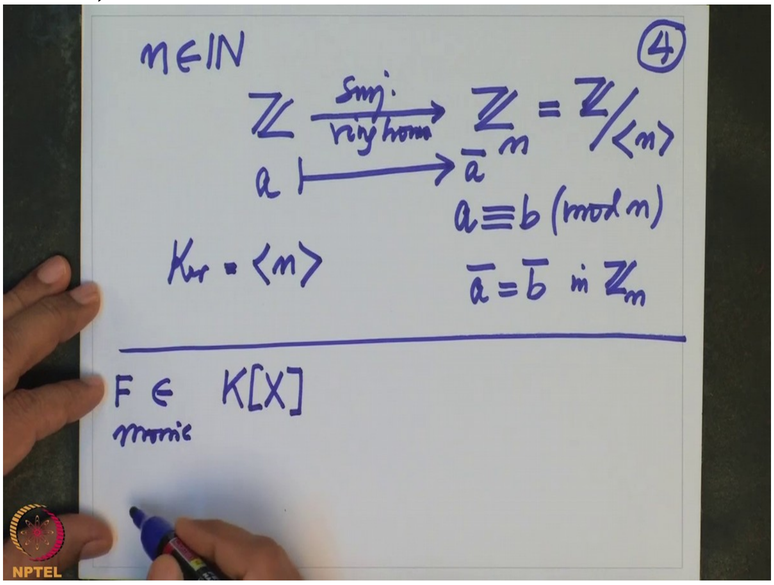
That is equivalent to saying the kernel of this map is precisely all multiples of n.

(Refer Slide Time 10:39)



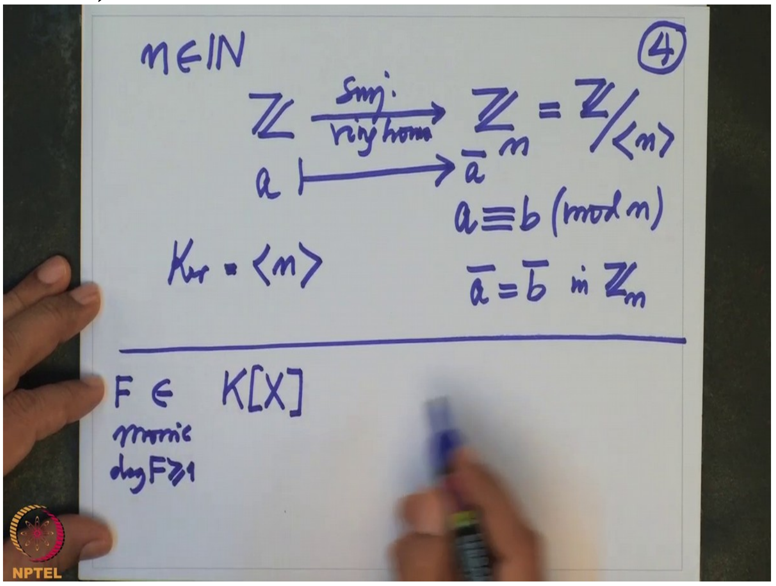
So similarly, same analogy I applied to the polynomial in $K[X]$ instead of natural number F, n I have monic polynomial F, monic.

(Refer Slide Time 10:56)



Degree is at least 1, so that it is non-constant.

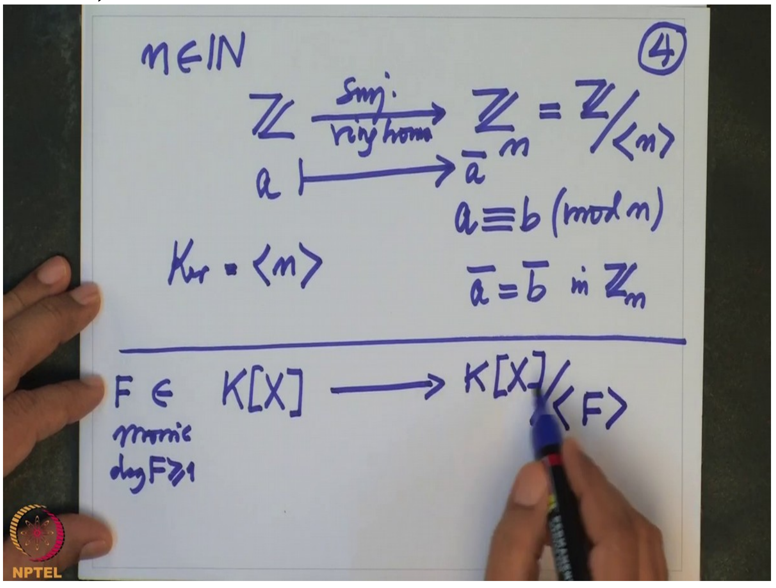
(Refer Slide Time 11:01)



And then we have gone modulo this polynomial, ideal generated by F.

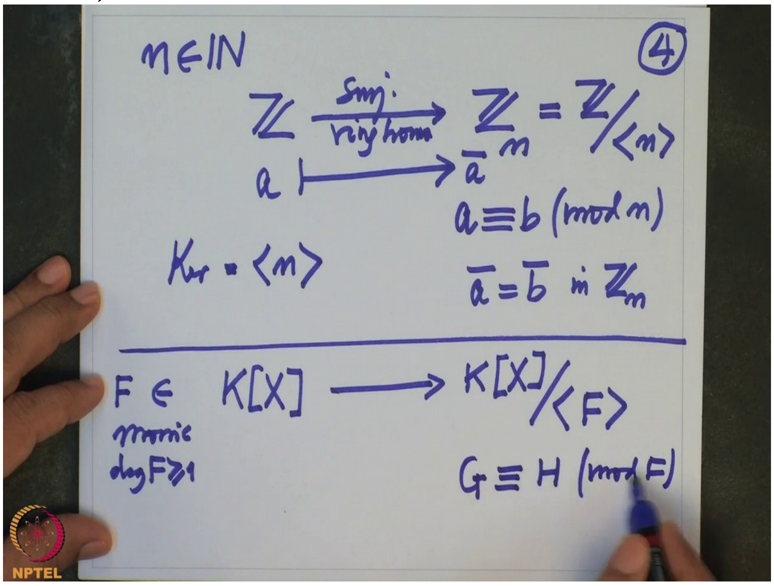
And what are elements here? Elements here are

(Refer Slide Time 11:12)



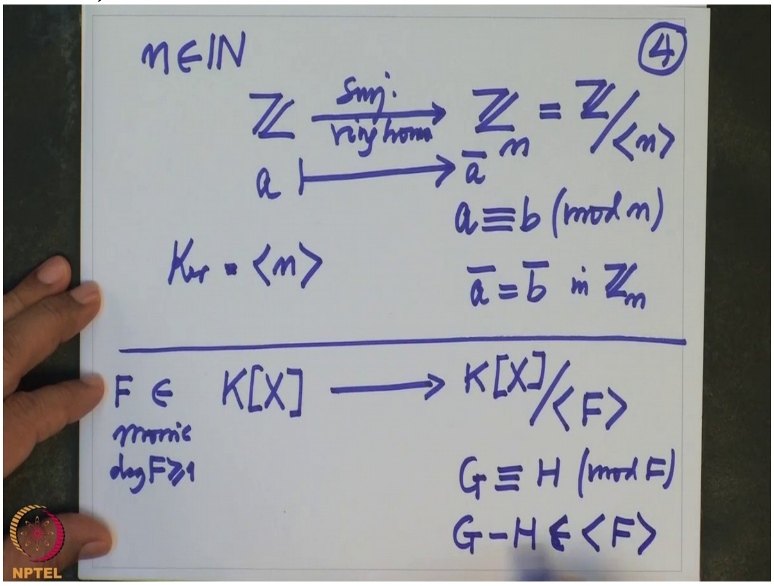
precisely, when do I write this and this? So I will write G and H, 2 polynomials. I will write this congruent to mod F simply mean, this meaning is

(Refer Slide Time 11:25)



the difference belong to the ideal generated by F. That means difference of these

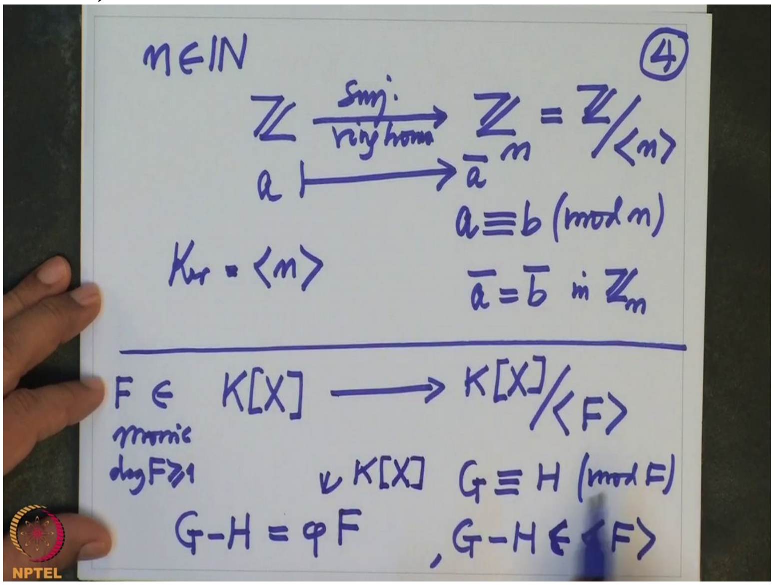
(Refer Slide Time 11:34)



polynomials.

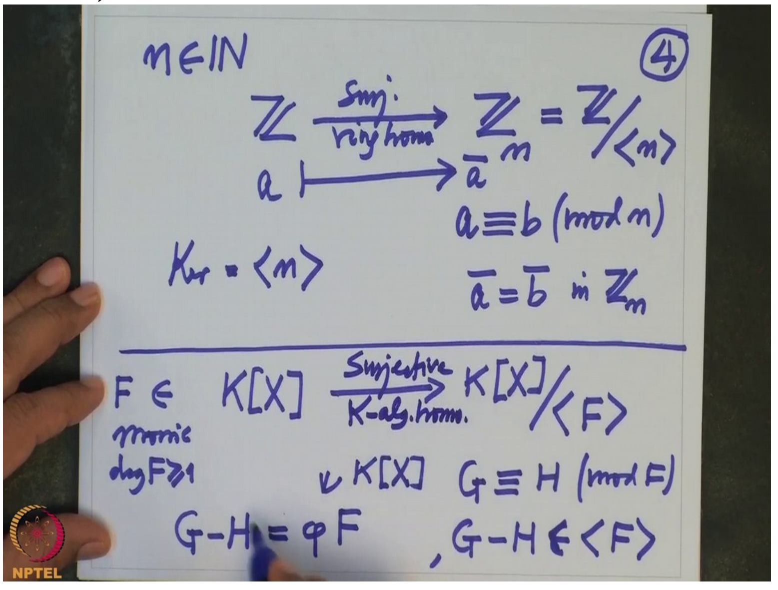
So that is F minus G is some multiple of F. So this is ϕ times F where ϕ is another polynomial in $K[X]$, the same analogy as this. So we

(Refer Slide Time 11:52)



get a surjective, surjective K-algebra homomorphism.

(Refer Slide Time 12:03)

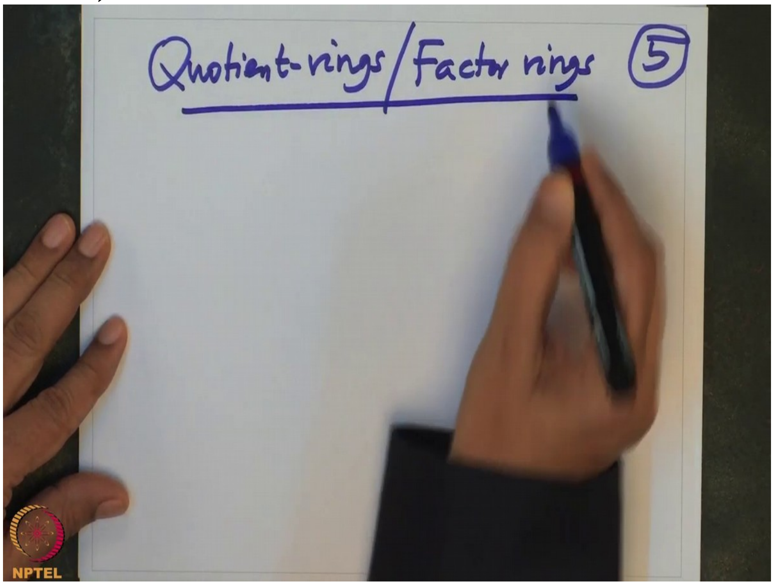


And kernel of this is precisely the ideal generated by F. And this ring is called quotient ring of $K[X]$.

And nothing special about these two rings. So more generally what know, this construction we will keep using it again and again and one would have studied this in, in a first course on algebra, these are also called quotient rings, or also called factor rings.

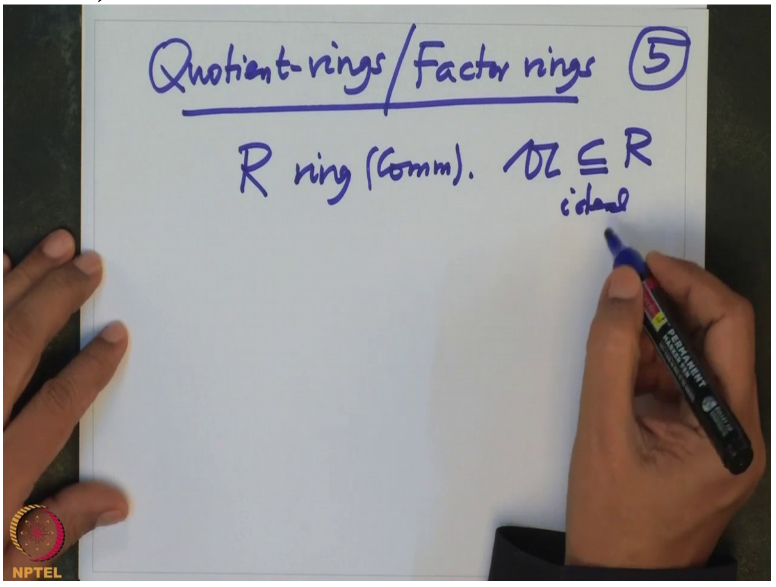
So what is thing?

(Refer Slide Time 12:42)



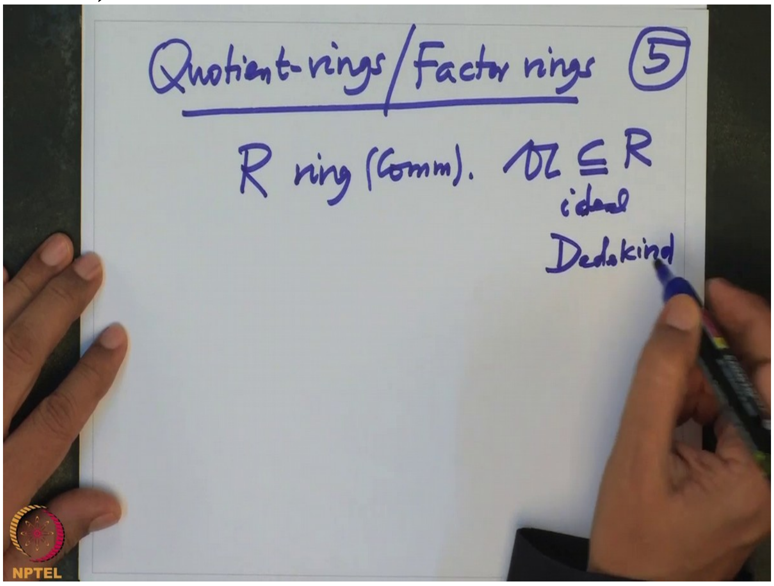
If you have ring R, R is arbitrary ring but assume commutative, commutative ring and suppose A is an ideal in R, ideal so last

(Refer Slide Time 12:58)



time I told you ideals were usually, the first time introduced by Dedekind. And Dedekind was a German mathematician.

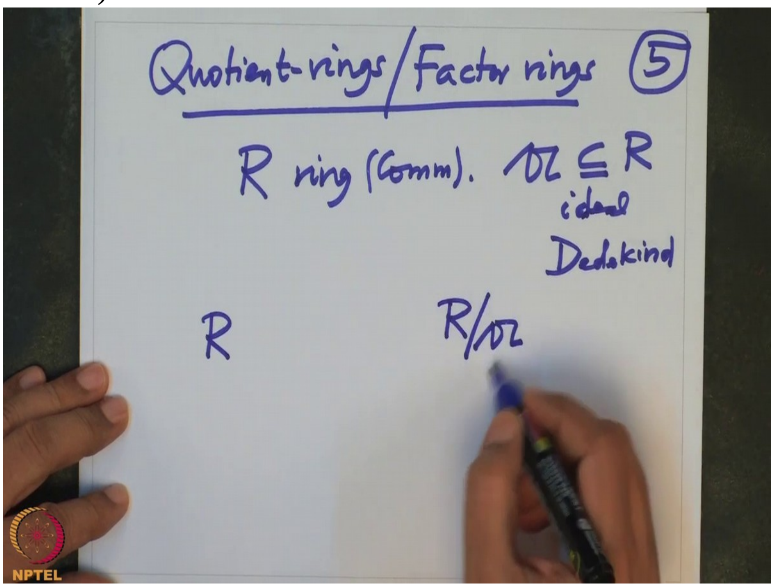
(Refer Slide Time 13:08)



So he has used his Gothic letters to denote ideals in arbitrary rings.

So if A is an ideal in R, then we have this ring R and we have constructed this new ring R mod A, the same as by the analogy of above two examples, what are the elements here? They are

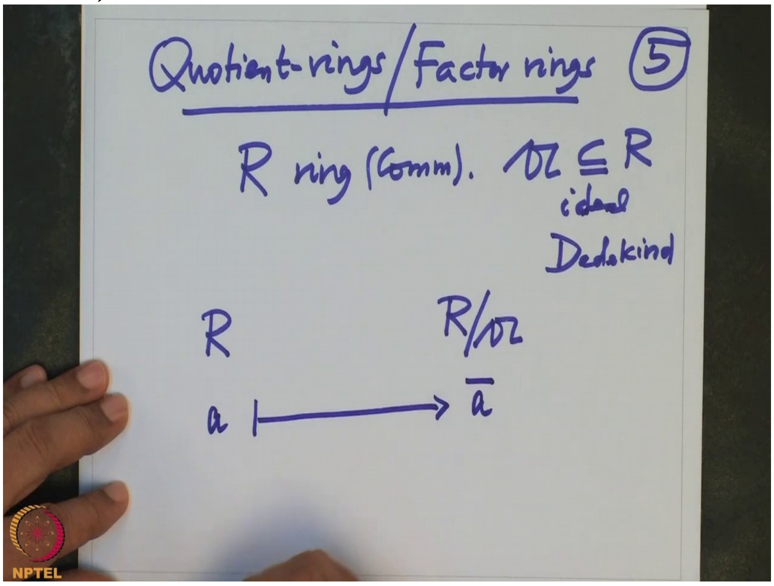
(Refer Slide Time 13:31)



element, precisely the equivalence classes when you read modulo A.

So that means given any element a here, we read mod this A denote by a bar

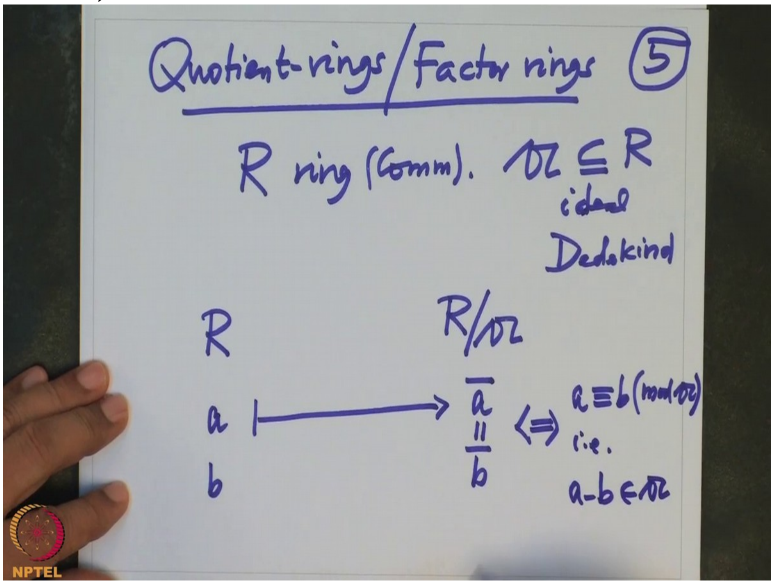
(Refer Slide Time 13:46)



and when do you say two $\bar{a}=\bar{b}$, that is equivalent to saying a congruent to b mod A, I use the same notation.

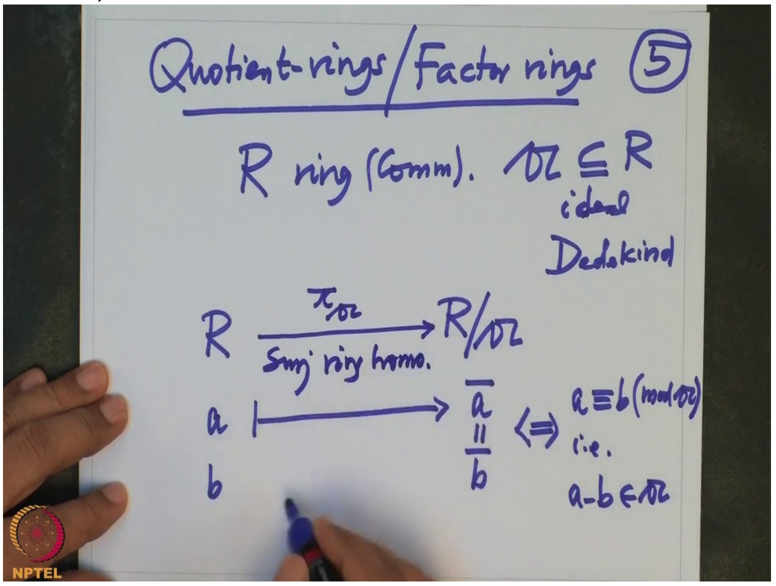
But this means, so that is the difference $a-b$ belong to the ideal A.

(Refer Slide Time 14:07)



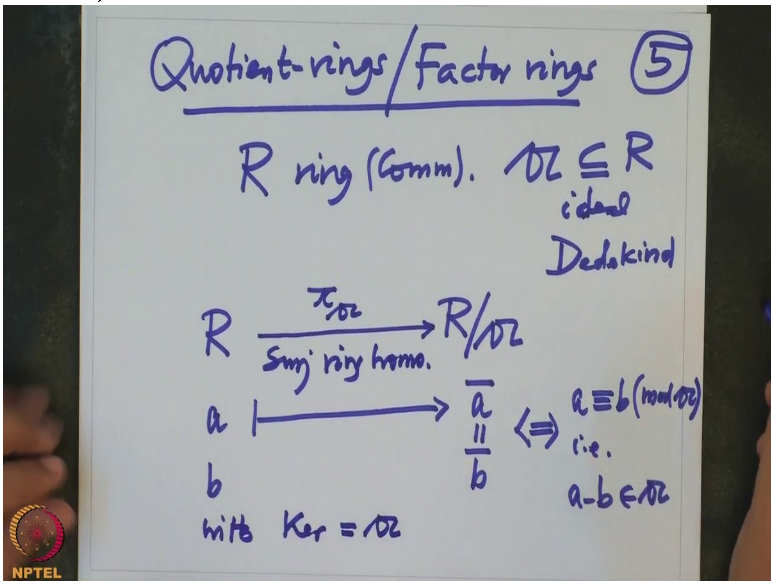
Now one check that this defines a new ring and that also the natural map is there, this map is sometimes denoted by π_A. This π_A is a surjective ring homomorphism with kernel

(Refer Slide Time 14:26)



equal to A.

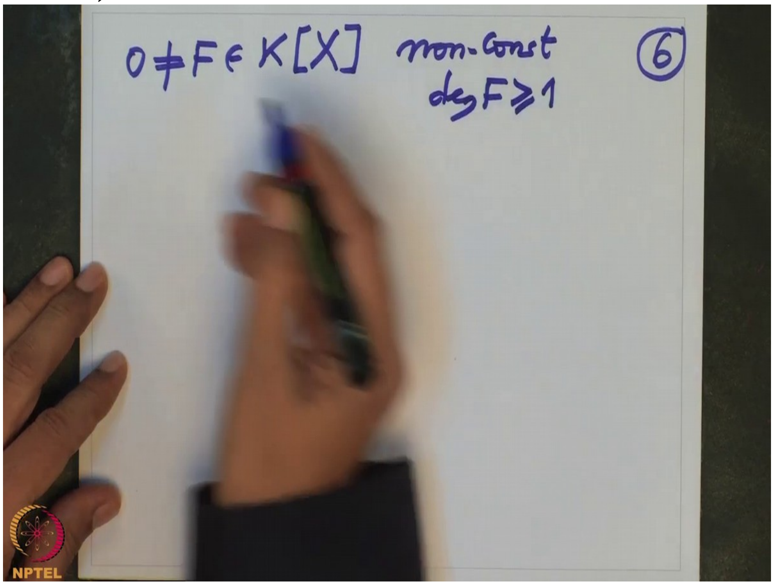
(Refer Slide Time 14:32)



So not only kernel of a ring homomorphism is an ideal but this shows also that every ideal is a kernel of some ring homomorphism. And this construction is very useful. And with this you can construct many more rings from a given ring. So this will give us a lot of examples of the rings in general.

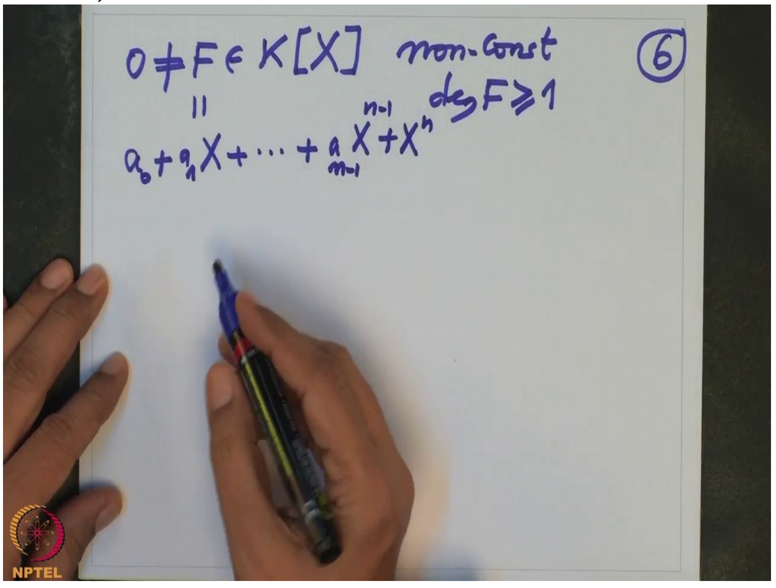
Ok, coming back to our problem, so I wanted to define, so given a non-zero polynomial F of degree non-constant, non-constant that means the degree of F is at least n, at least 1

(Refer Slide Time 15:18)



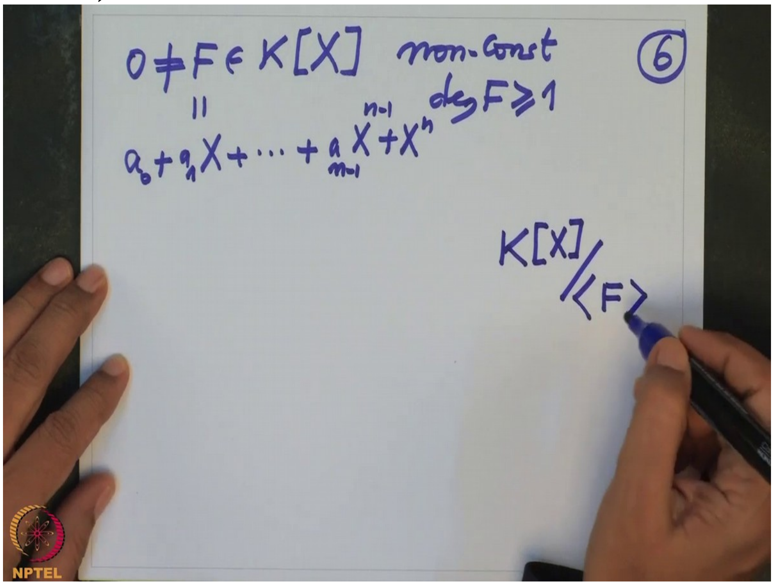
and F we have written it as monic, we are assuming. That we can always do it the when the base ring is a field so it looks like this.

(Refer Slide Time 15:33)



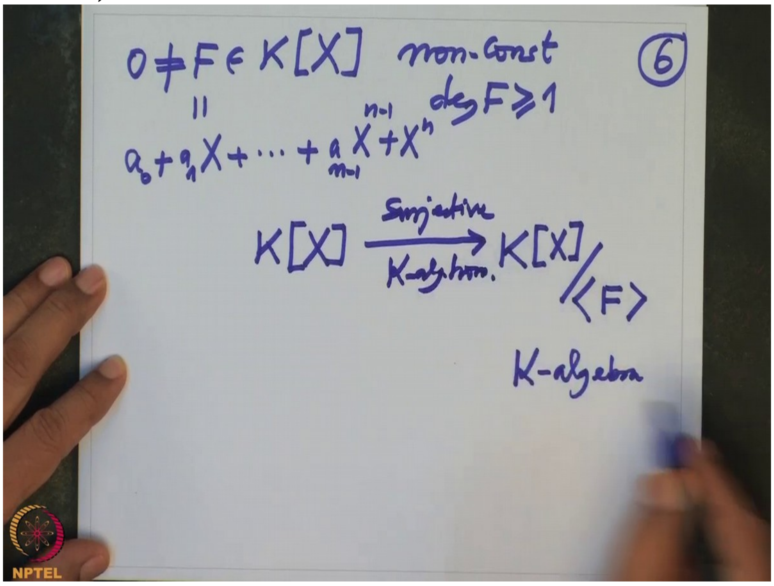
And then I have gone to the residue classes, these quotient ring and factor ring are also called residue class rings. So $K[X]$ and I will keep writing as $\frac{K[X]}{F}$ that means modulo ideal generated by

(Refer Slide Time 15:48)



F. This is my new K-algebra; this is surjective K-algebra, homomorphism

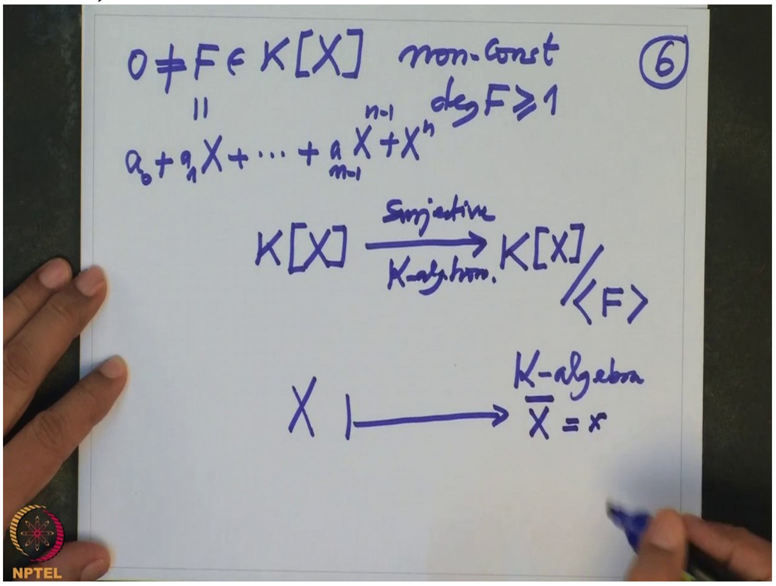
(Refer Slide Time 16:08)



from K X to this, which is surjective K-algebra homomorphism.

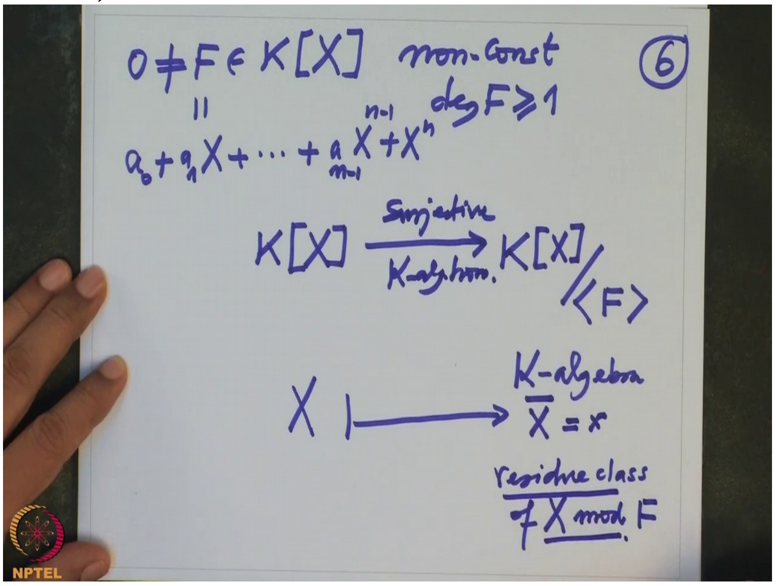
And this, therefore this X goes to $\overline{X}$, that $\overline{X}$ I am going to denote with small x,

(Refer Slide Time 16:19)



small x is called the residue class of X modulo F, mod F.

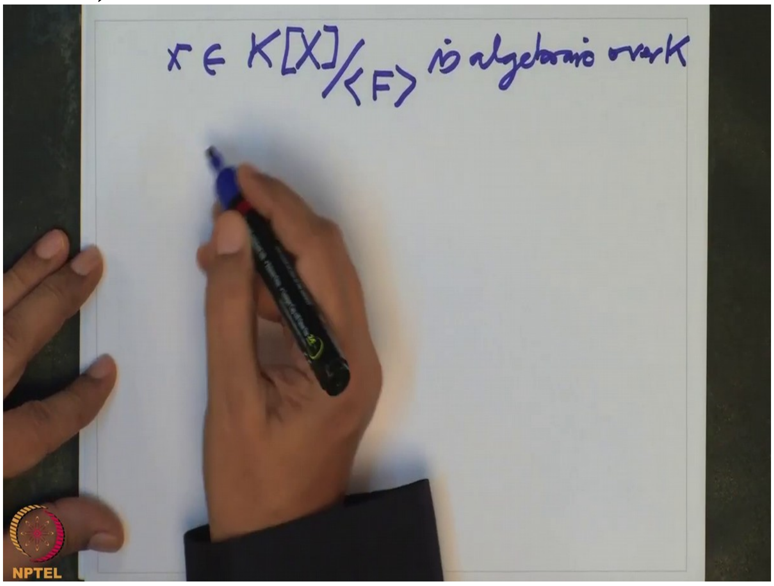
(Refer Slide Time 16:34)



And, and that is checked. So now we are debating whether this small x is algebraic over K or not.

Now I have a K-algebra. And I have an element there, and then we want to see whether this x is algebraic or not. So this small x in $K[X]$, this residue class ring is algebraic over K. That is

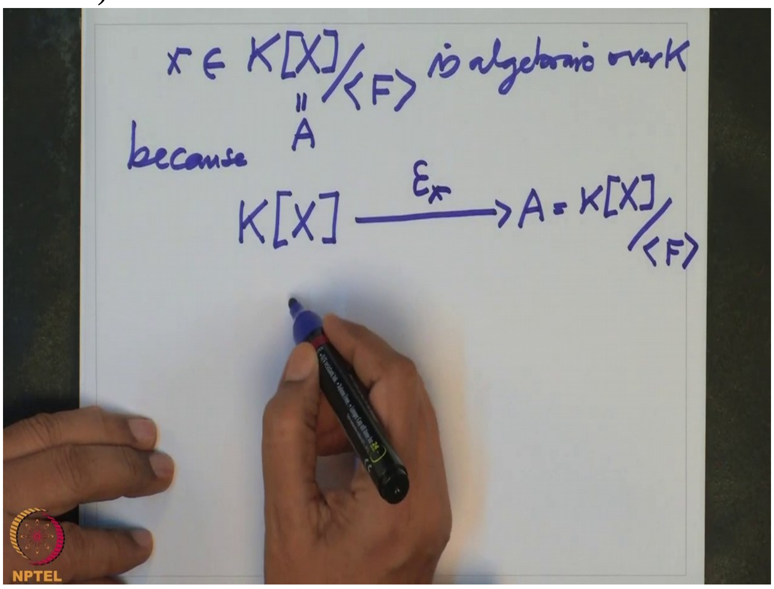
(Refer Slide Time 17:13)



simple, because, because what do we need? We need to know what is the substitution homomorphism. That substitution homomorphism from the polynomial ring $K[X]$, polynomial over ring $K[X]$ to this algebra.

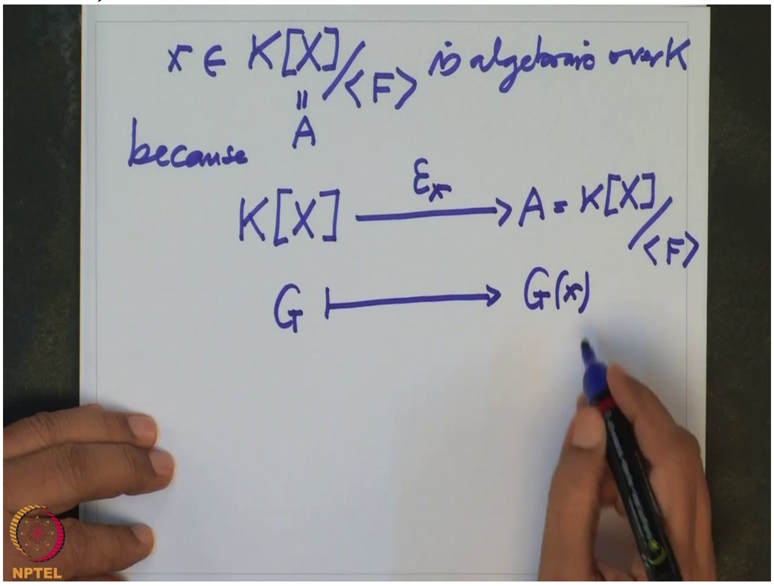
This is our algebra A, so if you write A that is this, and I want to know what is the, what is the epsilon x? That means what given any polynomial

(Refer Slide Time 17:43)



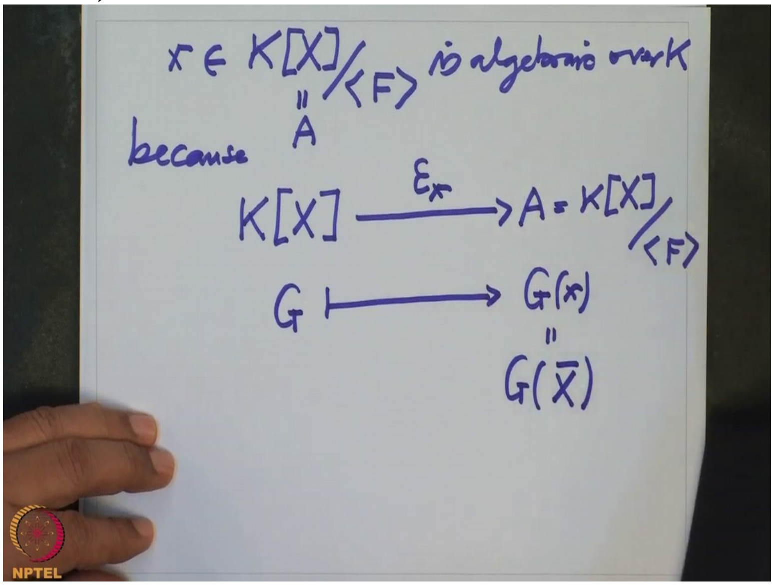
G I have to substitute instead of capital X, small x. But this is

(Refer Slide Time 17:50)



same as G of $\overline{X}$. But remember this is a

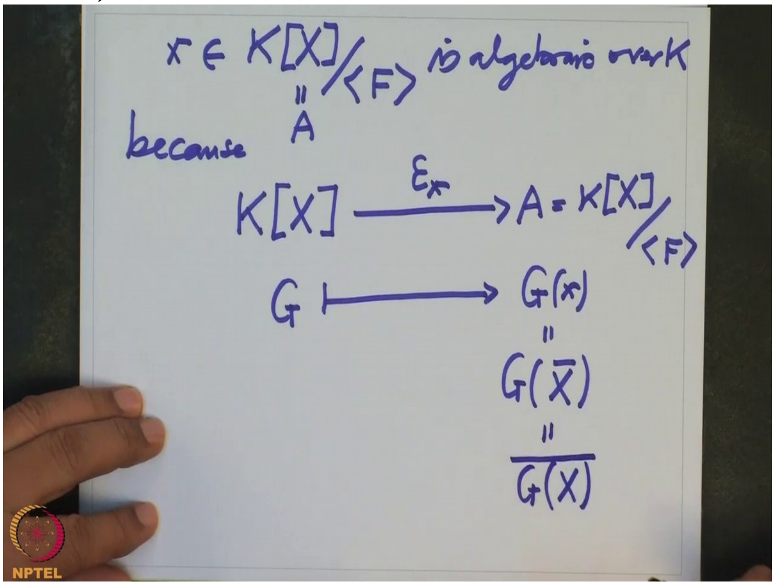
(Refer Slide Time 17:57)



K-algebra homomorphism. So whether I take the images first, whether I add first and then take the image, or take the images first and add, and similarly for multiplication these two operations are same.

So therefore this one is same as $\overline{G(X)}$

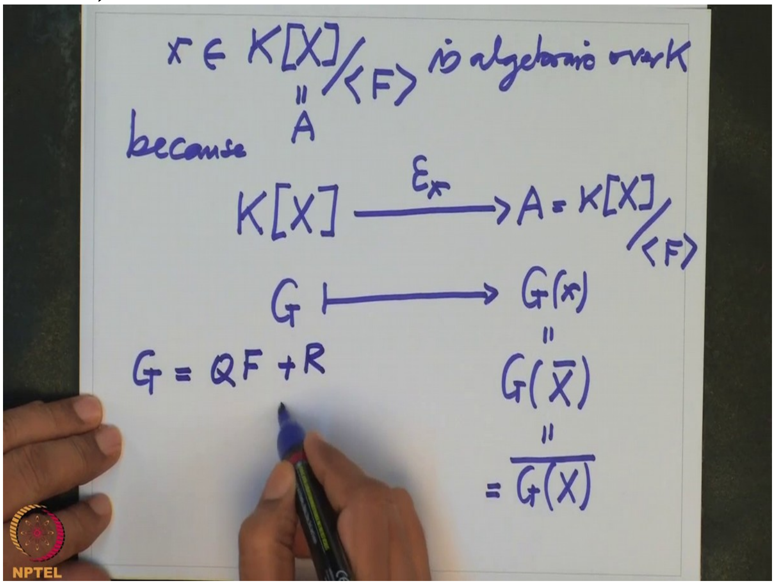
(Refer Slide Time 18:20)



that means reading this polynomial G modulo F that means take out the, this means what, what is this? How do you find this? This is, you have polynomial G given and already we had this F and that is monic, so I am going to perform the division with remainder by F to G so we will get a polynomial $Q \times F + R$ where R is a remainder.

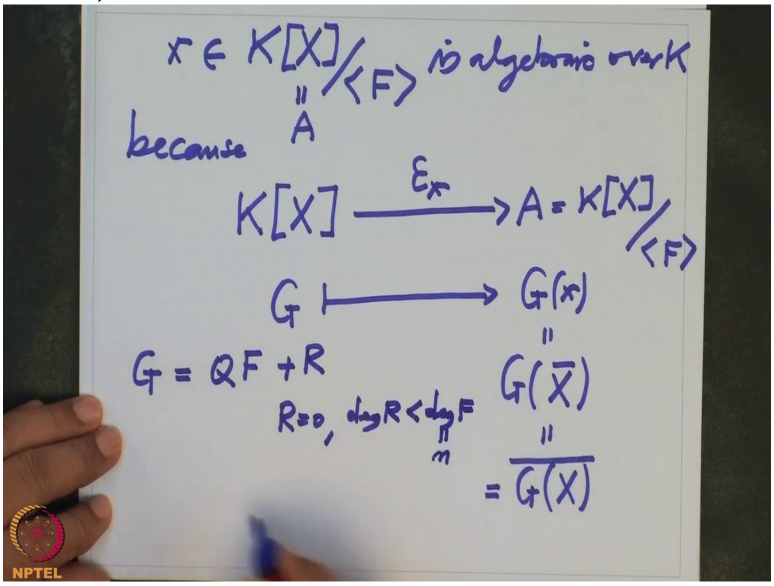
And the remainder

(Refer Slide Time 18:54)



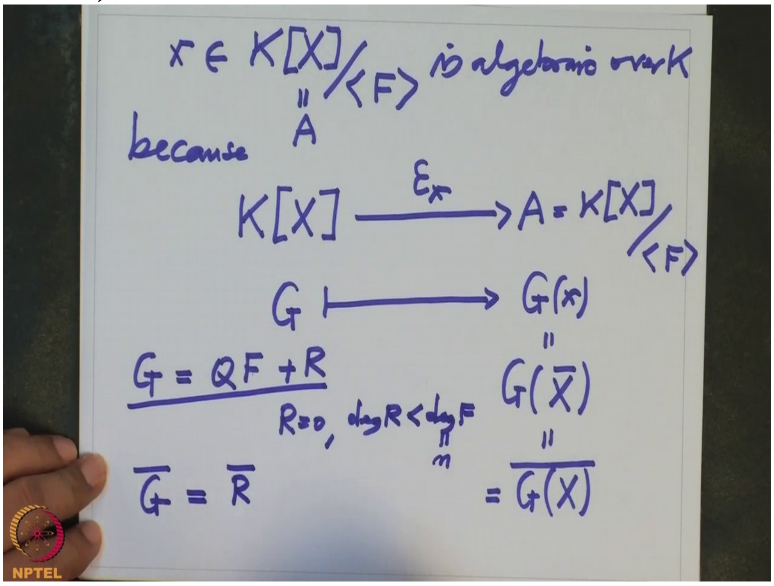
is either zero or the degree of the remainder is less than the degree of the dividend, dividend has degree n so this is degree F which is n, so

(Refer Slide Time 19:08)



therefore when I read this equation modulo F I get $\overline{G}$ equal to $\overline{R}$, because this part will go away because it is a multiple of F

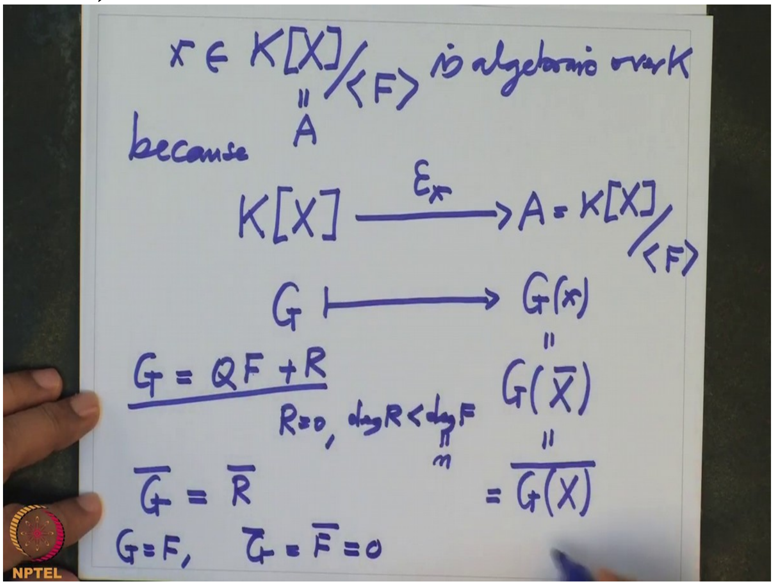
(Refer Slide Time 19:19)



So therefore any polynomial here is a bar of a polynomial whose degree is less than n or may be zero also.

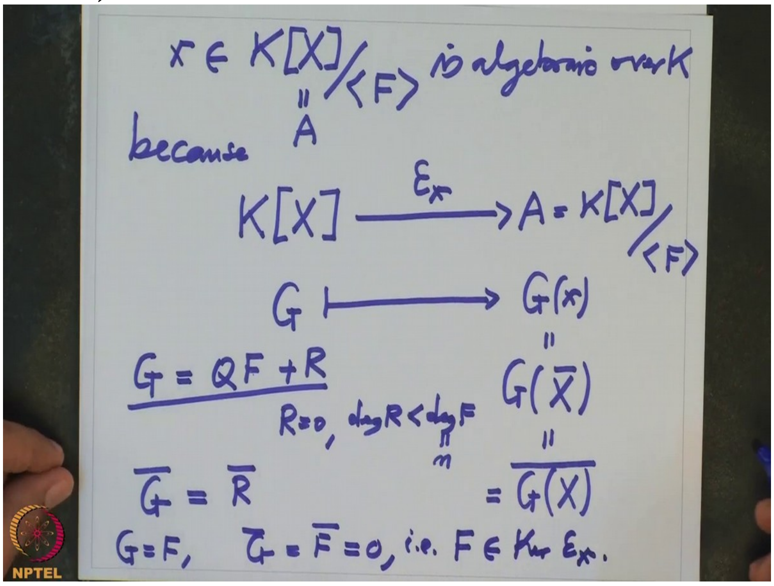
So in any case the polynomial F where do they go? If I take G equal to F, what is $\overline{G}$ then? $\overline{G}$ is $\overline{F}$, but $\overline{F}$ is, F is a multiple of F, so this is actually zero. So $\overline{G}$ is actually zero

(Refer Slide Time 19:47)



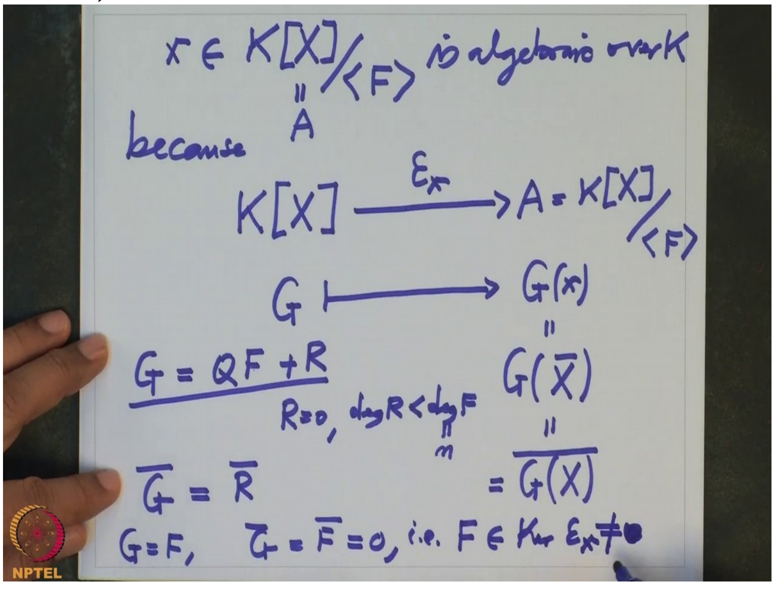
polynomial, F bar is actually zero polynomial. That means, so this simply means the polynomial capital F belongs to the kernel of substitution homomorphism by this small x.

(Refer Slide Time 20:02)



And that is, in particular this F is non-zero, because F is non-zero, this kernel ϵ_x is, kernel of ϵ_x is non-zero

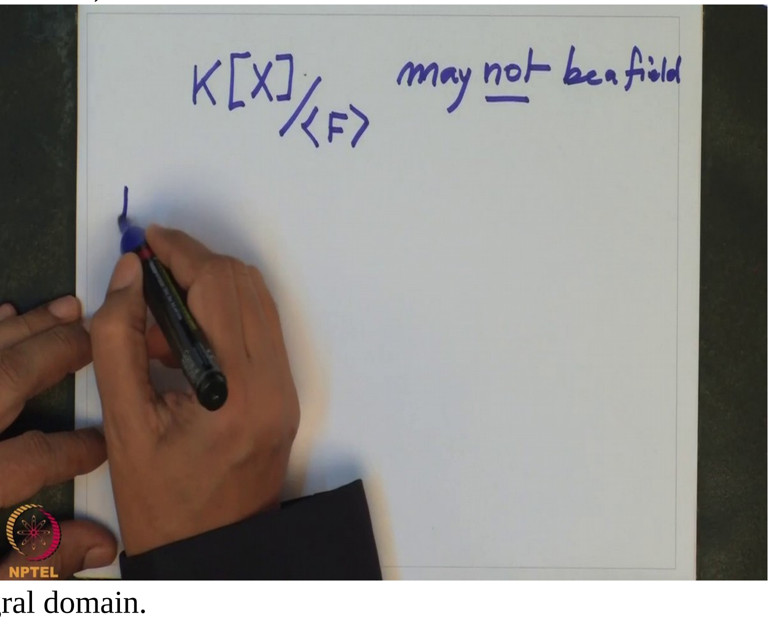
(Refer Slide Time 20:12)



and therefore this, this K-algebra homomorphism has a non-zero kernel and that precisely means that x is algebraic.

So we have seen that, how do you make, how do you get more and more examples of algebraic elements? This is the way to get more and more examples of algebraic elements. Also the last remark in this example, I want to make stress on this point, that if you look at this, this algebra, $\frac{K[X]}{F}$, this algebra may not be, may not be a field. In fact

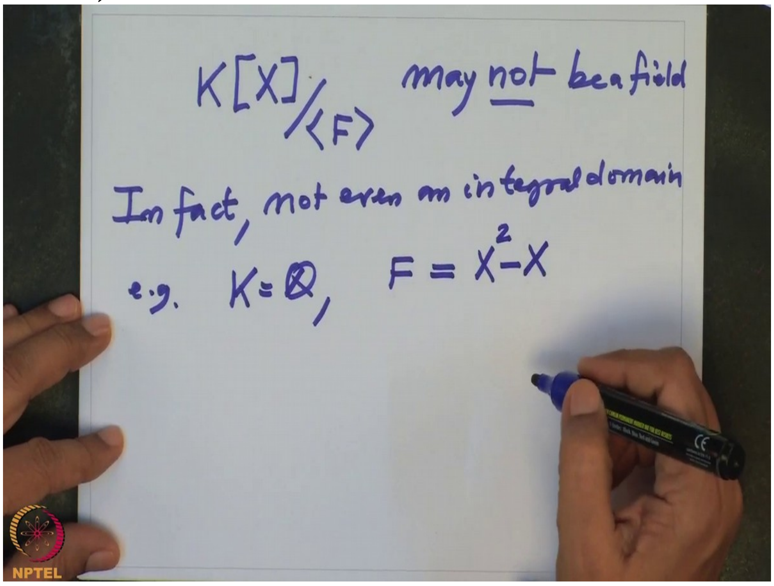
(Refer Slide Time 20:59)



not even an integral domain.

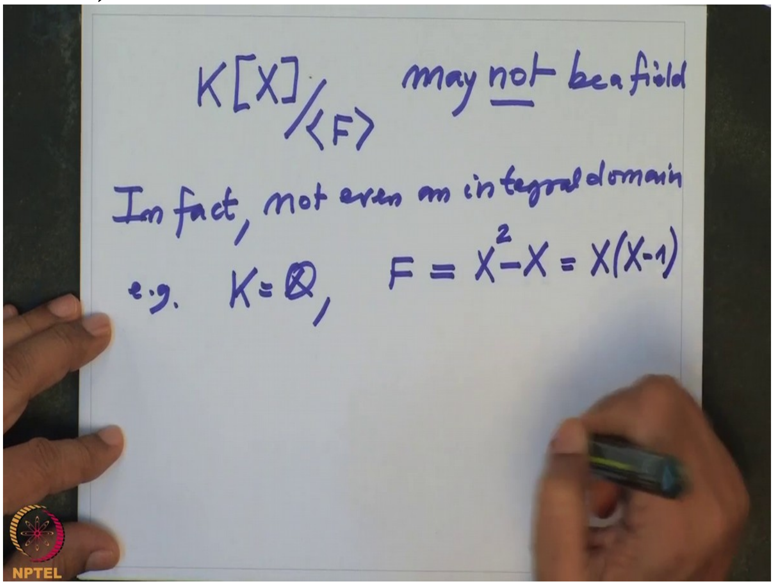
For example, for example if I take K equal to $\mathbb{Q}$ and F equal to, let us say the polynomial $X^2 - X$,

(Refer Slide Time 21:28)



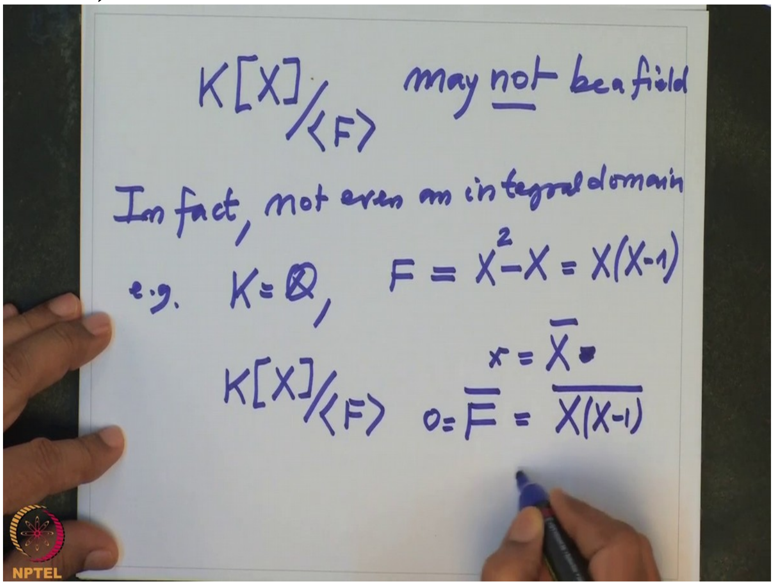
which is monic, degree is 2, so this is same as $X \times (X-1)$.

(Refer Slide Time 21:36)



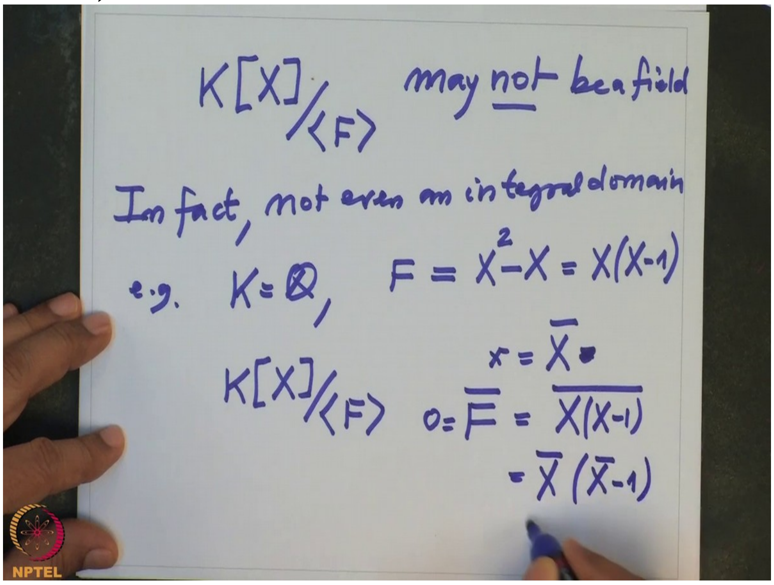
And what is, what is then, what is this $\frac{K[X]}{F}$, modulo F? In this our small x which is $\overline{X}$, and what do we know? F bar which is zero, but $\overline{F}$ is $\overline{X(X-1)}$ but

(Refer Slide Time 22:07)



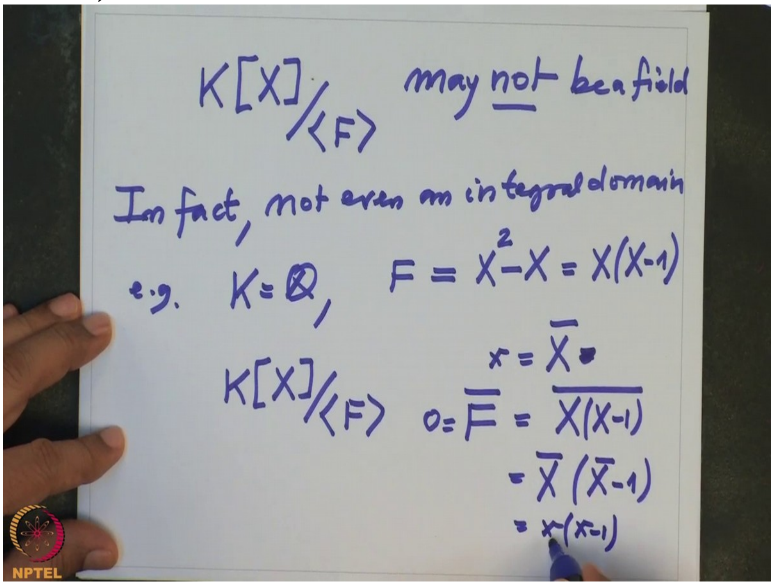
that is $\overline{X}(\overline{X}-1)$

(Refer Slide Time 22:12)



which is small $x(x-1)$,

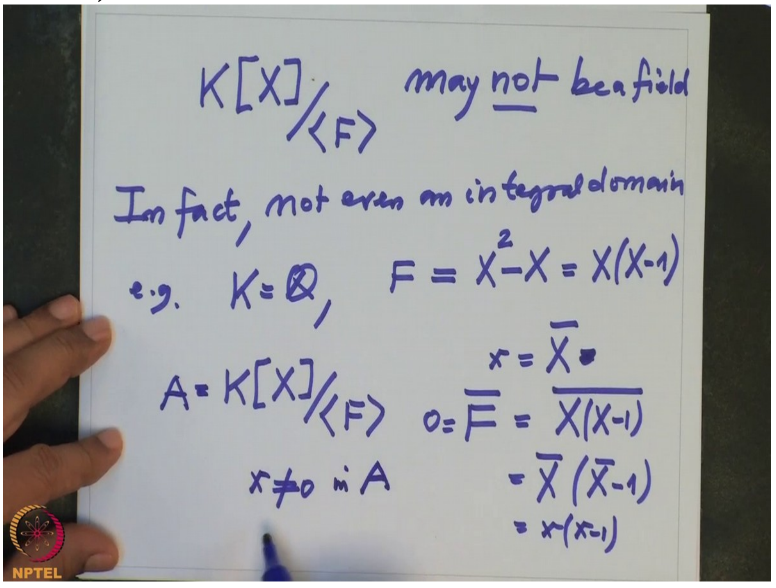
(Refer Slide Time 22:15)



so you see small $x(x-1)$ is zero but small x cannot be zero. Small x is non-zero in this.

This is our A, in A because

(Refer Slide Time 22:28)



small x is zero means what? That means F will divide X in A. But F is a monic polynomial and if F divides this X, then degree of x should be more than degree of F. But degree of x is 1, so therefore this is non-zero. So therefore it is not even an integral domain.

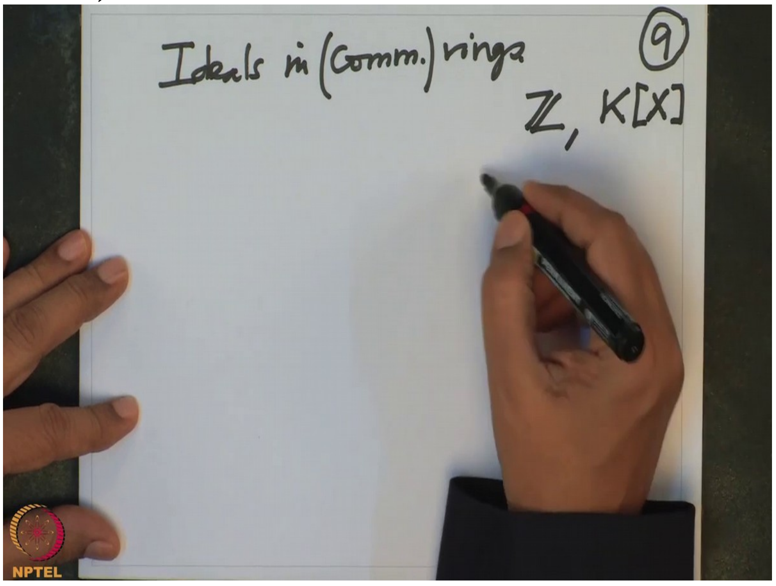
So, and also this phenomena, if you carefully observe, this is also related to being zero or not. So if a polynomial has a zero, then it will not in general be an integral domain and so on. So, to, to go little bit I want to recall now the concepts of, two concepts of ideal which will make this language more transparent as well as easier to understand.

So two things now which I will need and then I will go on to the characterization of algebraic elements, so these two concepts, so remember we have defined in general ideals in A, ideals in commutative rings.

(Refer Slide Time 23:50)

And the model examples of rings we had were $\mathbb{Z}, K[X]$. In these rings actually we have

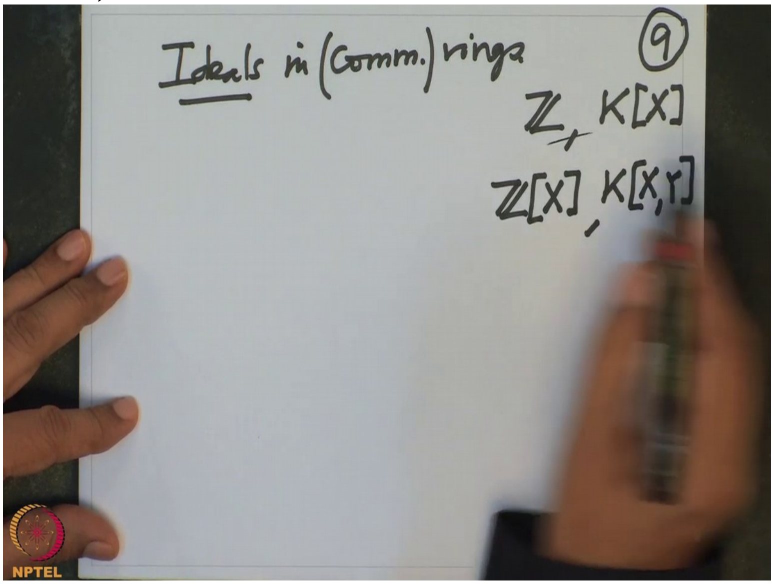
(Refer Slide Time 24:01)



all the description for all the ideals. And also we have seen the moment you take, for example ring like this, $\mathbb{Z}[X]$, polynomial ring with integer coefficients, or polynomial ring over a field but more than 1 variable.

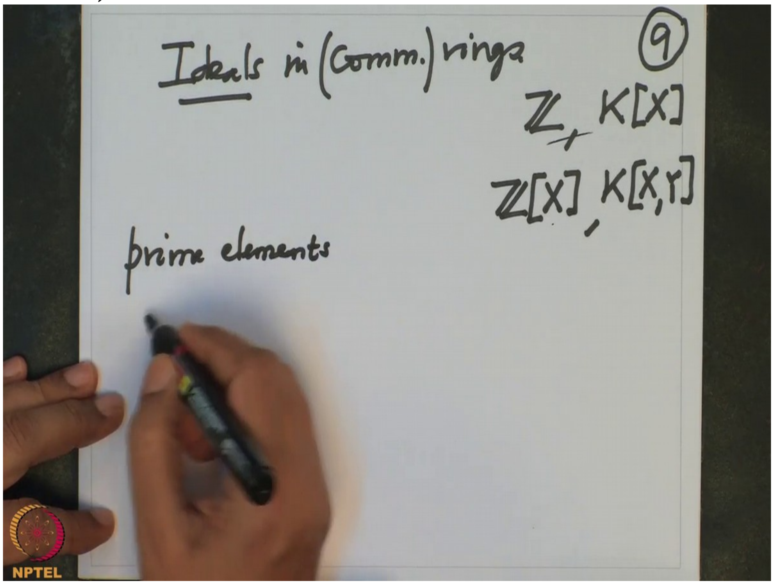
Already

(Refer Slide Time 24:22)



it is very difficult to give a structure of ideals in this rings. Because in this rings there are non-principal ideals. In this ring all ideals are principals, Ok. So corresponding to the concept prime elements

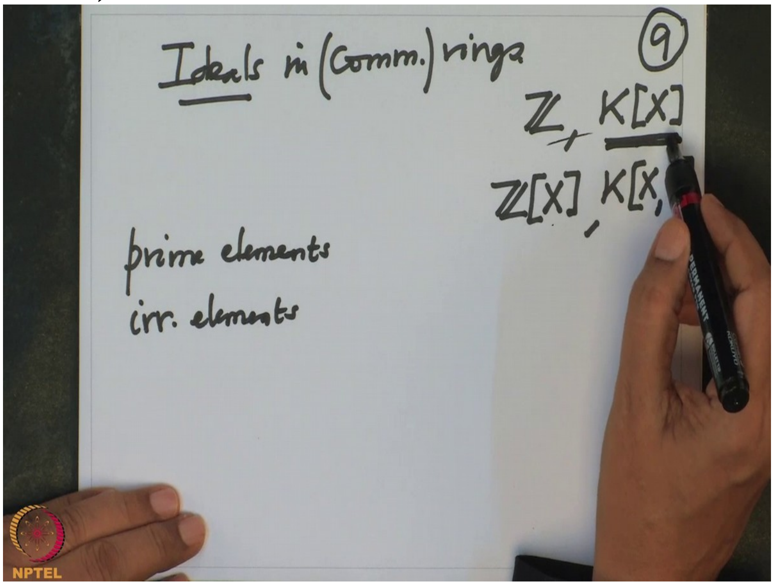
(Refer Slide Time 24:46)



or what are called irreducible elements.

See remember irreducible polynomial, we were dealing with irreducible polynomials with coefficients in a field

(Refer Slide Time 25:00)



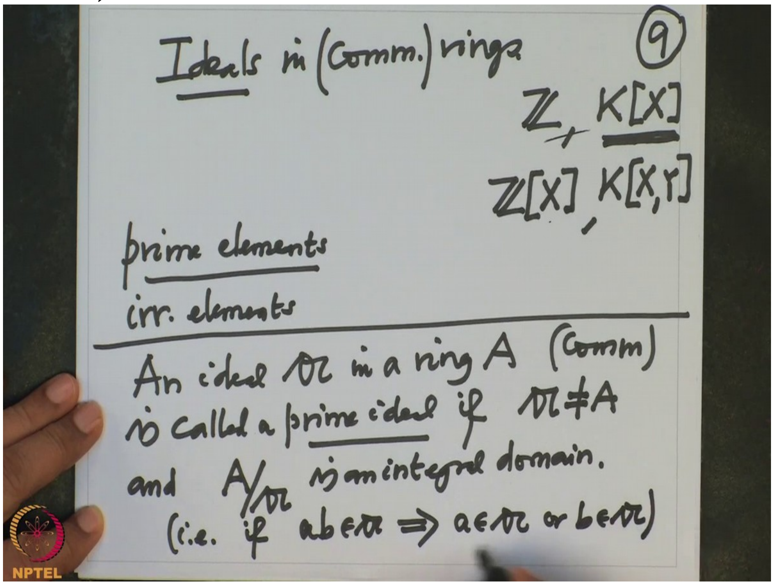
and they are the polynomials which do not have proper factors.

That means the only factors are itself and units. Units in the polynomial ring we know units are only the non-constant units. In this ring units are even much less. They are only plus minus 1. So these concepts gave rise to some ideals. These ideals are very important. So let me introduce a definition of them which are direct generalization of these prime elements.

So an ideal A in a ring, arbitrary ring commutative, commutative always is called prime ideal, is called a prime ideal if, first of all that A, ideal A should not be the whole ring A and modulo that, that means the residue class ring A modulo A is an integral domain. So the last condition is very easy to check.

That is equivalently, if a product a times b belongs to ideal A, then one of them should belong to A, either a will be in A or b will be in A.

(Refer Slide Time 26:39)

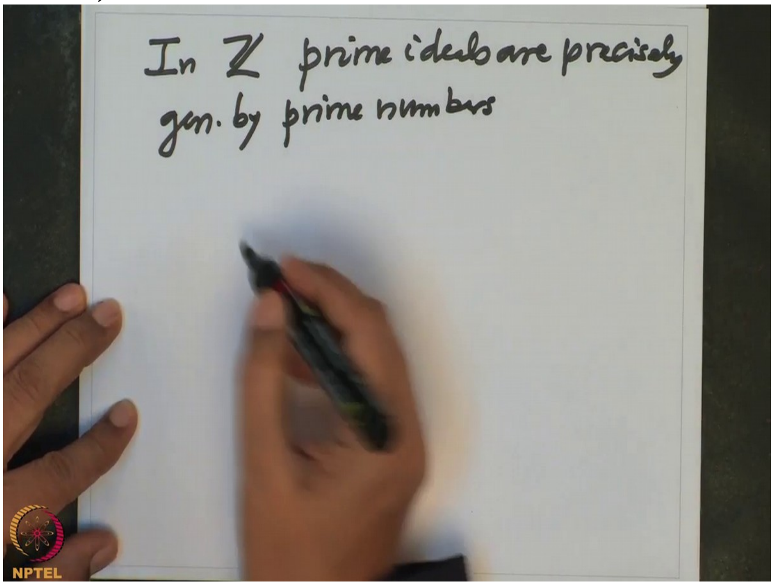


So this is actually the correct definition of prime element also.

An element is called prime if a P divides the product then it divides one of them. Because divisibility condition is replaced by belongs to in case of ideals.

So that those are necessarily the prime ideals. And the easy example, the first example of prime ideals in the ring $\mathbb{Z}$, in $\mathbb{Z}$, prime ideals are precisely, are precisely generated by prime numbers, prime numbers. This is just the restatement of the definition.

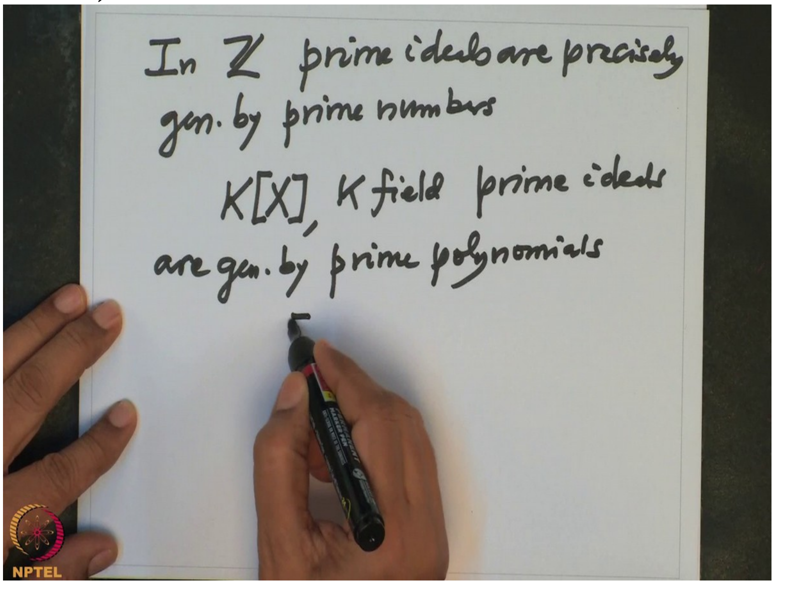
(Refer Slide Time 27:27)



Similarly in the ring, polynomial ring over a field, arbitrary field they are precisely prime ideals here, ideals are generated by prime polynomials.

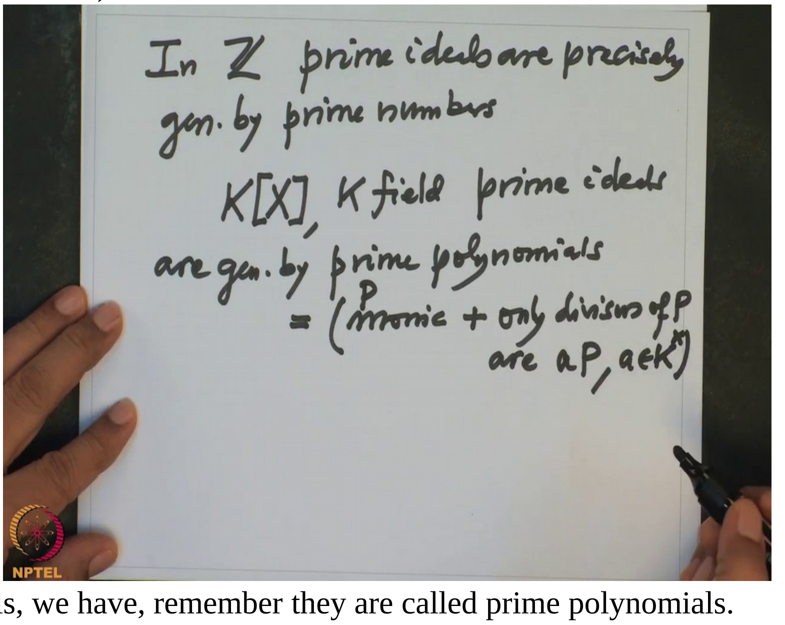
Now what are the prime polynomials? Just let me recall.

(Refer Slide Time 27:54)



Prime polynomials are monic and only factors are, only divisors are, a polynomial P is called prime if P is monic and only divisors of P are some constant multiples of P where A is a non-zero constant in the field.

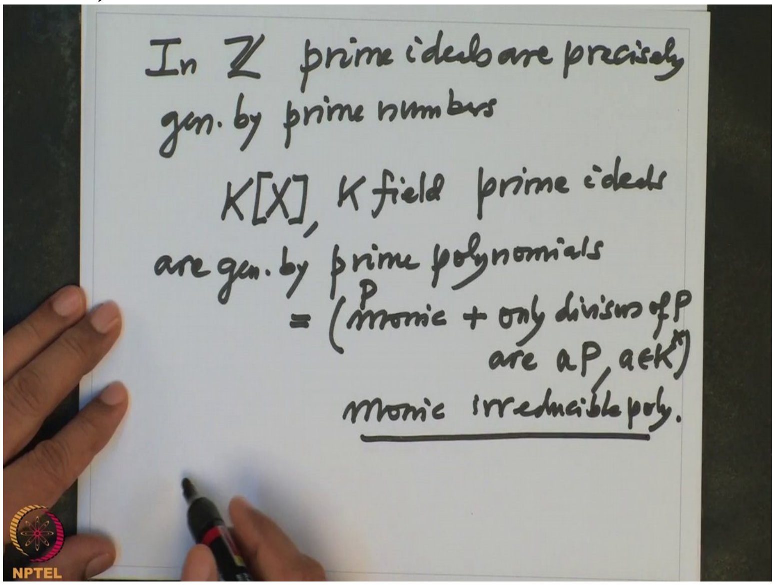
(Refer Slide Time 28:24)



Such polynomials, we have, remember they are called prime polynomials.

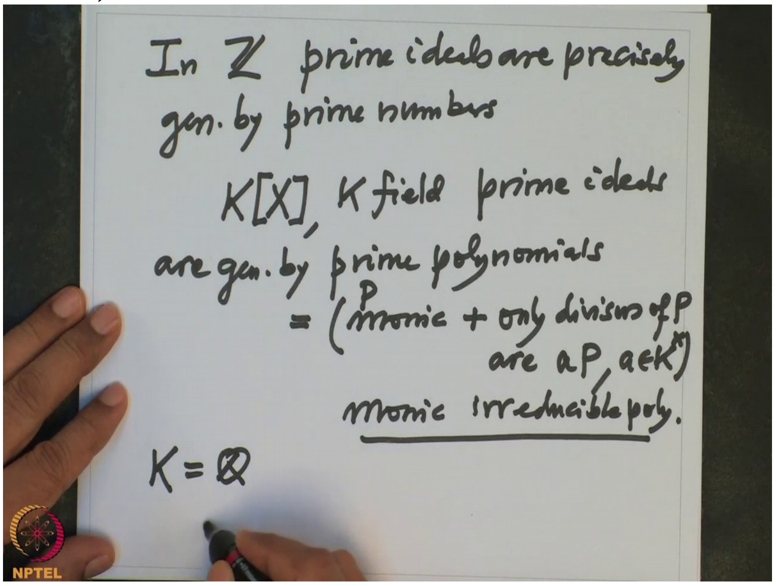
In other words, they are irreducible polynomials, monic irreducible polynomials. So they are monic, irreducible polynomials. And we have described,

(Refer Slide Time 28:43)



we know that if K equal to ℚ there are enough of them, in fact given any n,

(Refer Slide Time 28:52)



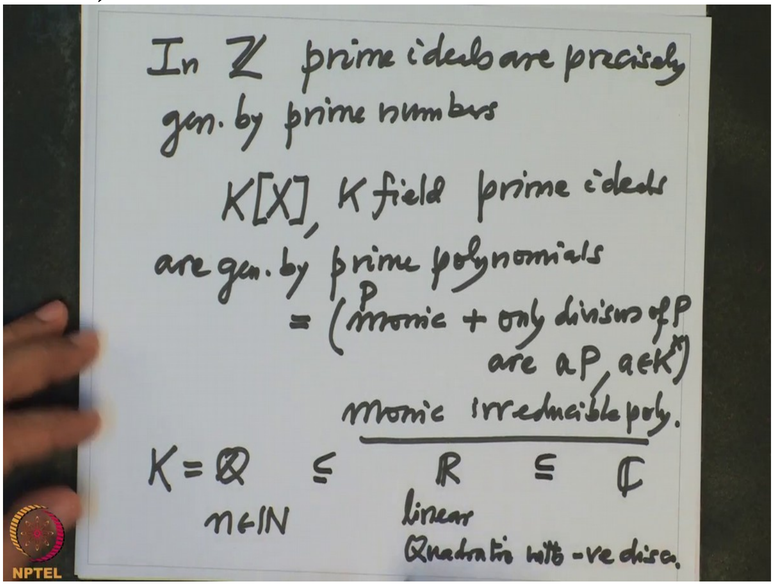
there are many, many polynomials of degree n over ℚ which are irreducible and, but over ℝ they are fewer.

Over ℝ the only polynomials are linear ones, linear there is degree 1 polynomial and quadratic, quadratic with the, with negative discriminant, whatever it is.

And over ℂ we only want to prove that the only prime polynomials are the linear ones, and this is precisely the restatement of fundamental theorem of algebra, which we have not proved it but we will prove it soon.

So

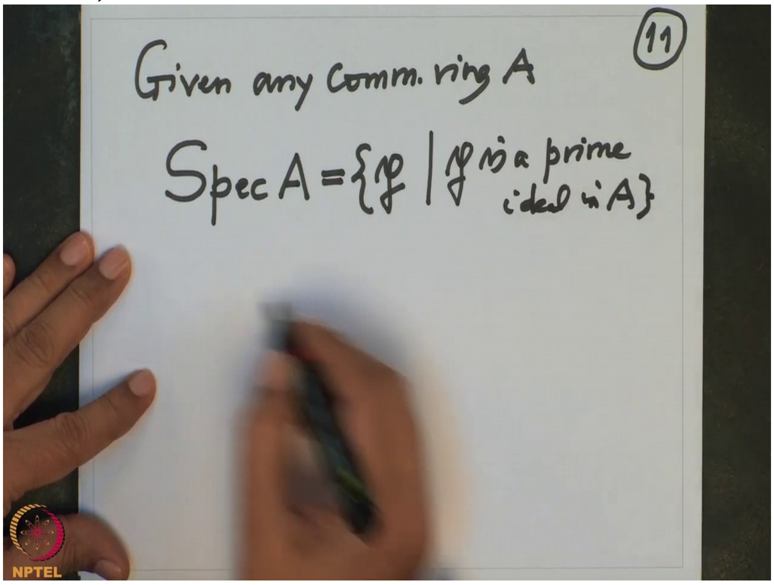
(Refer Slide Time 29:41)



this is what the prime ideals are very important and in general we know in these rings there are prime ideals but in general we do not even know that off-hand that given any commutative ring there is a prime ideal.

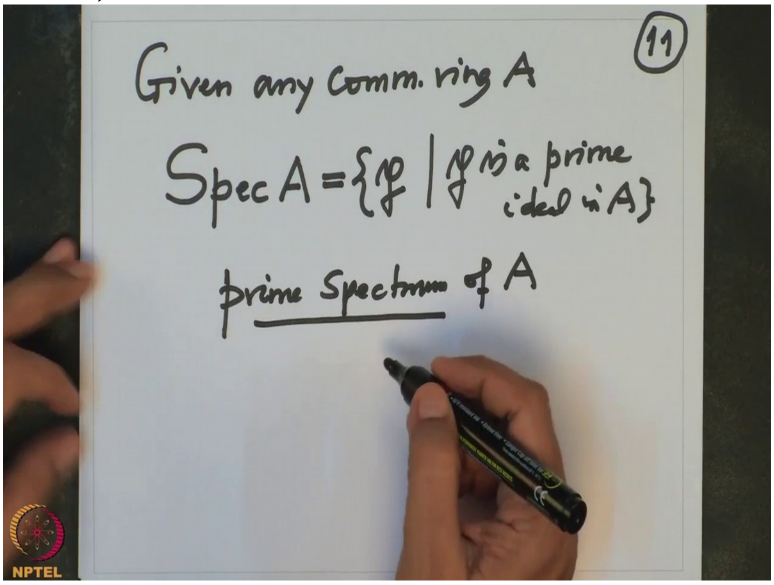
So let me just state it. We will not use much about this but it is very important. So given any ring, commutative ring R, given any commutative ring A, the set of prime ideals I am denoting by Spec A, this is the set of all P, P is now Gothic P such that P is a prime ideal in A. This set

(Refer Slide Time 30:39)



is called prime spectrum of A. This is one of the principal

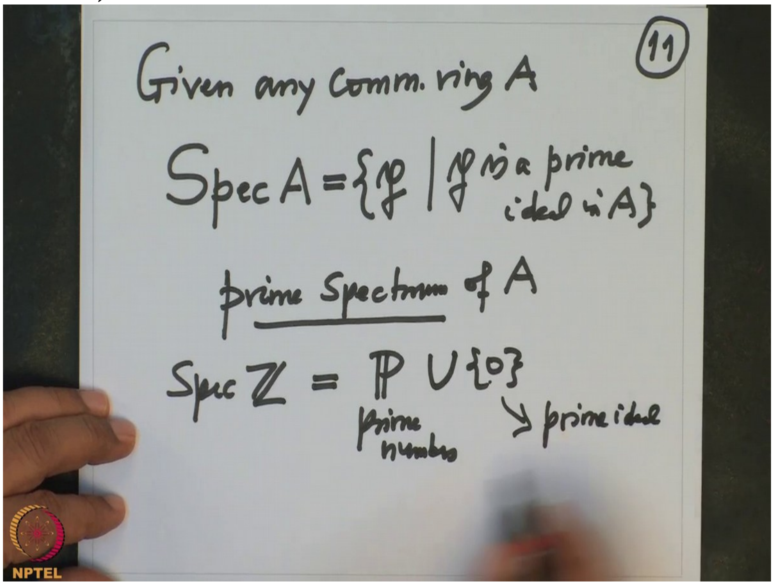
(Refer Slide Time 30:51)



objectives to study in modern algebraic geometry.

So for example, Spec of $\mathbb{Z}$, this is precisely the set of prime numbers and there is only one more prime ideal in $\mathbb{Z}$ besides prime number and that is generated by zero, that is a zero ideal. Zero ideal is prime in $\mathbb{Z}$ because $\mathbb{Z}$ is an integer domain. So this is also prime ideal.

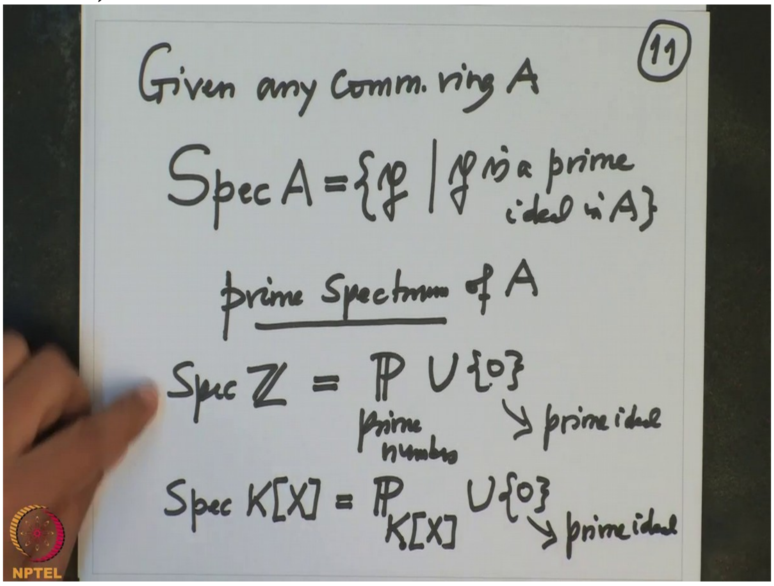
(Refer Slide Time 31:25)



Similarly for, this same thing we go for polynomial ring in one variable over a field K that is the set of prime polynomials in $K[X]$, I use the same notation, now I introduce the suffix here that indicates that they are prime polynomials in this, union 0, 0 is the, the polynomial 0 is also prime ideal in K because modulo that it is an integer domain so this is also a prime ideal.

So these,

(Refer Slide Time 31:58)



these are both, these are infinite sets. But in general it is not clear whether given a ring has a prime ideal or not, but that is very easy because one studies instead of even the special classes of ideals, for maximal ideals and that maximal ideals, one proves, there is a theorem of Krull which says that given any commutative ring there is definitely a non-zero maximum ideal and maximum ideals are prime etc.

So this will give enough flow of prime ideals in a ring to go on our study more and more. This was necessary to introduce because I will want to use some of these modern language in the next exposition.

And remember again, about the course, this course, though it is very historically, very ancient course I want to use modern methods to give classical proofs and that will lead us to more far-reaching concepts and proofs and

(Refer Slide Time 33:06)

it will open up the subject and it is still active area of research in mathematics which has tremendously many applications in the other fields. With this I will stop.