Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 12
Kernel of homomorphisms and ideals in K[X],Z

(Refer Slide Time 00:26)

Alright, so in few minutes back we saw ring homomorphisms, algebra homomorphisms, examples and so on. Now let us continue little bit more. In

(Refer Slide Time 00:40)

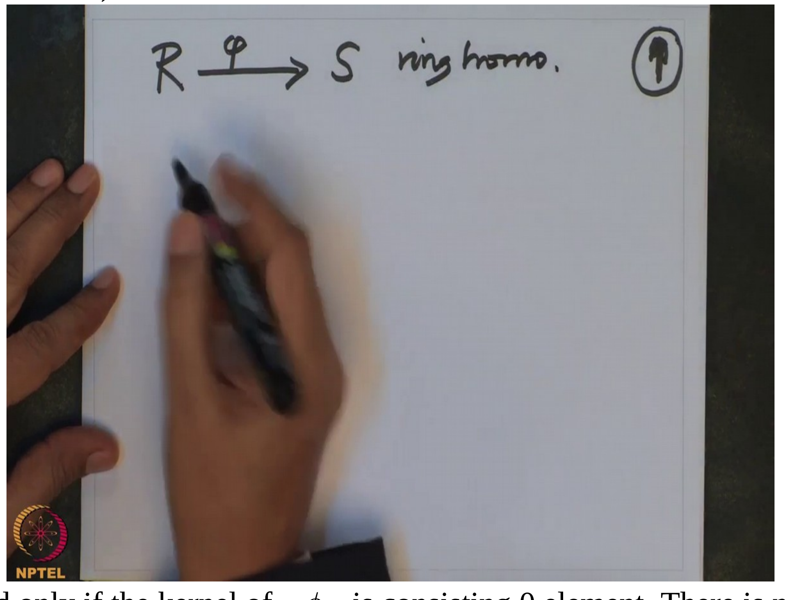
group theory one studies now how do you get an isomorphism from a given group homomorphism?

How do you test a given group homomorphism is injective or surjective, and such corresponding things for the ring homomorphisms or K-algebra homomorphisms I am going to state only and the proofs I will leave it to the participants.

They are exactly along the same lines as one do in a Group Theory. So for example, so when do we say, that how do you test that given ring homomorphism R to S, ring homomorphism ϕ injective? So ϕ is injective if and only if the kernel ϕ which is by definition, all those elements of the ring are, which are mapped to 0, that is $\phi(x)=0$.

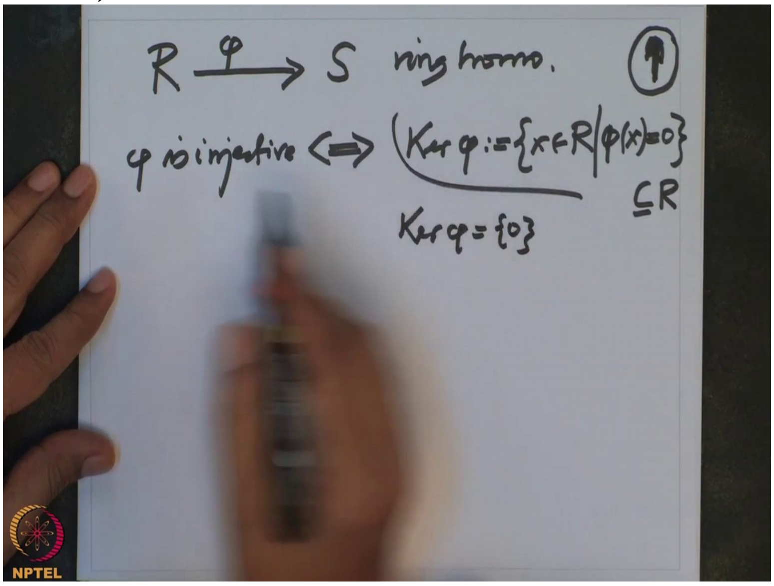
So this is a subset of R and it is not just a subset, it has some more properties. I will come in a minute, so ϕ

(Refer Slide Time 01:31)



is injective if and only if the kernel of ϕ is consisting 0 element. There is no

(Refer Slide Time 02:22)

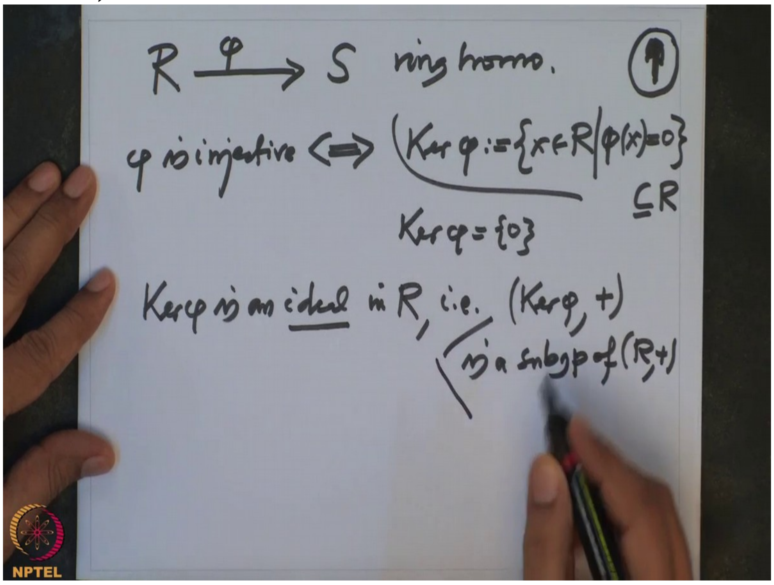


non-zero element of R goes to 0 under ϕ, then ϕ is injective.

Now what are the more properties, what are the more properties of this kernel? That it is an ideal, kernel ϕ is an ideal in R. So now I have used this word, new word, ideal in R, so that simply means that is first of all, under addition it is a subgroup. So kernel ϕ under addition is a subgroup of R, (R ,+) that is one

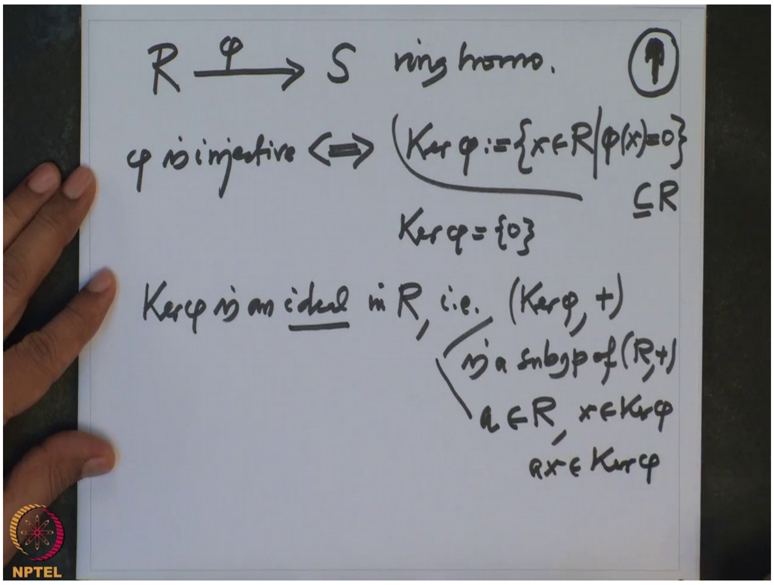
And another property is

(Refer Slide Time 03:05)



if I have arbitrary element a in the ring R and x in the kernel, then $a\,x$ is also in the kernel.

(Refer Slide Time 03:20)

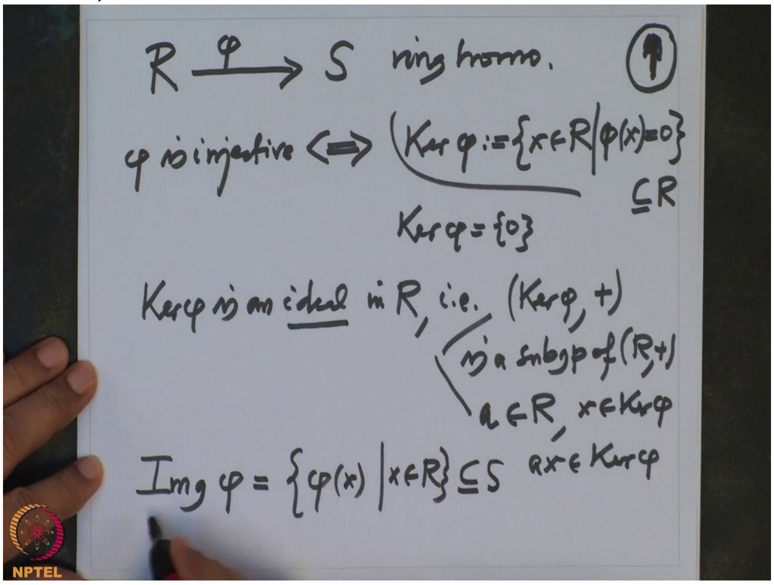


And because we have in a commutative ring, we are not going to be bothered about left ideal, right ideal and so on. Similarly here only it is enough that we multiply on the left. So it is better that we assume now rings are commutative always. Ok that is an ideal.

I will soon give examples of ideals in some rings. And like injectivity how do you test the surjectivity? It is easy. That as usual, for map between the two sets we denote image of ϕ to be all those elements $\phi(x)$ as x varies in R. Take all the elements of R and take all their images. This is the subset of S which is called the image of S.

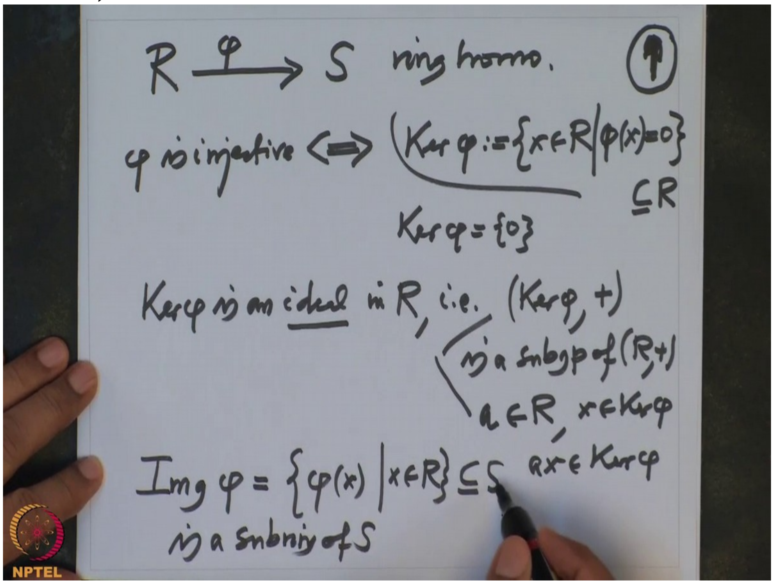
And note that this is a sub-ring of

(Refer Slide Time 04:16)



S. So let me remind you sub-ring means

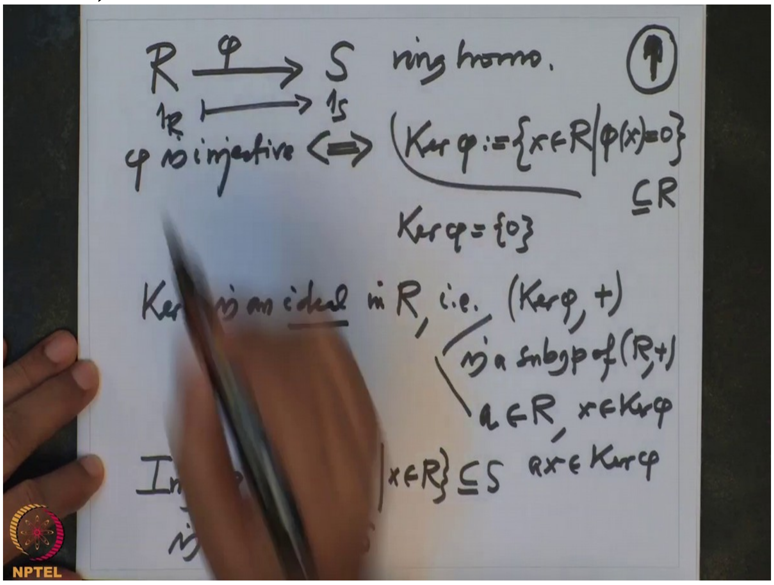
(Refer Slide Time 04:29)



with respect to the same binary operations, plus and multiplication of S, this subset induces, induced on this subset is also a ring. And in particular that 1 also belongs here. So for that, let me remind you because our assumption is very important. 1_R goes to 1_S .

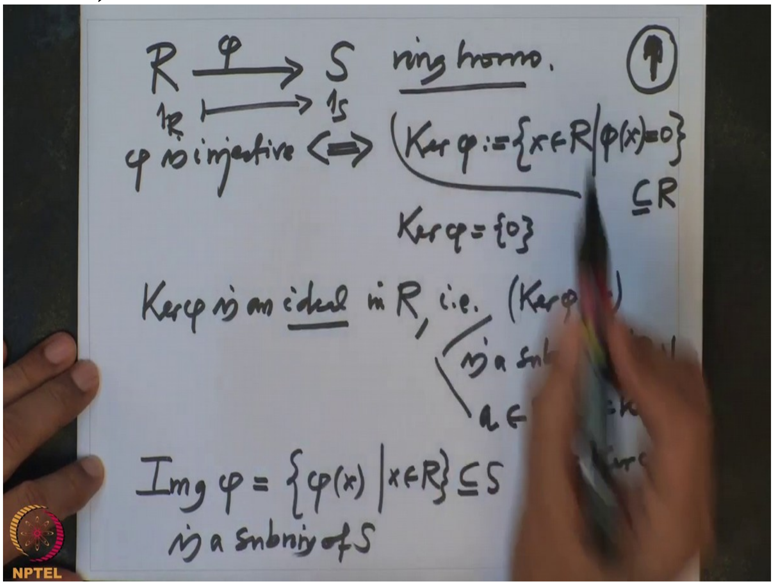
So that means

(Refer Slide Time 04:52)



1_S is in the image. So 1_S belongs here and the remaining properties are just followed from the fact that it is a ring homomorphism,

(Refer Slide Time 04:59)

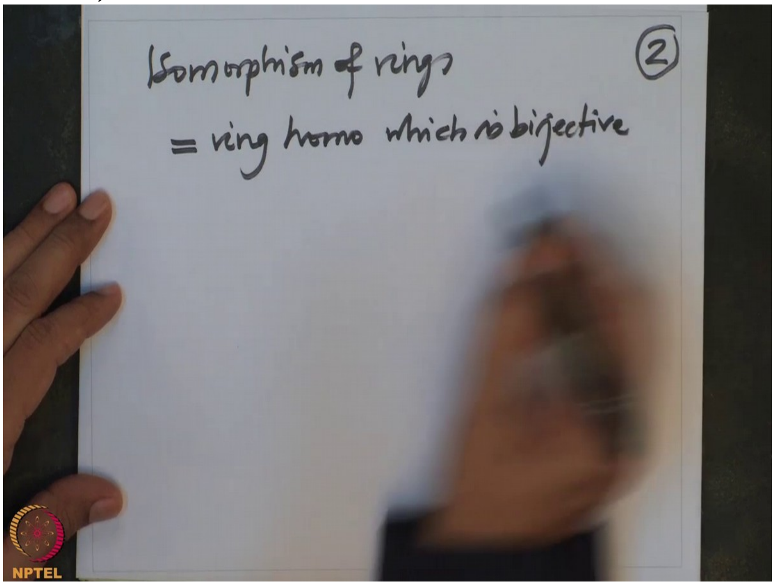


that is all. So if you, if you want to, and what is the isomorphism of the ring? Isomorphism of the rings, of ring that means

(Refer Slide Time 05:18)

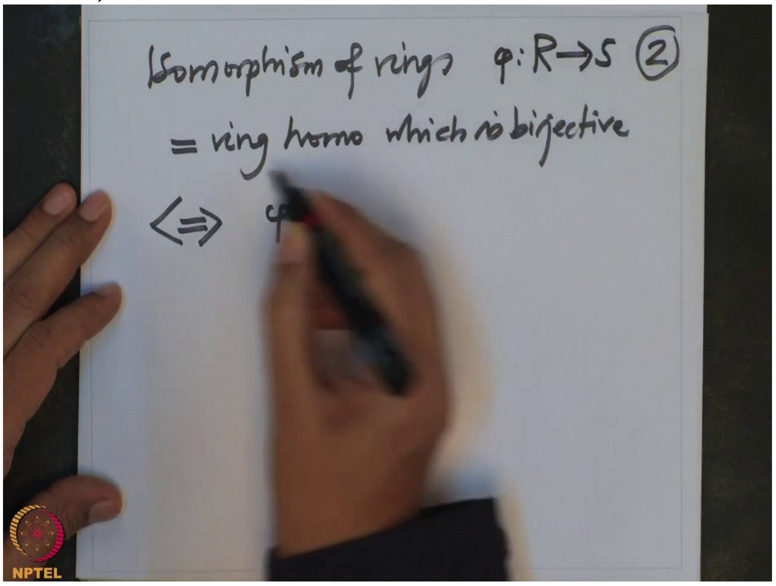
ring homomorphism which is bijective.

(Refer Slide Time 05:33)



This is equivalent to saying that ϕ ; so isomorphism ϕ from R to S is a

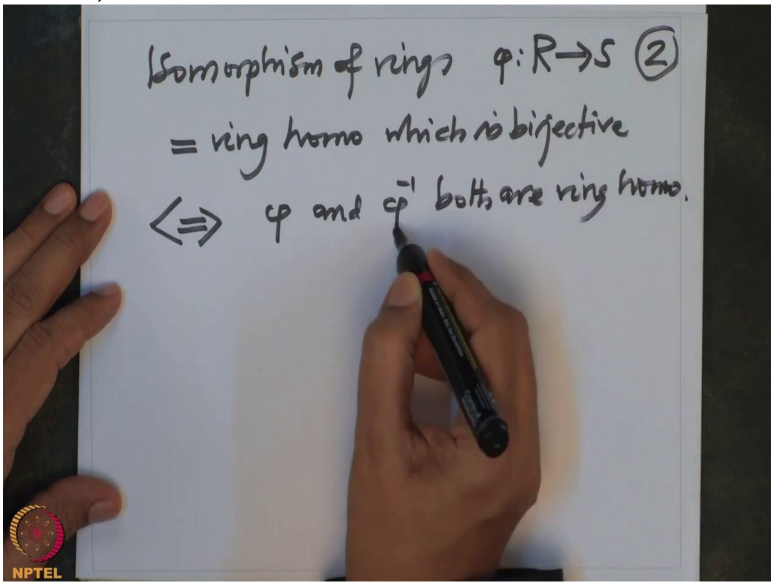
(Refer Slide Time 05:45)



ring homomorphism which is bijective.

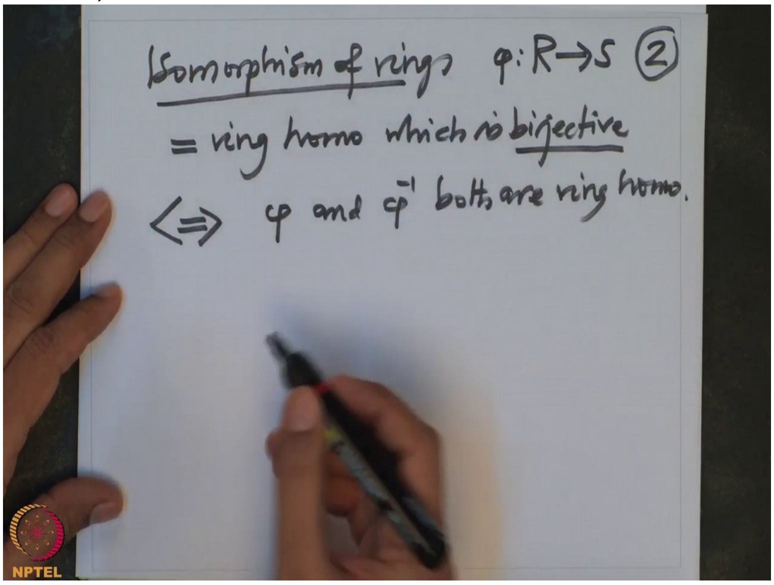
That means ϕ and ϕ inverse both are ring homomorphisms.

(Refer Slide Time 05:57)



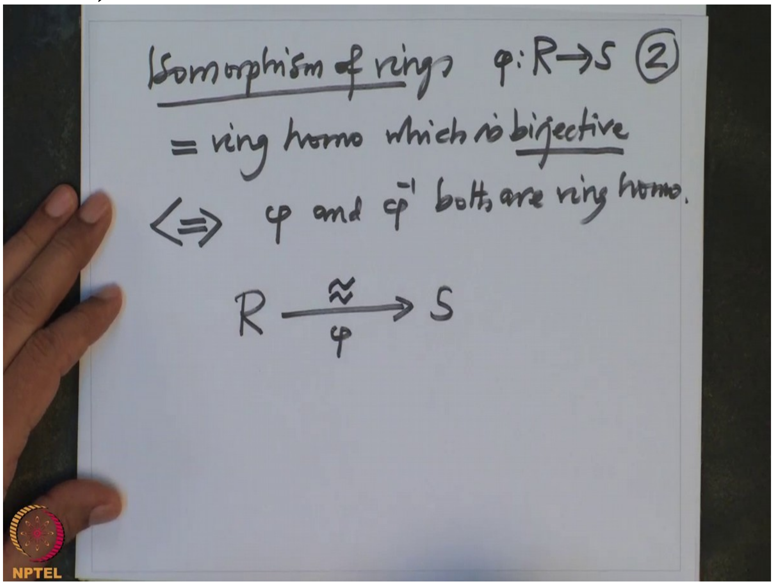
Remember because of this bijectivity ϕ inverse makes sense and both are ring homomorphisms. Then one says it is an isomorphism. And

(Refer Slide Time 06:06)



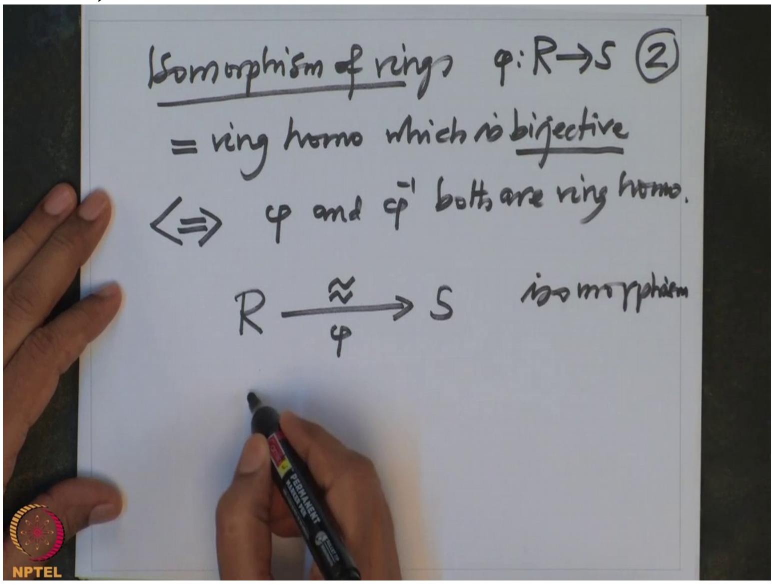
this is usually denoted by R to S ϕ and to show that it is bijective, it is

(Refer Slide Time 06:13)



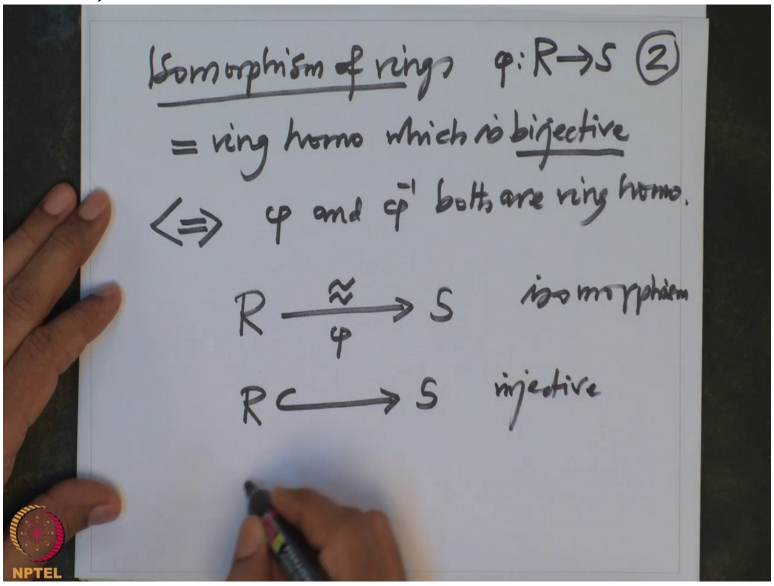
denoted like this. So this is a typical notation one will use for the isomorphism of the rings. And

(Refer Slide Time 06:22)



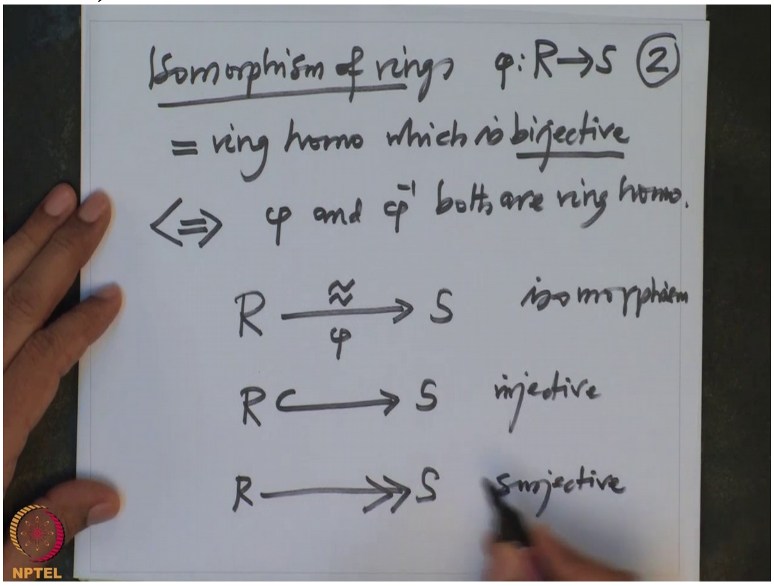
for injectivity normally one writes R hook arrow S, so this means injectivity

(Refer Slide Time 06:34)



and R to S surjectivity is denoted by putting 2 arrows. This is surjectivity. This is the standard notation we will adopt

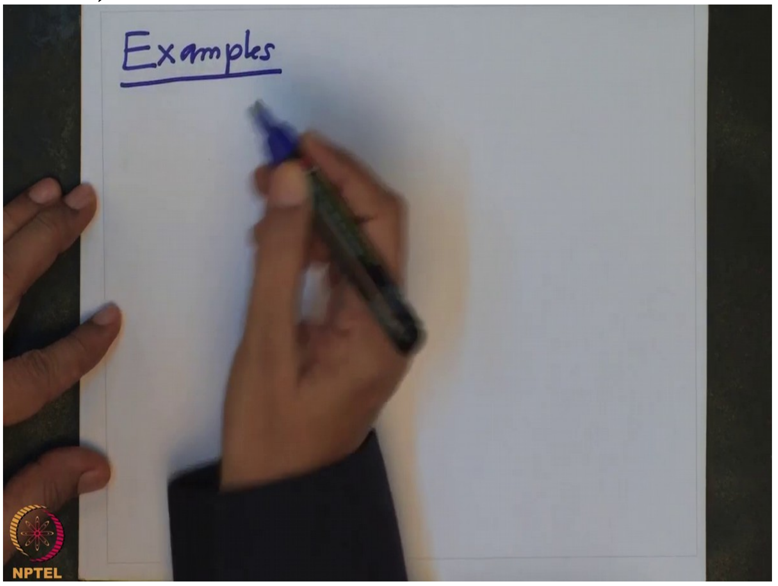
(Refer Slide Time 06:44)



in this course. So now let us see some examples of ring ideal isomorphisms and so on.

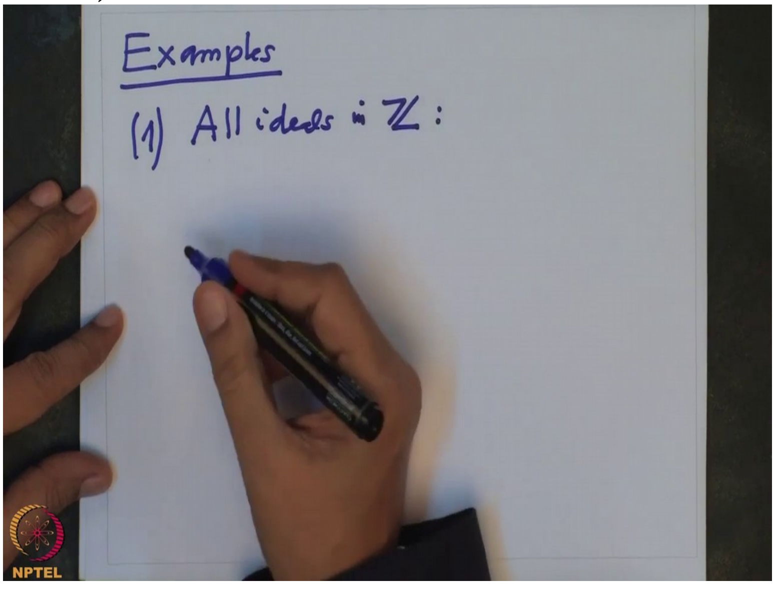
So,

(Refer Slide Time 07:11)



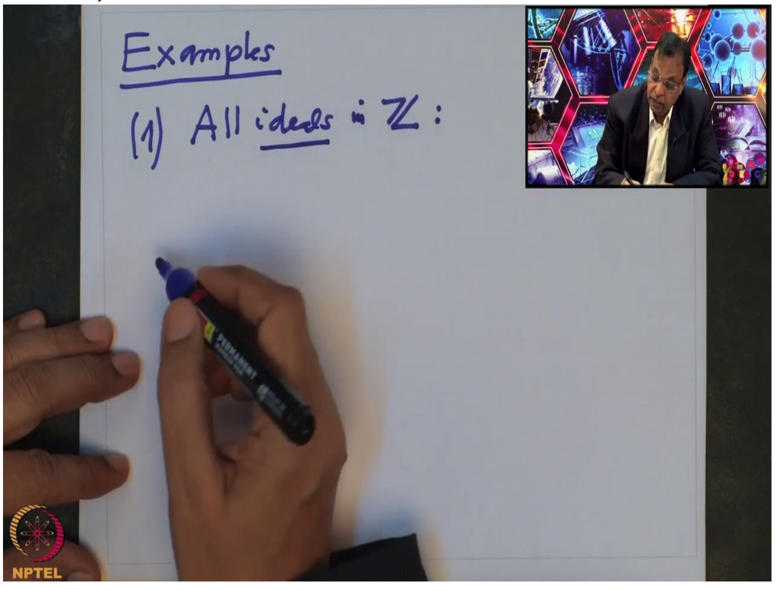
so first of all I want to give some examples where you can describe the ideals. So first, one can describe all ideals in $\mathbb{Z}$.

(Refer Slide Time 07:21)



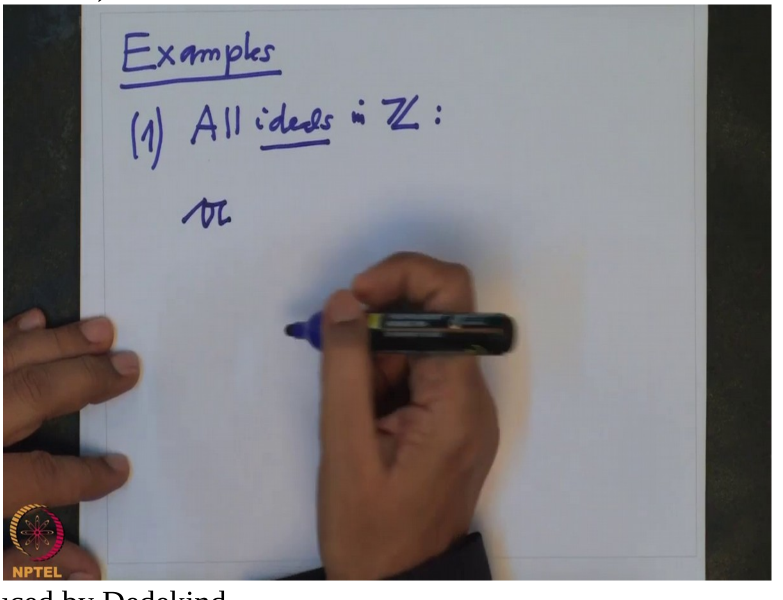
So how do you do that? So take any, the ideals

(Refer Slide Time 07:27)



they are usually denoted by the Gothic letters A, B, C etc.

(Refer Slide Time 07:31)

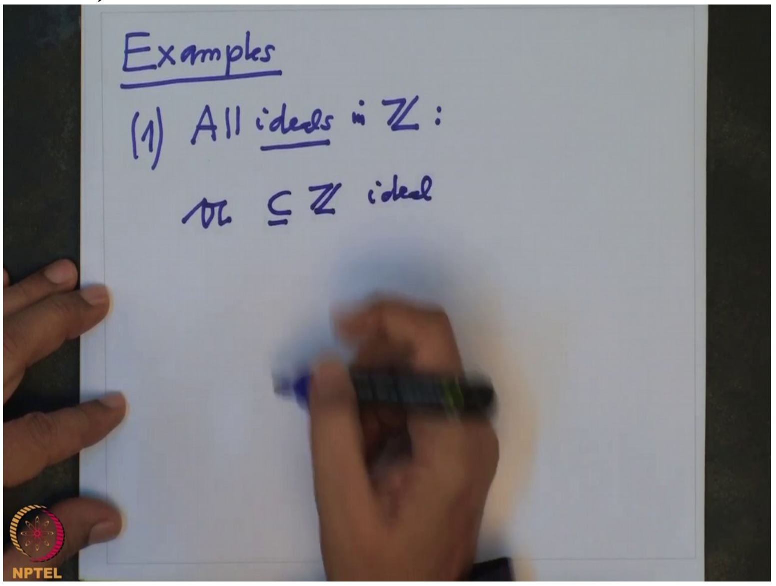


These are introduced by Dedekind.

Dedekind was a German mathematician and therefore he used German letters which are, which is, which are Gothic letters to denote ideals in the rings.

So suppose A is an ideal in $\mathbb{Z}$.

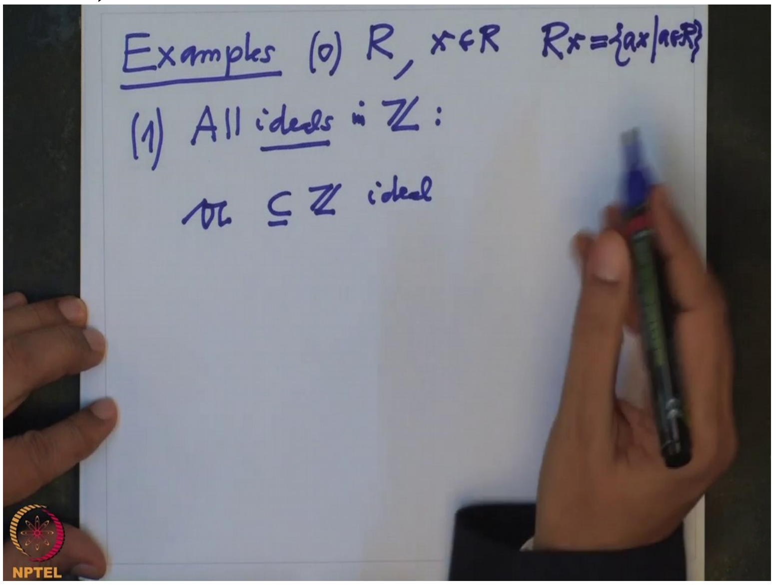
(Refer Slide Time 07:54)



Then I want to show that it is generated by a single element. What does that mean? First of all, before I started this, I should have given examples in arbitrary ring. So let us take R be any ring and x be any element in R.

Then if I take all multiples of this x, R multiples of x that obviously I would denote by R times x. This is by definition, all ax where a is varying in R.

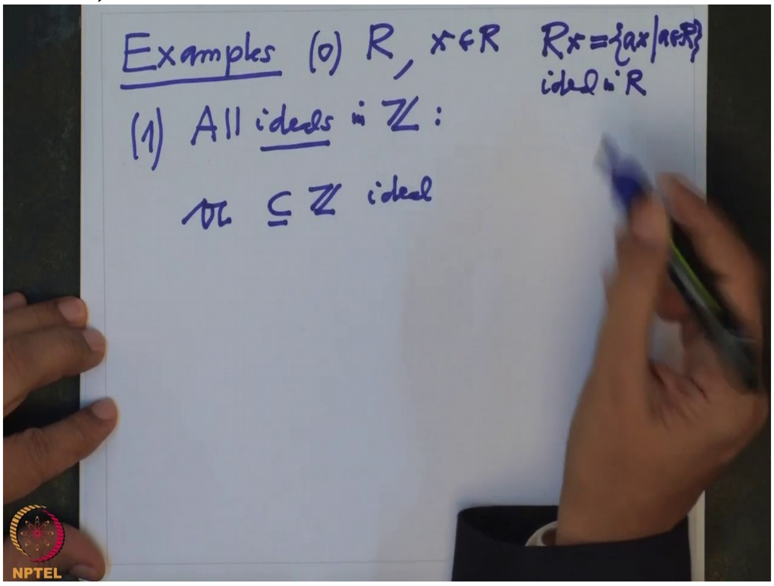
(Refer Slide Time 08:28)



And I want to check that this is an ideal in R.

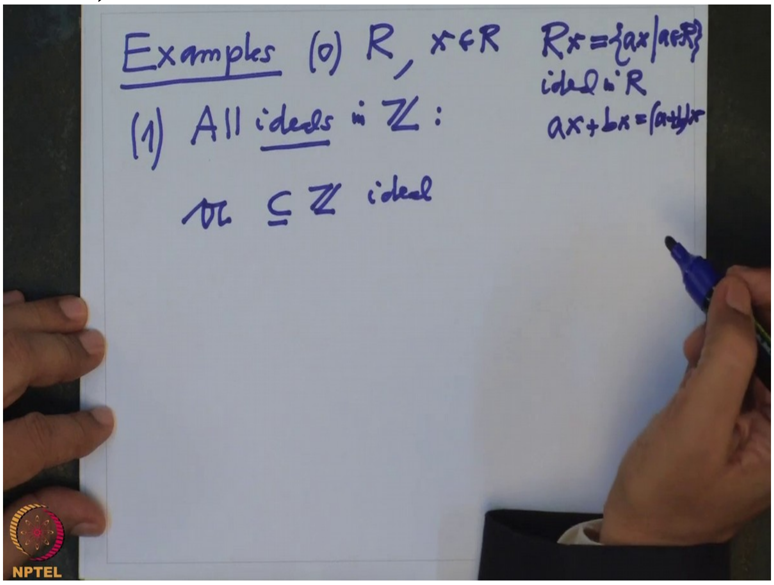
And

(Refer Slide Time 08:36)



how do I check that? So I have to check that it is an subgroup under addition, which is clear. Because if I take 2 elements like this, $ax+bx$, then because of our rules this is nothing but a plus b when I add first and then multiply.

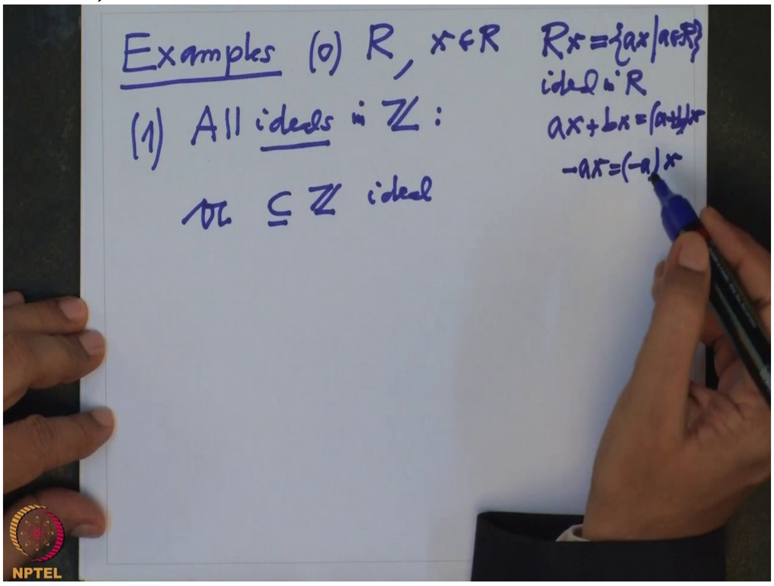
(Refer Slide Time 08:53)



So therefore it is again a multiple of x. So it is closed under addition.

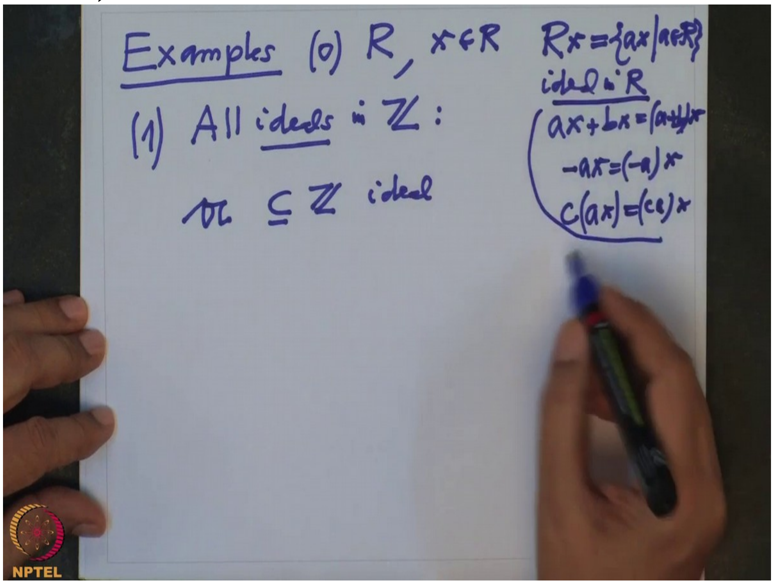
Similarly it is closed under sub, negation because minus of a x is same as minus a into x.

(Refer Slide Time 09:10)



So it is a subgroup. And it is clearly closed under scalar multiplication of R because if I take c times a x it is same c a times x. So what we have checked is this is an ideal in R. This ideal is called principal ideal generated by x,

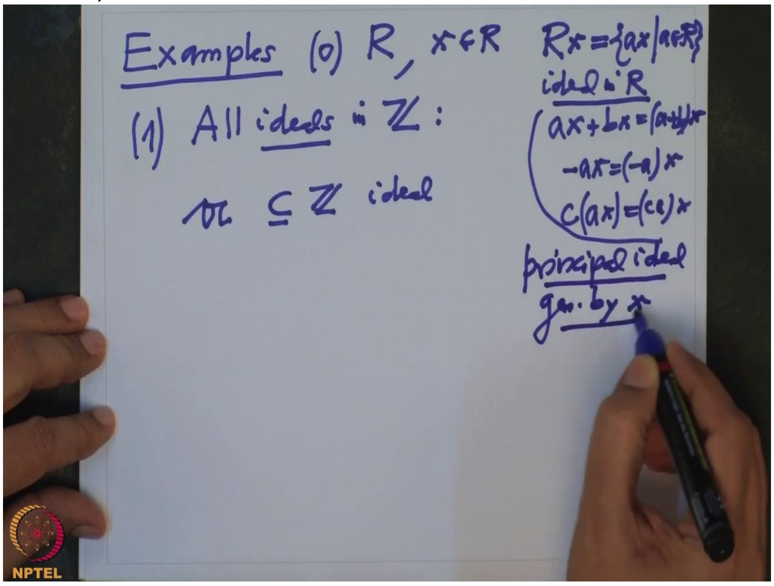
(Refer Slide Time 09:29)



principal ideal generated by x.

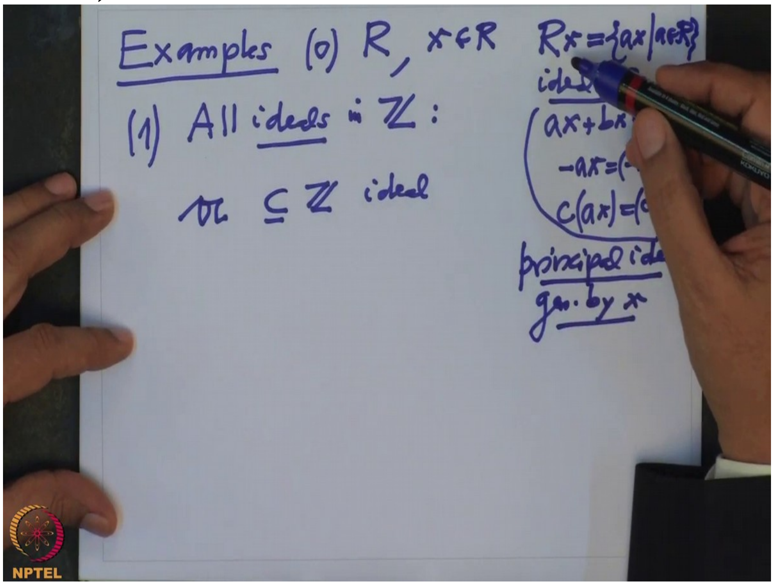
And note that this x

(Refer Slide Time 09:41)



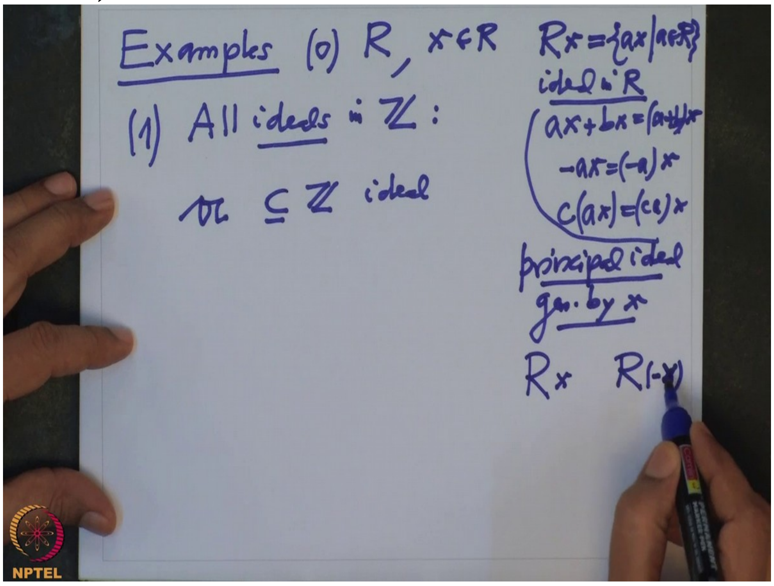
may not, this x may not be uniquely determined

(Refer Slide Time 09:46)



by this ideal, if you give the ideal then you cannot, you need not get back x. For example minus x is also generating in the same ideal. So Rx is same as $R(-x)$. Remember, this means all R multiples of $-x$,

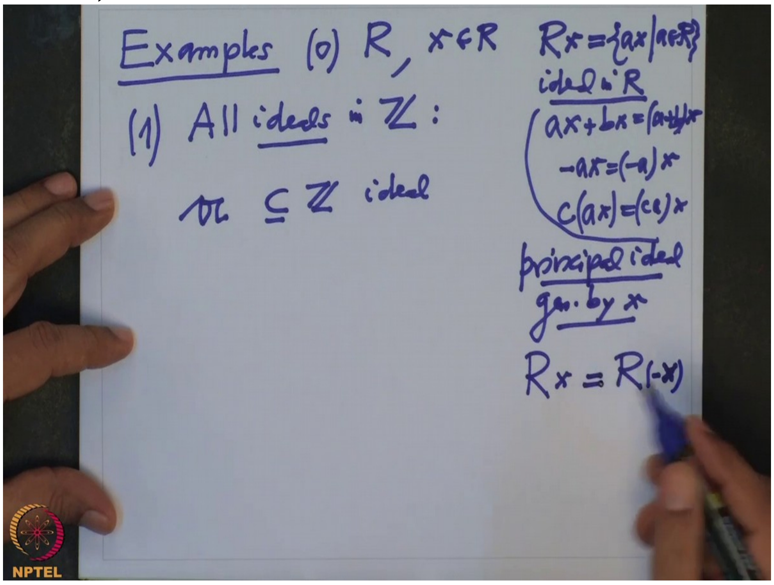
(Refer Slide Time 10:09)



minus x is a additive inverse of x. So these two ideals are same.

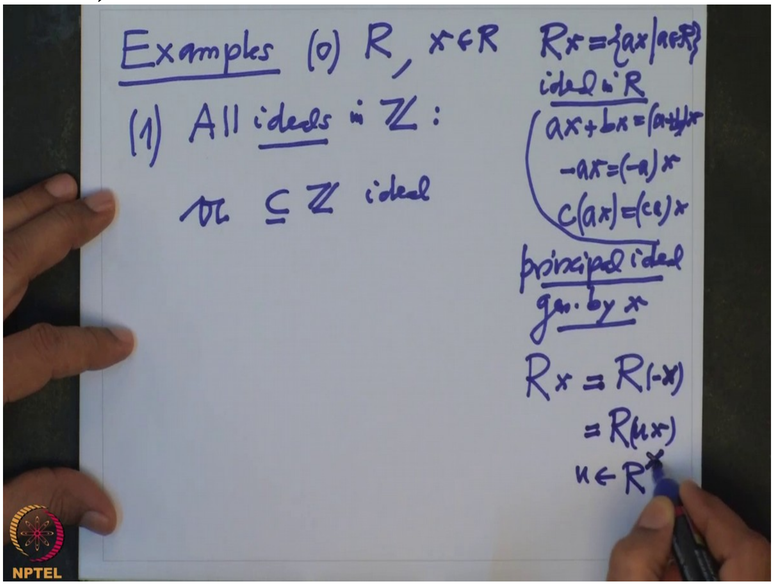
So therefore

(Refer Slide Time 10:15)



in particular, not only this, in particular also, this is also same as R times, R multiples of any ux, where u is a unit in R. Remember we had notations for units in R.

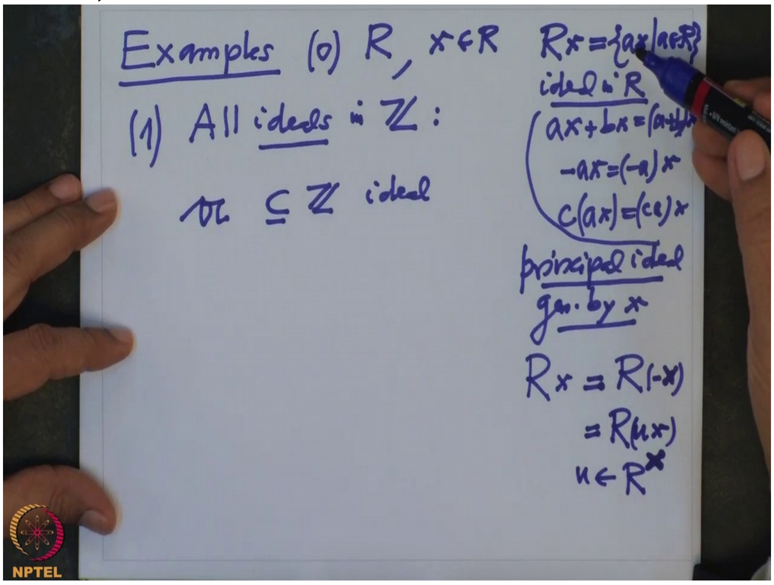
(Refer Slide Time 10:33)



These are set of al invertible elements with respect to multiplication.

So these 2 ideals are, so u and, x and u x generate the same ideal. So you cannot

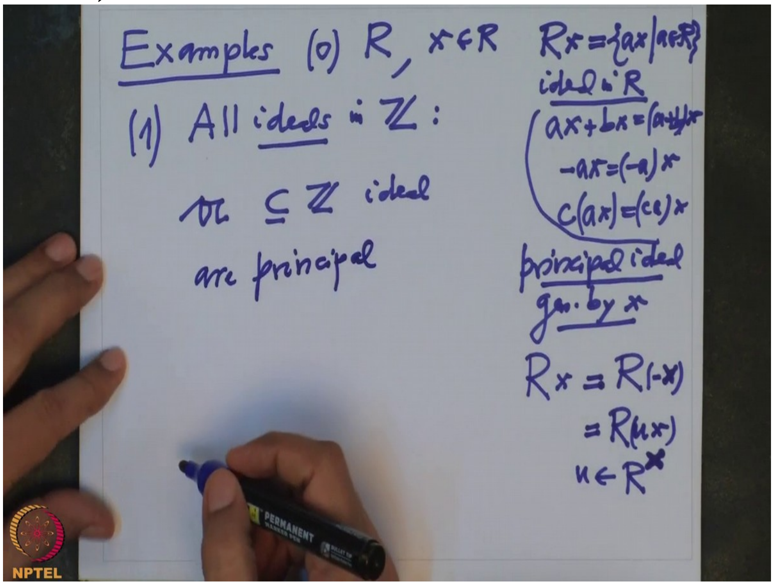
(Refer Slide Time 10:45)



recover a generator from an ideal. But if it is generated by single element then one calls it a principal ideal generated by x. And the first statement I wanted to make that all ideals in $\mathbb{Z}$ are principal.

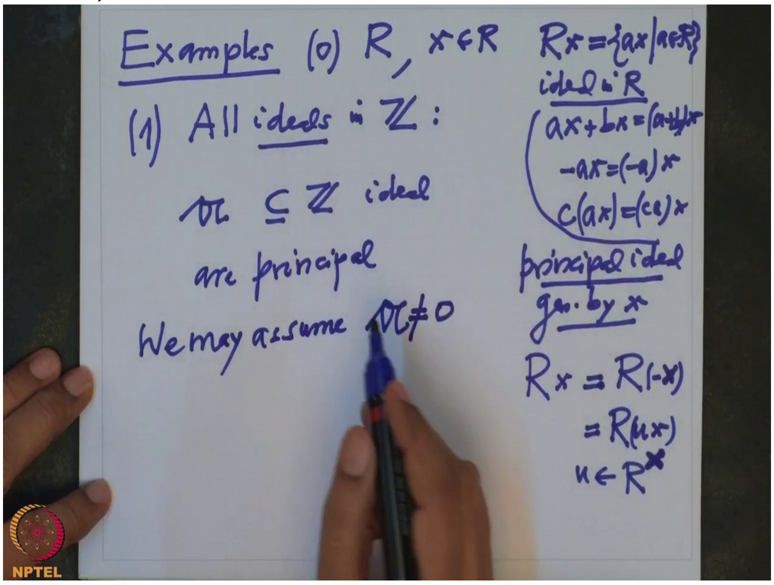
So we have a good knowledge of ideals in the ring $\mathbb{Z}$.

(Refer Slide Time 11:06)



And how do you check this? The important tool to check this is what we have mentioned earlier the division with remainder. So to prove it is principal, we may assume A is 0, non-zero because A is a 0, 0 is always

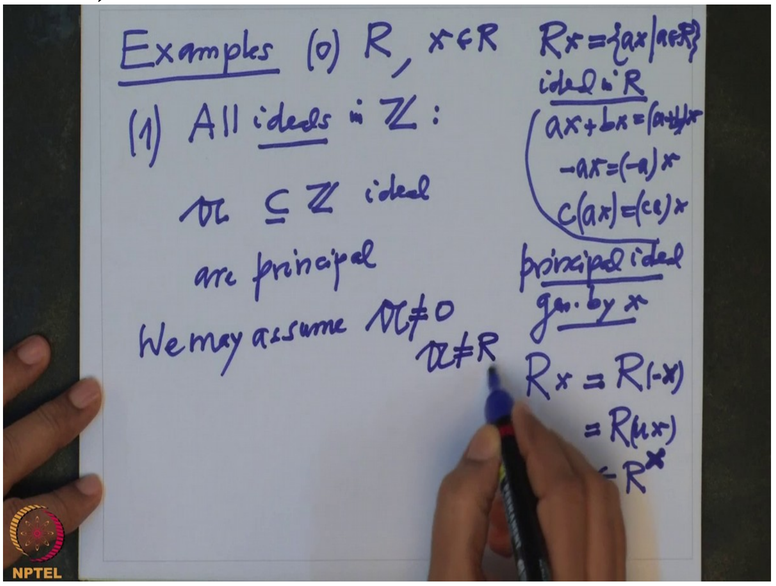
(Refer Slide Time 11:33)



an ideal in a ring, and it is clearly generated by 0. So it is principal.

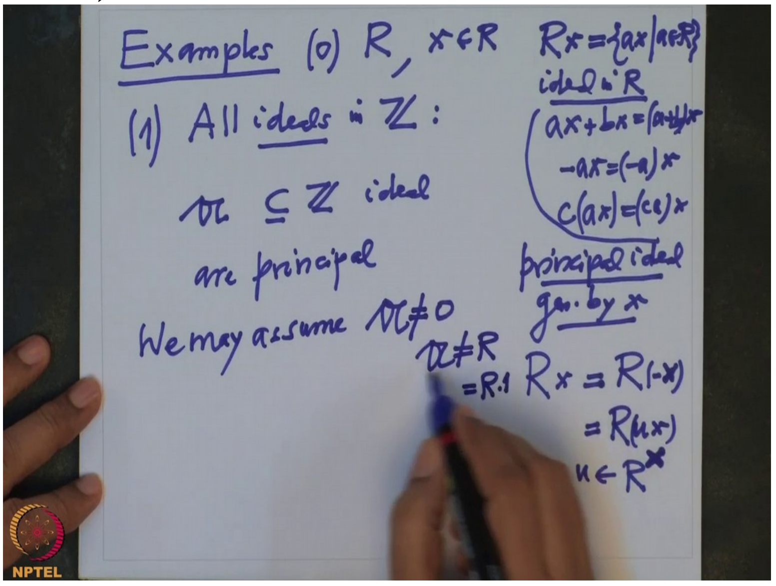
So similarly I can also assume A is not R because R is also

(Refer Slide Time 11:46)



an ideal, R is generated by the element 1. So these are called

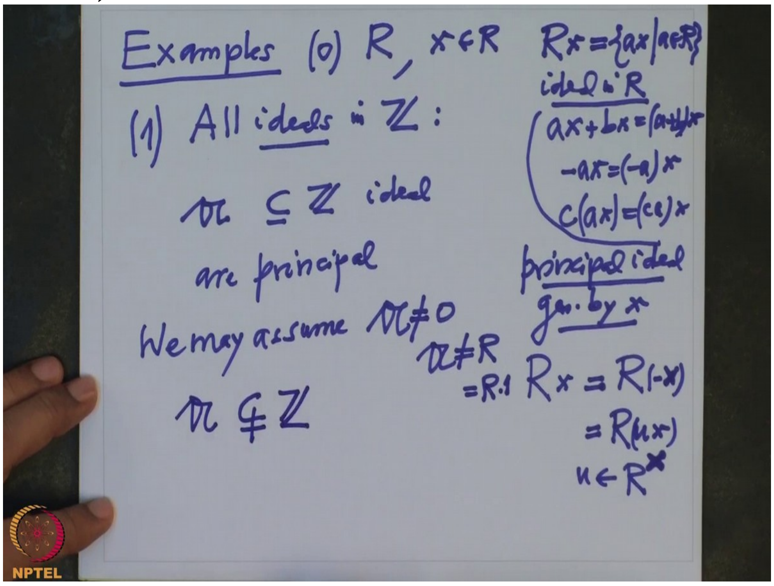
(Refer Slide Time 11:51)



trivial ideals. Trivial ideals is 0 and the whole ring, they are obviously ideal in any ring. They are called as trivial ideals.

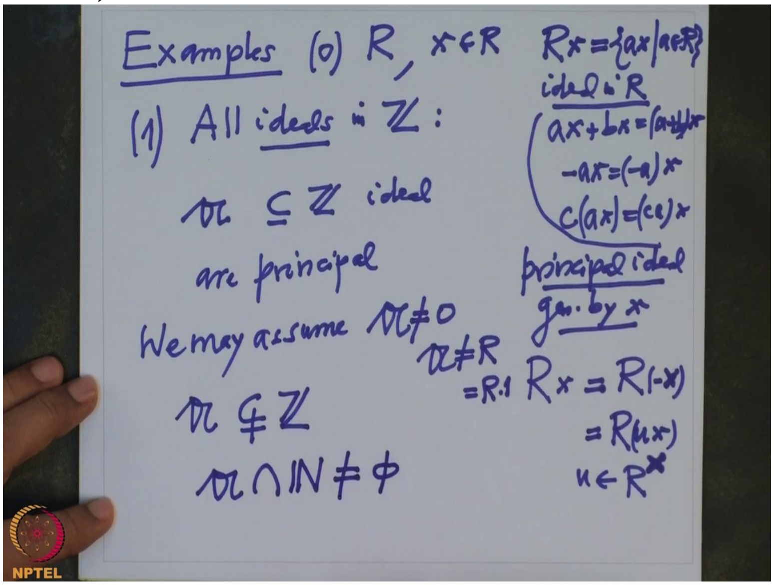
R is usually called a unit ideal and 0 is called a 0 ideal. So to prove it is principal, I will assume A is non-zero and A is also R. If anyone of the case happens then there is nothing to prove. Now we have a proper subset of $\mathbb{Z}$

(Refer Slide Time 12:24)



and I look now, I take the minimum element. So let us take $A \cap \mathbb{N}$ then this is non-empty.

(Refer Slide Time 12:39)

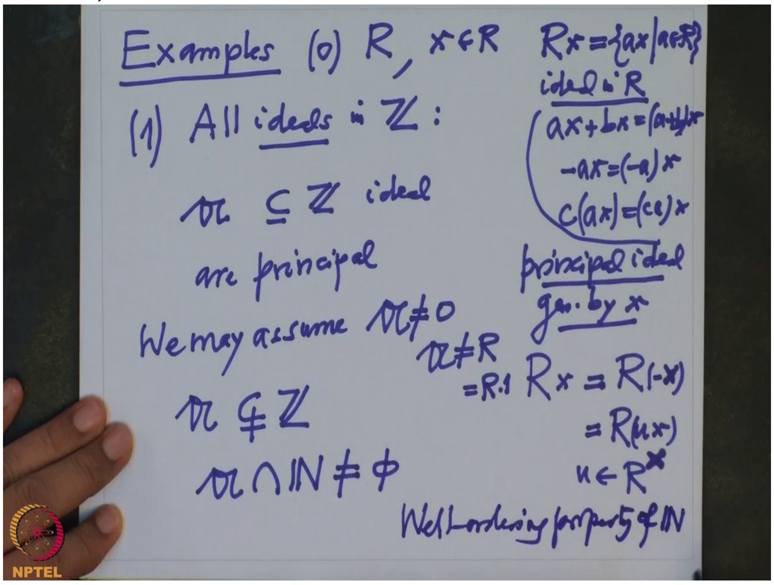


Because I know that A has at least 1 non-zero element, if it is positive already that element is in $\mathbb{N}$ and A, therefore it is non-empty. If that element is negative, then I take negative of that element which is also in A because A is an ideal and therefore in any case, $A \cap \mathbb{N}$ is empty.

And now I want to use the basic property of natural numbers which says that every non-empty subset of natural numbers has the minimum.

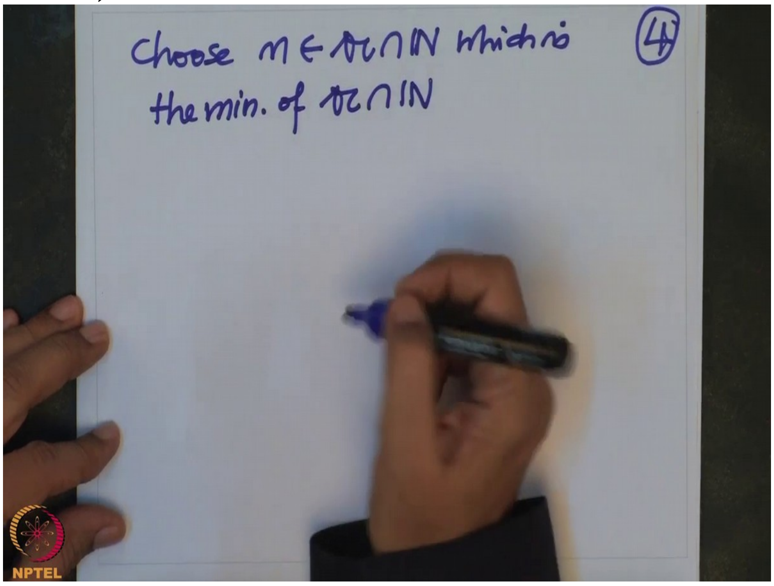
This is called well-ordering property of $\mathbb{N}$, of $\mathbb{N}$ that says that every non-empty

(Refer Slide Time 13:23)



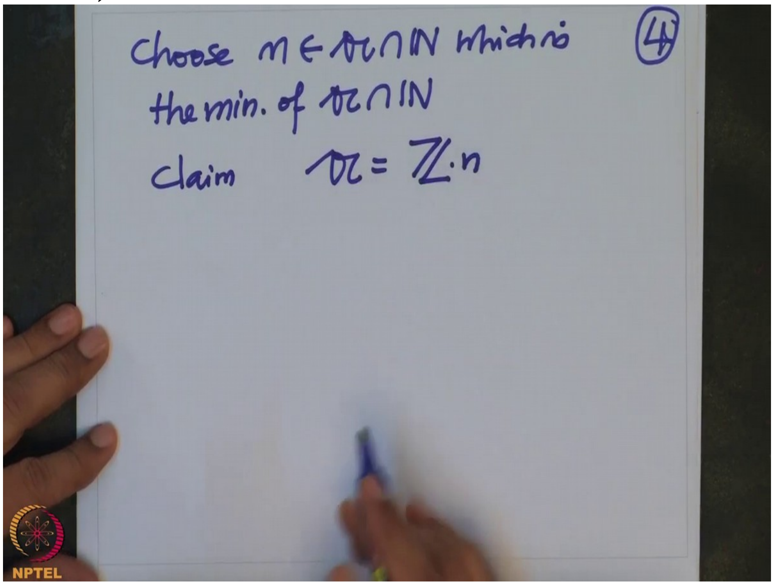
subset of $\mathbb{N}$ has a minimum. So I apply to this subset, so choose $n \in A \cap \mathbb{N}$ which is the minimum, minimum of $A \cap \mathbb{N}$.

(Refer Slide Time 13:48)



And claim is A is nothing but all $\mathbb{Z}$ multiples of n.

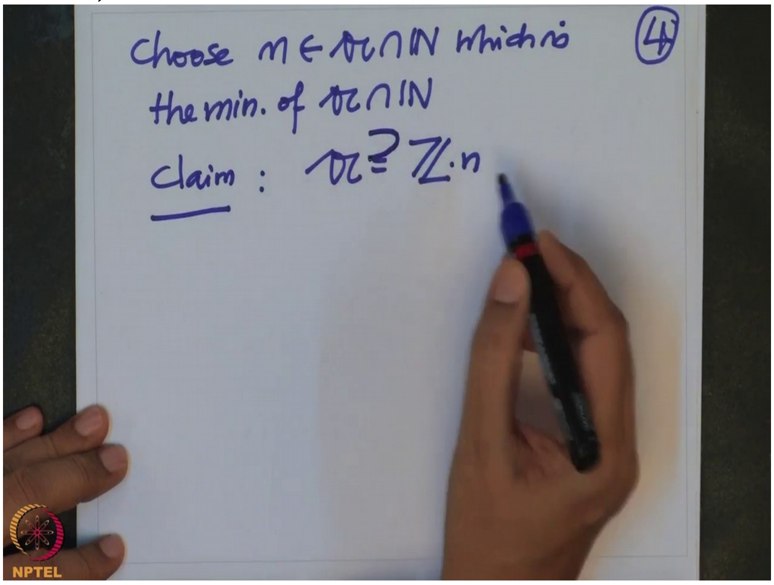
(Refer Slide Time 13:57)



That is what we want to prove.

And that will finish our proof that A is the principal ideal. So obviously this inclusion is obvious

(Refer Slide Time 14:07)

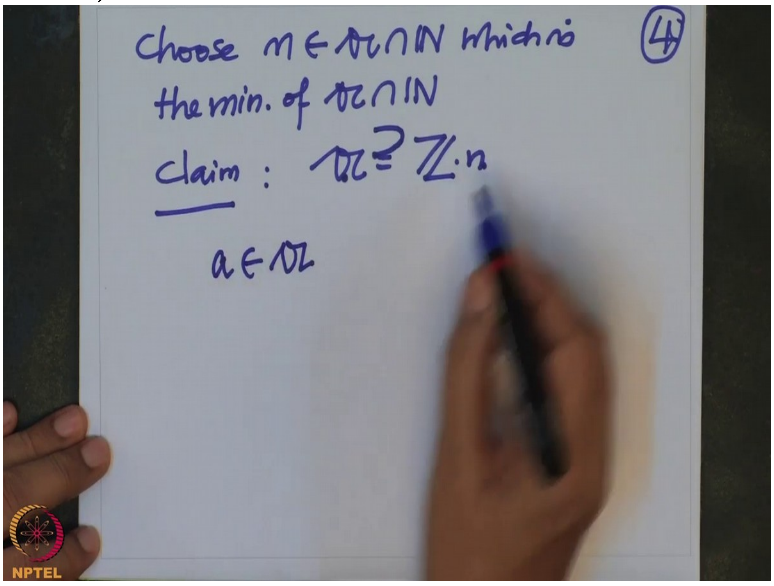


because we chose this n to be in the ideal A. So because it is an ideal, all $\mathbb{Z}$ multiples of n are also in that set, because it is an ideal.

Second condition of the ideal, that if I take the arbitrary element in the ring and arbitrary element in the ideal then the multiplication is also again in the ideal. So this is clear. I want to prove the other way.

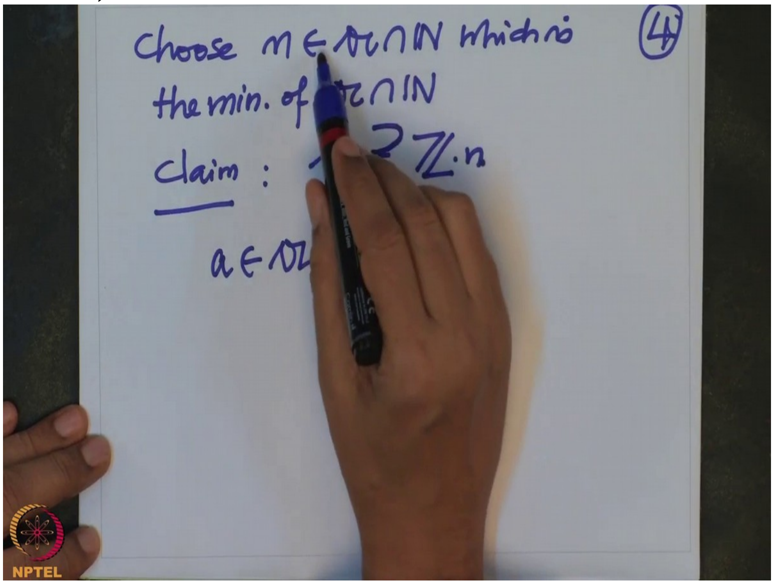
So start with any element a in A. And I want to show that this a

(Refer Slide Time 14:38)



is the multiple of this n, $\mathbb{Z}$ multiple of n. So what we can do with a and n? a and this n, we are given. Obviously this a is, n is non-zero

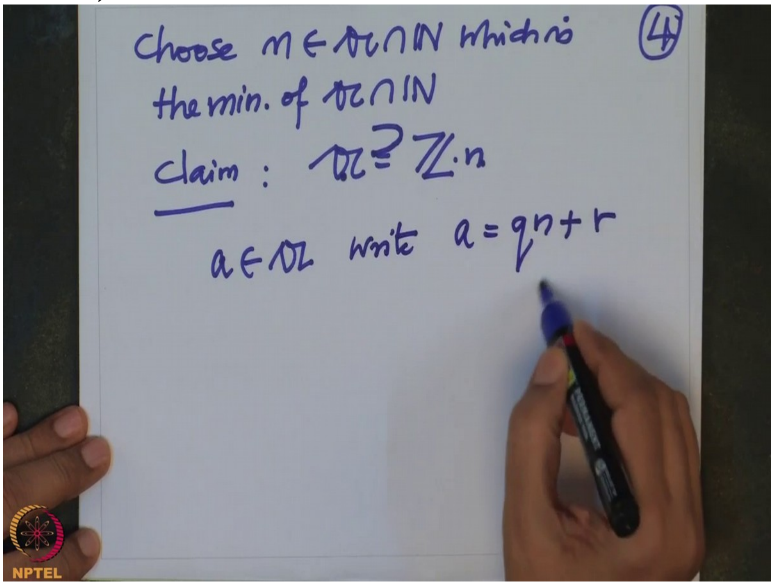
(Refer Slide Time 14:48)



because A, $A \cap \mathbb{N}$ we are assuming, we have chosen a non-zero element in $A \cap \mathbb{N}$, so this is a minimum.

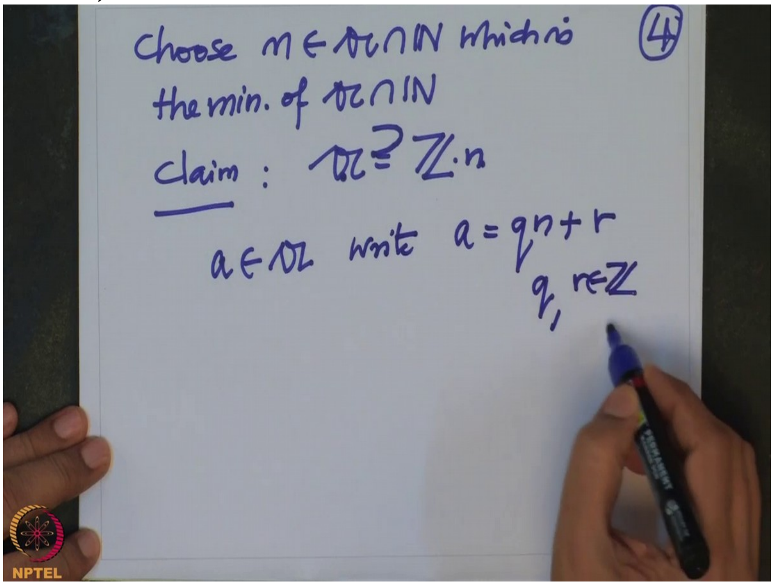
And now we can divide A by n so therefore write, by division algorithm write a as q times n plus remainder r

(Refer Slide Time 15:14)



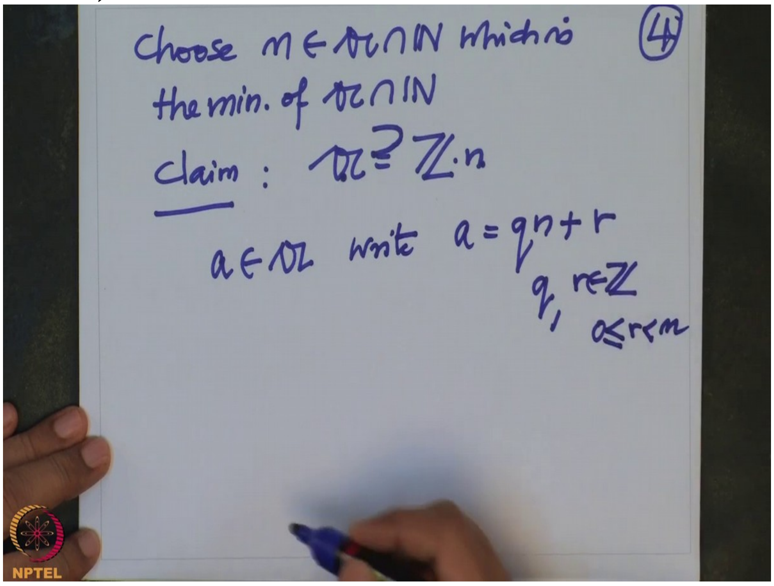
where q and r are elements in ℤ

(Refer Slide Time 15:18)



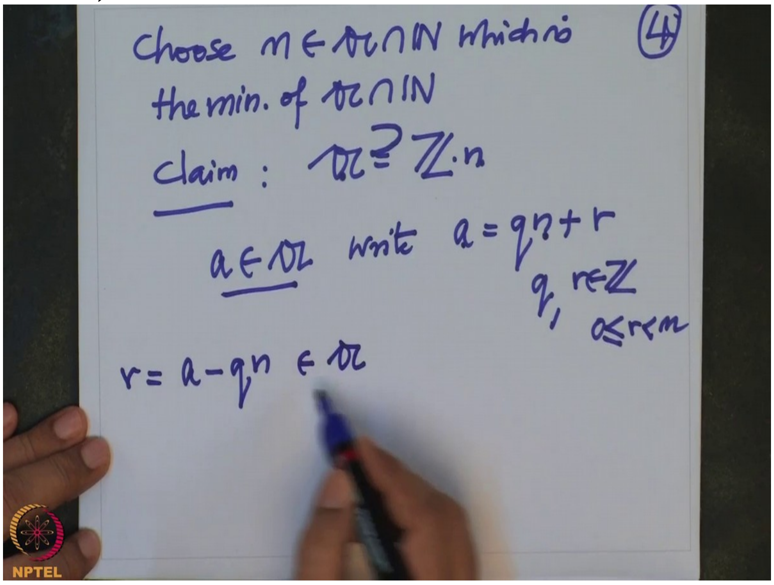
and r is strictly less than n.

(Refer Slide Time 15:24)



Now look here, this equation says that this a is in A, this n is in, this multiple is in $\mathbb{Z}$ multiple therefore it is in the ideal A so when I shift it to this side, a times q n, this is r but this is in the ideal A because of the definition

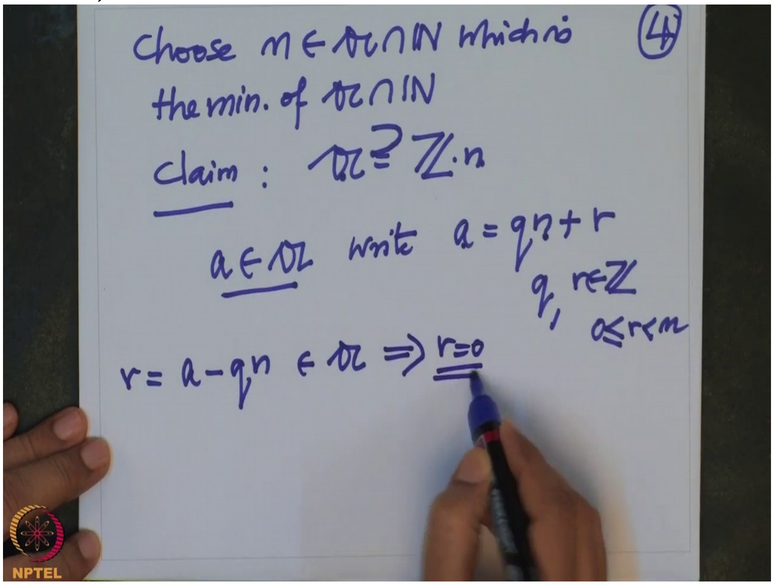
(Refer Slide Time 15:44)



of the ideal and therefore r has to be 0.

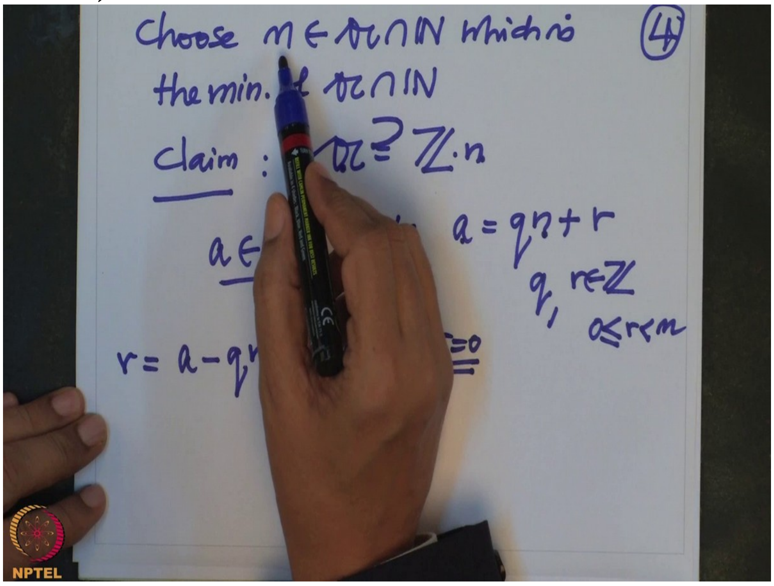
If r is not 0,

(Refer Slide Time 15:51)



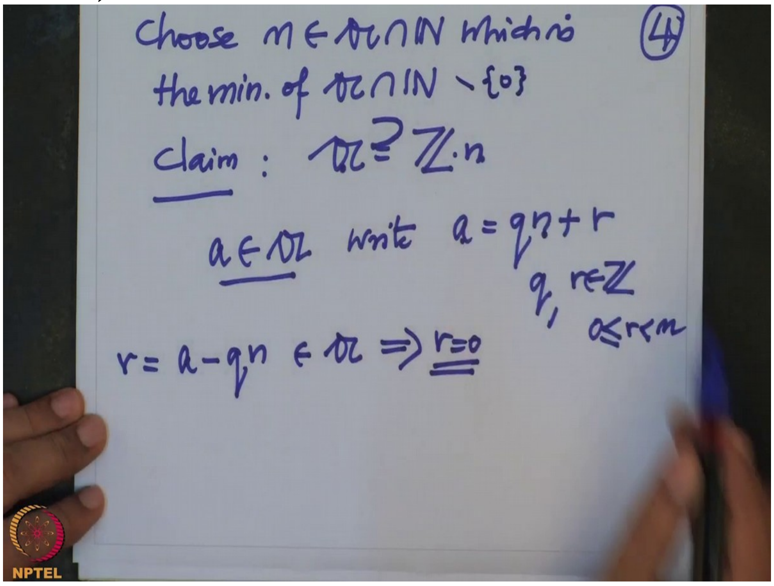
that will contradict the minimality of n. So just to be very sure that we have taken, remember we have chosen

(Refer Slide Time 16:02)



n in this which is the minimum in this minus 0 I should have said.

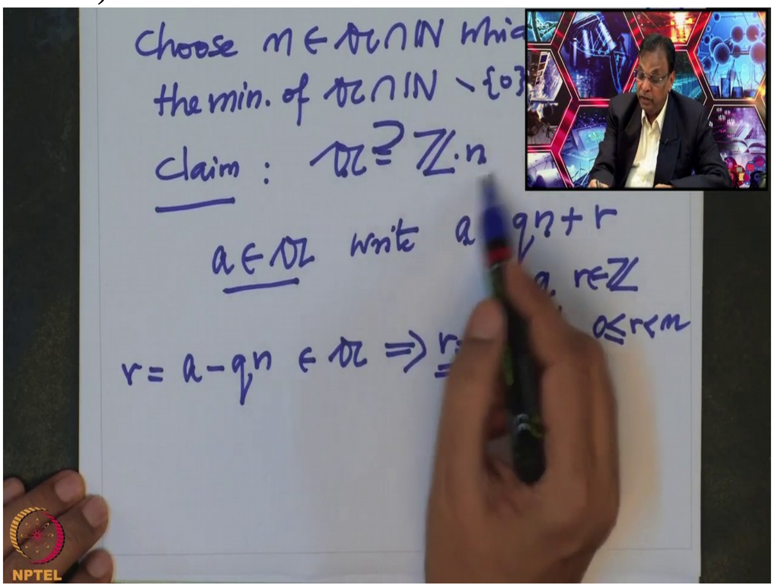
(Refer Slide Time 16:08)



That is, that was what, that is why we need to assume a is non-zero. So therefore this proves that all ideals in $\mathbb{Z}$ are principal and remember the only tools we have used in this is the division with remainder.

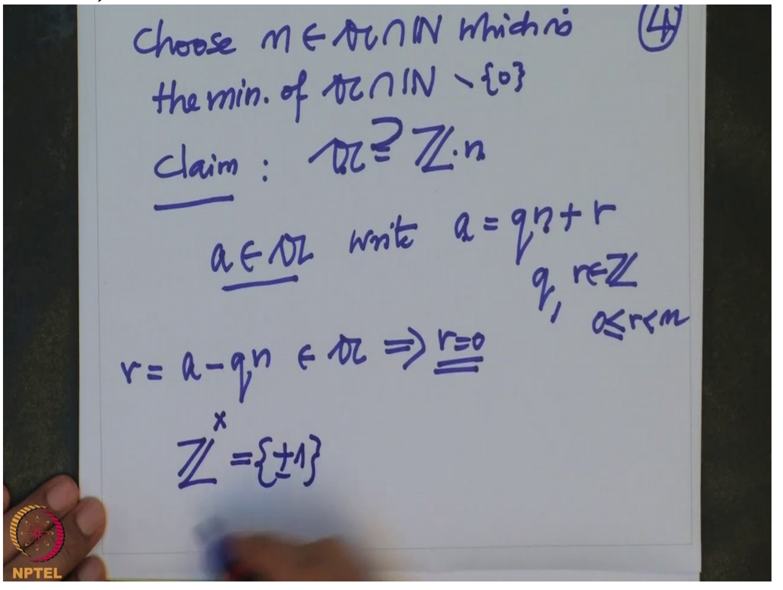
And not only that if I choose now, what are the choices, how many, can I recover back from this ideal

(Refer Slide Time 16:36)



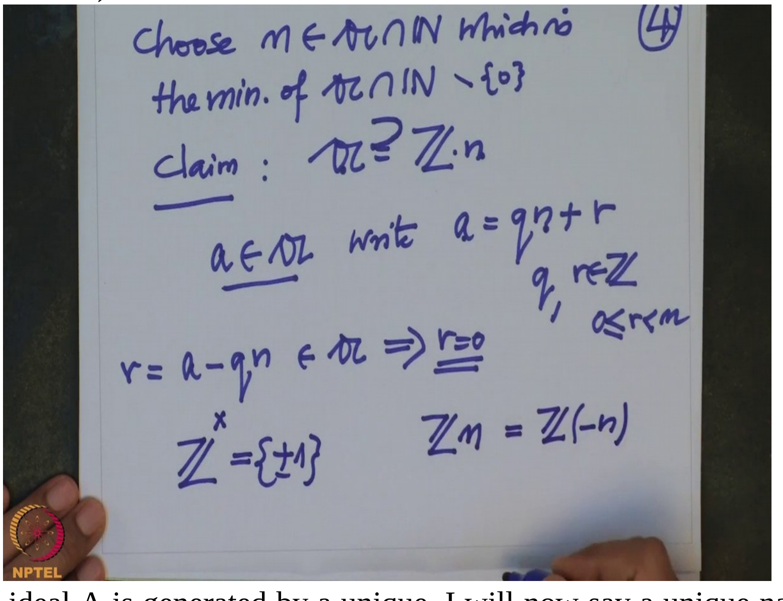
this n, the generator, there are only 2 possibilities because we have, in this ring as a property that the units are only 1 and minus 1. These are the only 2 units.

(Refer Slide Time 16:51)



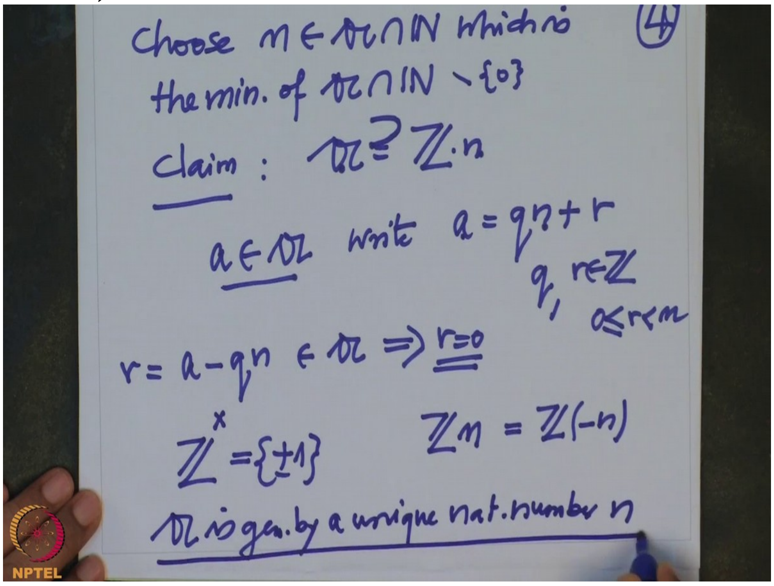
So therefore the only possibility is the $\mathbb{Z}$ multiples of n is same as $\mathbb{Z}$ multiples of minus n.

(Refer Slide Time 17:01)



So therefore this ideal A is generated by a unique, I will now say a unique natural number n, unique natural number n

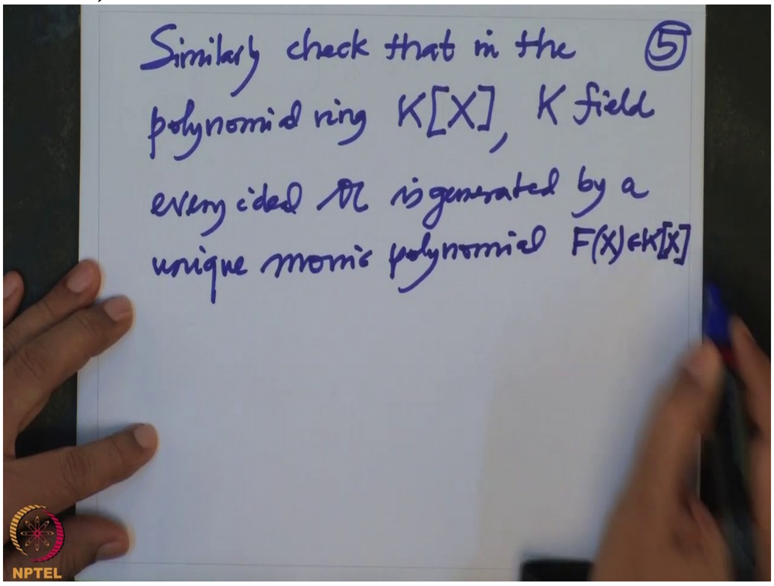
(Refer Slide Time 17:20)



n because this gives the possibility to remove the negative ones. So and nothing special about this ring.

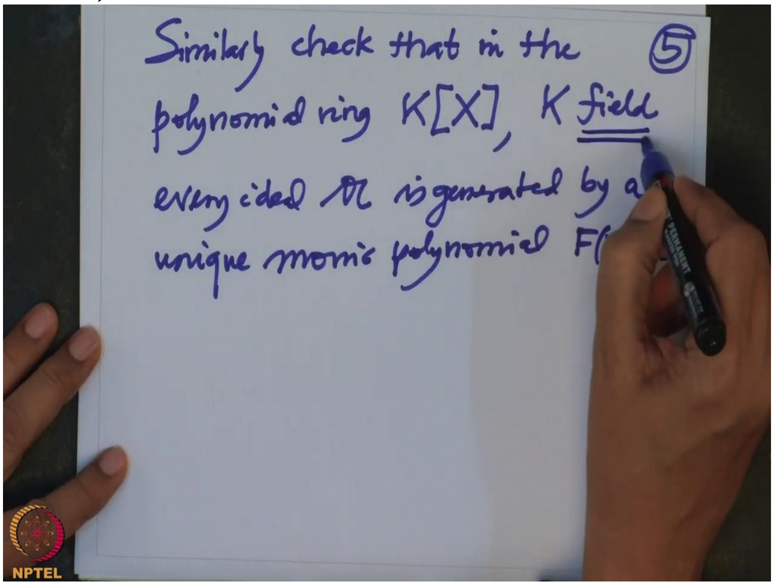
So I will state without proof and one should check this, I will just say similarly, check that in the polynomial ring, $K[X]$ where K is a field, every ideal A is generated by a unique monic polynomial $F(X) \in K[X]$.

(Refer Slide Time 18:30)



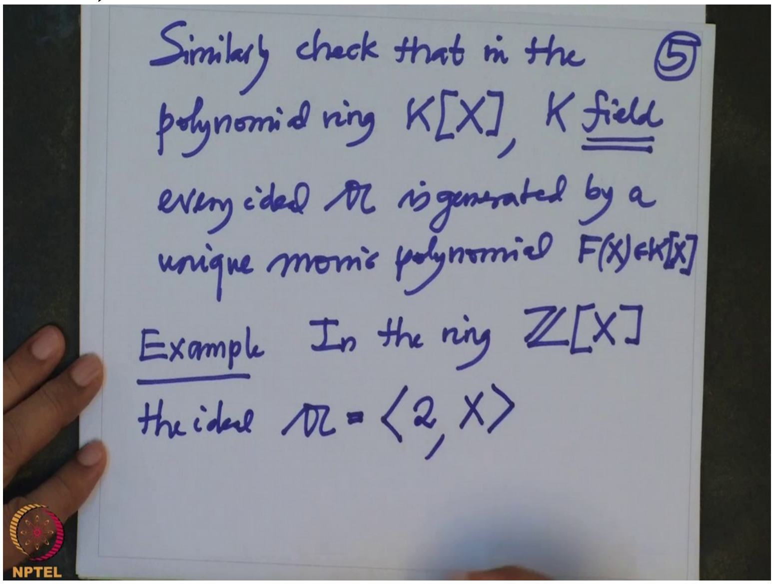
Same proof, we just take, because there we have used the division algorithm. Here also division algorithm is available because K is a field,

(Refer Slide Time 18:41)



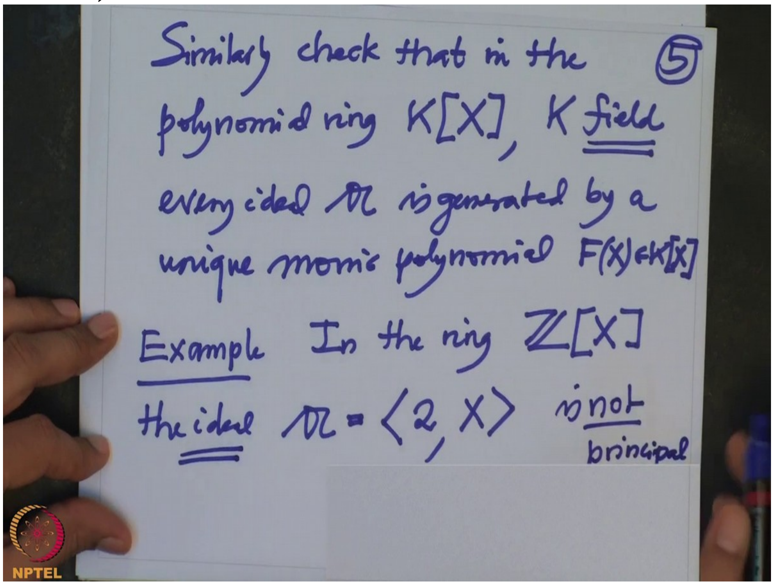
Ok. So before I go on, at least one example where not all ideals in all rings are principal. For example, in the ring $\mathbb{Z}$ polynomial ring, its coefficient in the ring $\mathbb{Z}$, the ideal A which is generated by 2 and X, what does this mean?

(Refer Slide Time 19:22)



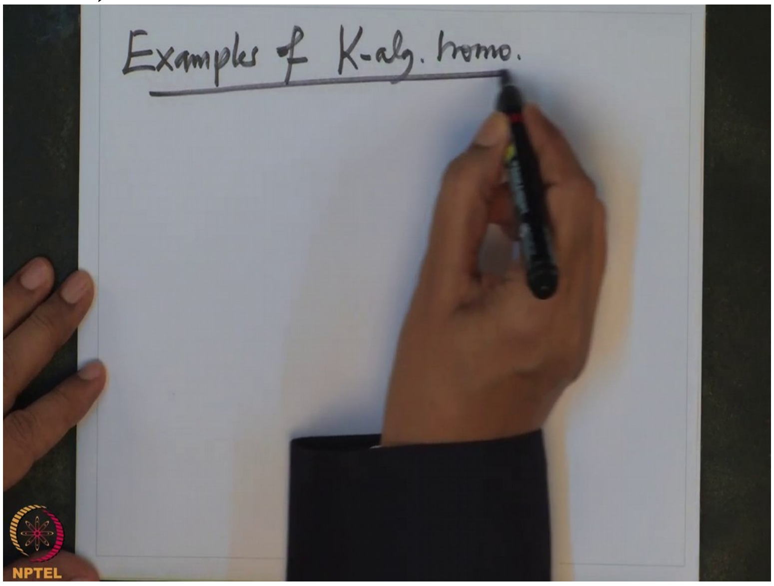
This is indeed an ideal and also check that this ideal is not principal. This I will leave it to you to check,

(Refer Slide Time 19:34)



Ok.

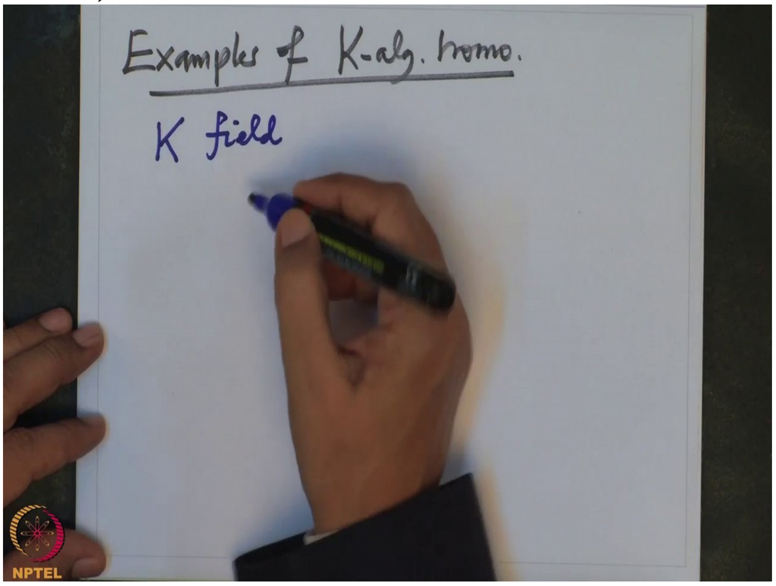
(Refer Slide Time 19:59)



So, on the way we are going to find more examples of ideals, right. So I want to give few more examples of algebra homomorphisms. So for example, examples of K-algebra homomorphisms.

So, so you have 2 K-algebras, so one K-algebra, so K is a field I will take. Though it is not really necessary that K is a field

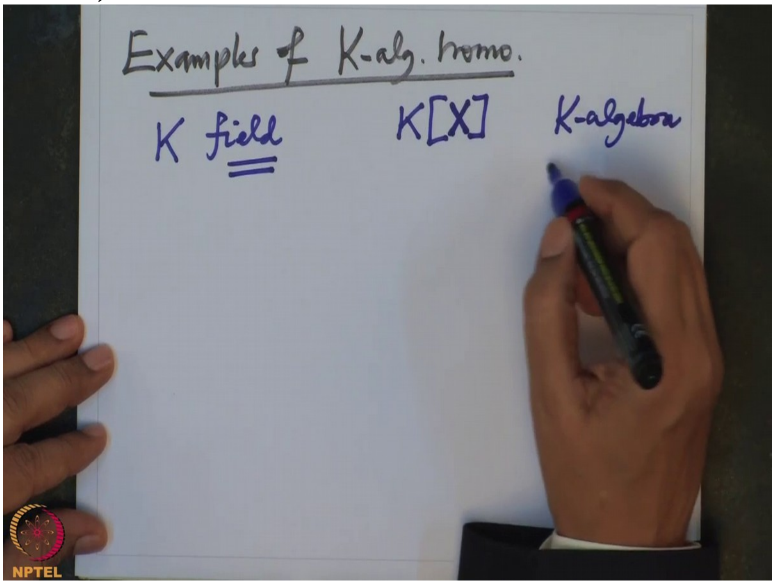
(Refer Slide Time 20:13)



but if I keep assuming more general thing then this course will get more and more delayed and more and more going away from our aim, so let us assume that K is a field. And the typical K-algebras that we are going to deal is $K[X]$, a polynomial ring over K in one variable X.

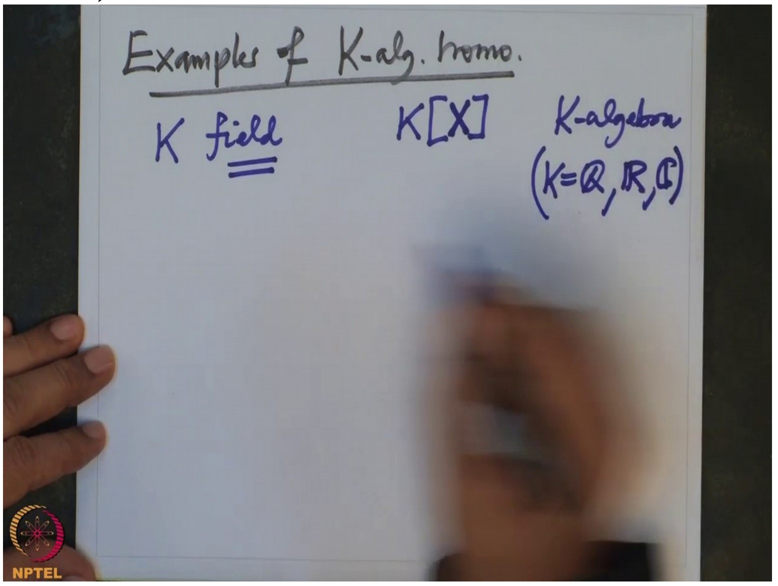
So this is clearly K-algebra. So typically

(Refer Slide Time 20:42)



you should keep in mind, take K equal to $\mathbb{Q}$ and these are all polynomial with rational coefficients. Or K equal to $\mathbb{R}$ or K equal to $\mathbb{C}$. These are

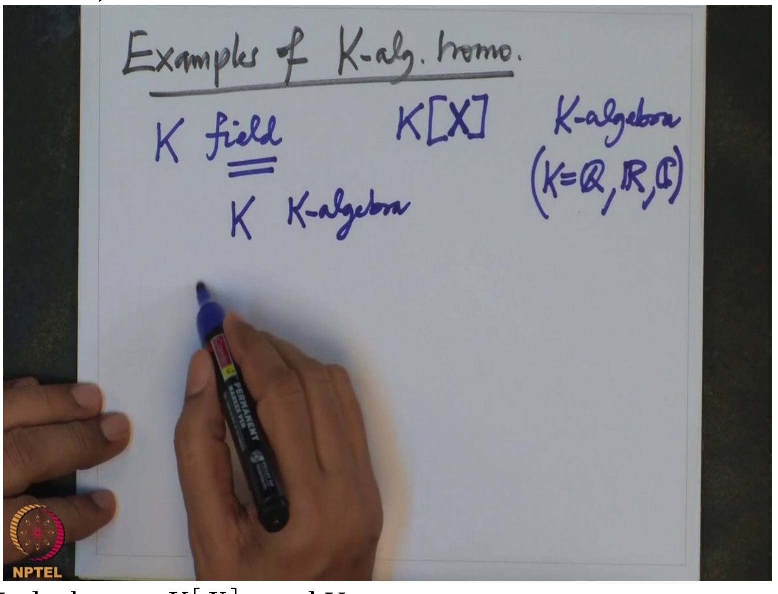
(Refer Slide Time 20:53)



the typical examples.

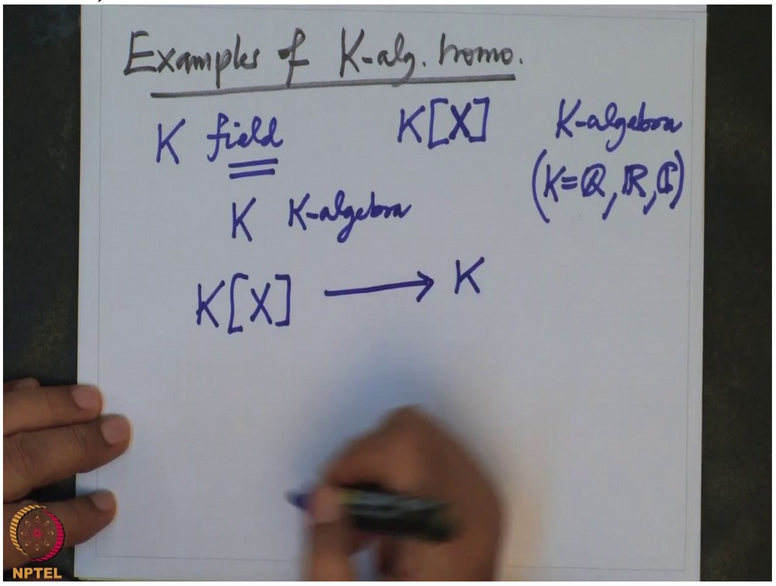
And now take K itself is a K-algebra, K is also a K-algebra with the same scalar multiplication as the multiplication in K. So I

(Refer Slide Time 21:09)



have these two K-algebras, $K[X]$ and K.

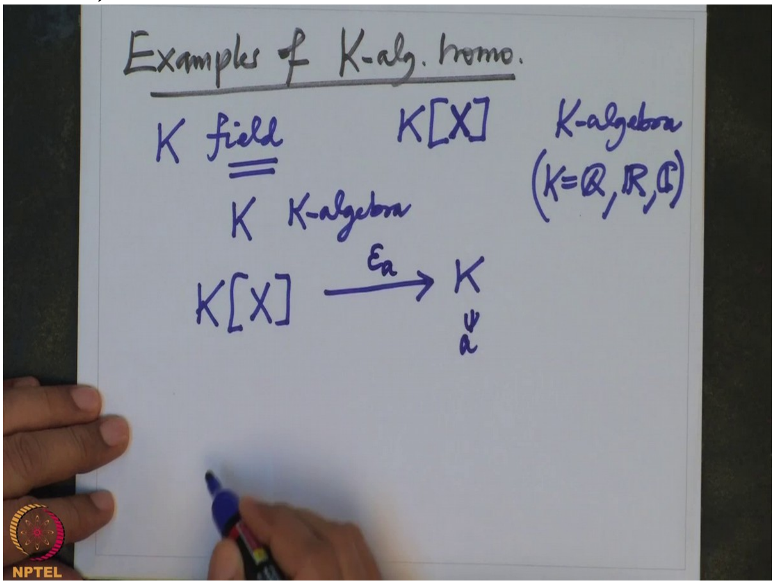
(Refer Slide Time 21:17)



And I want to give a map between these two. It should be K-algebra homomorphism and K-algebra homomorphism means it is a ring homomorphism and it is K linear map.

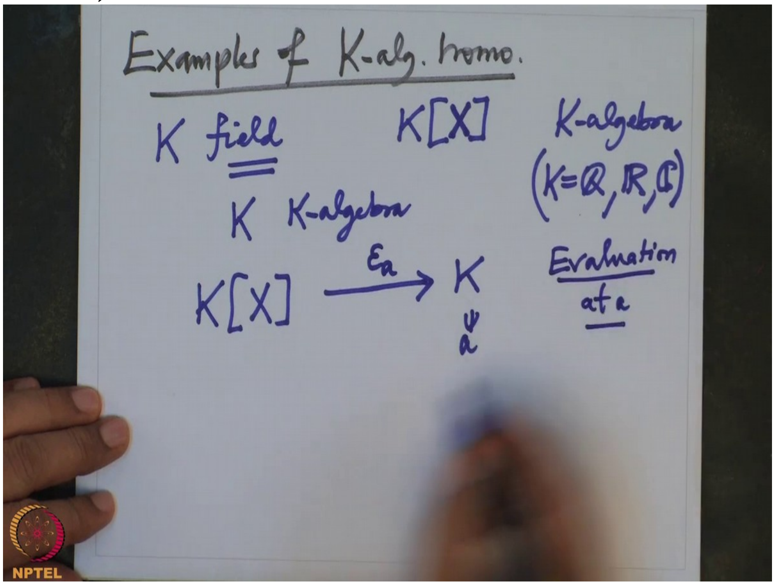
So given any element a in K this epsilon a

(Refer Slide Time 21:35)



or E a, E is for evaluation, evaluation at a. What is this map?

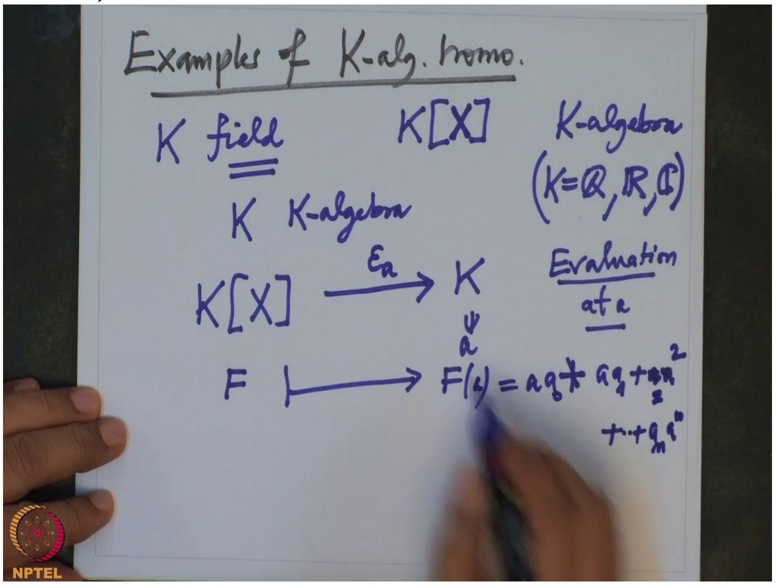
(Refer Slide Time 21:47)



Take any polynomial F and map it to F of a. F of a is a times a 0 plus a times a 1 plus so on. Just put, wherever there is X, put that is a. And the next term will be; I should actually write the coefficient first. So a 2 times a square etc etc a n times a power n.

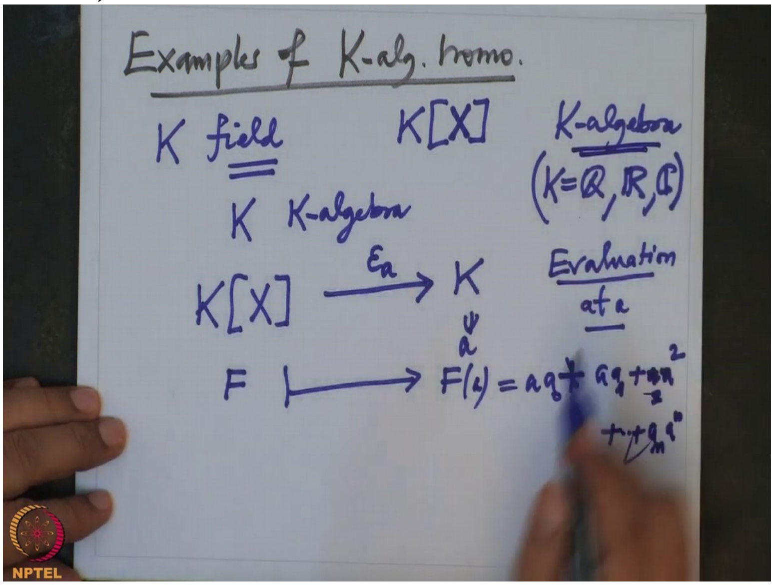
This makes sense

(Refer Slide Time 22:26)



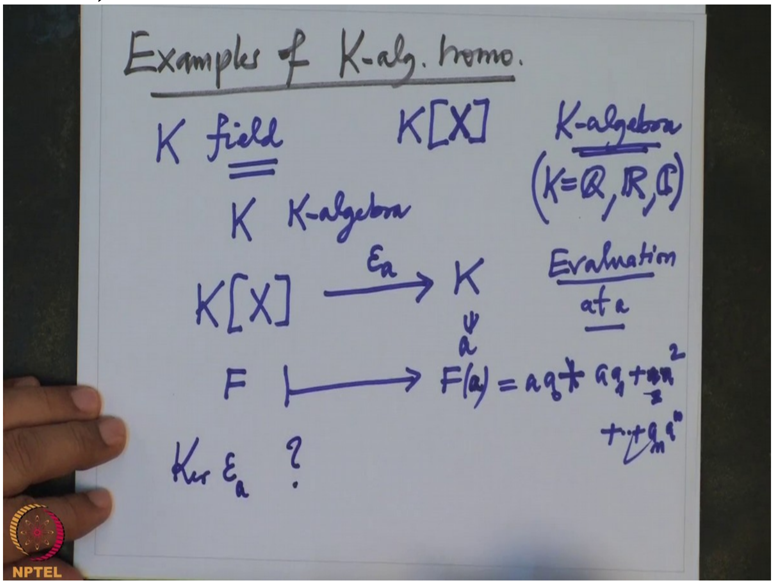
in K now because all these are the elements of K. That is precisely why we needed a concept of K-algebra.

(Refer Slide Time 22:33)



So this is precisely what we call it F of a. And we are interested in, given an element, given a polynomial F we want to find a so that F of a is 0, so that means precisely we are interested in finding out the kernel of y. This is what we are interested in.

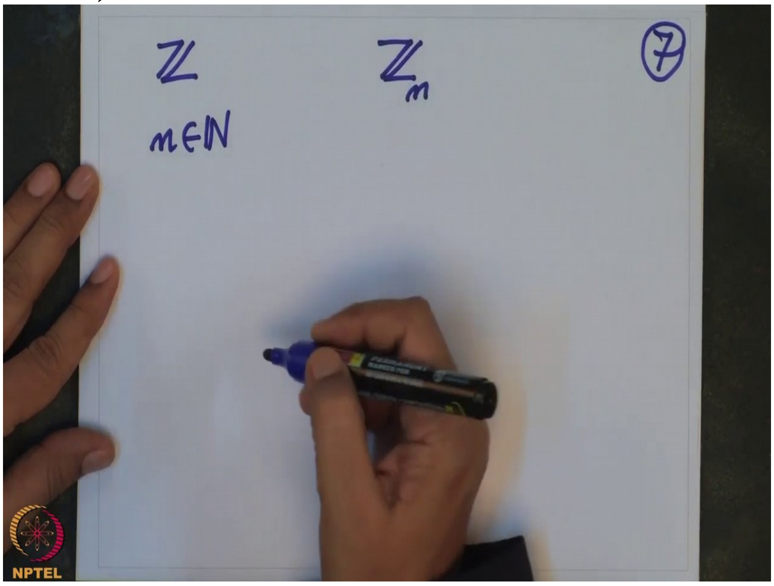
(Refer Slide Time 22:55)



And particularly knowing, so it is an ideal, we know kernel is an ideal. This is ring morphism so this is an ideal. And also we know it is a principal ideal. Also we know that this ideal is generated by a unique generator, unique monic generator and that is what we are going to formalize for the, and the little bit more general situation.

But before I do that I also need a construction of a new ring by ring ideal. So remember from $\mathbb{Z}$ and given any integer n, natural number we have constructed a new ring called $\mathbb{Z}$ modulo n.

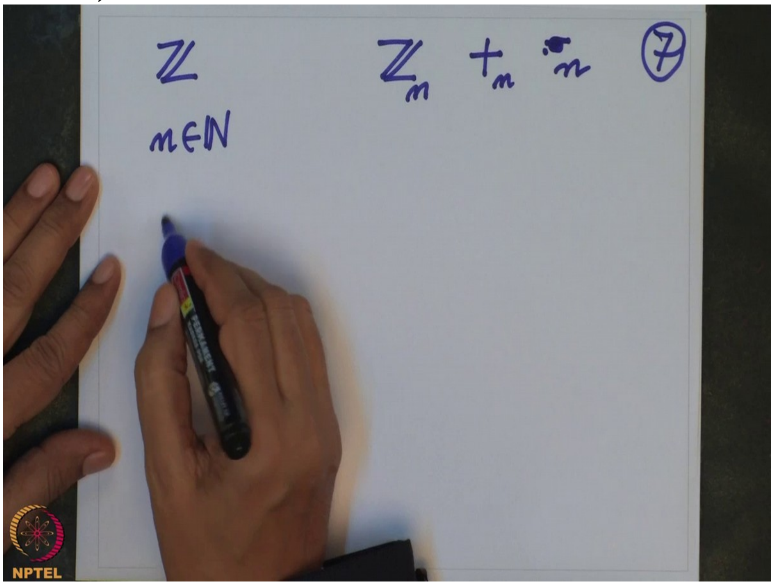
(Refer Slide Time 23:43)



This ring was constructed by using $\mathbb{Z}$ and n by taking the operations addition modulo n and multiplication modulo n.

Similarly

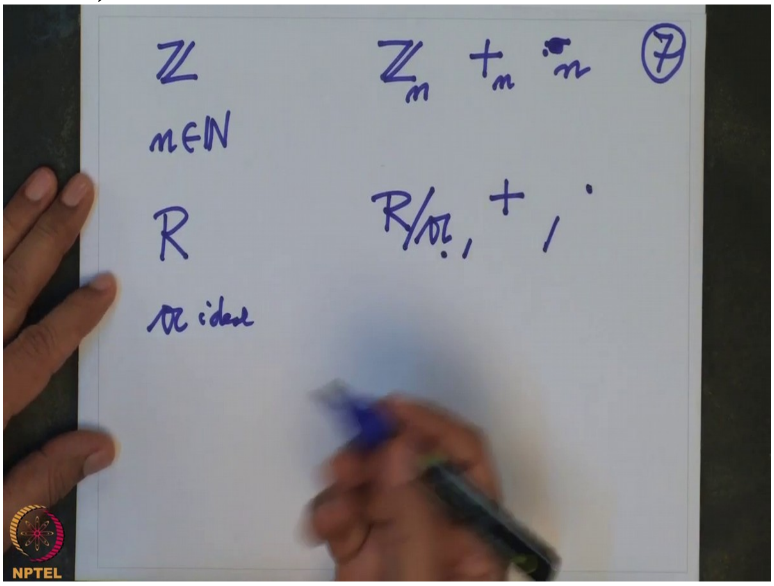
(Refer Slide Time 23:58)



given any ring R and given any ideal A, I am going to construct a new ring which will be denoted by R modulo A. So the new ring, the addition there I will use a similar construction.

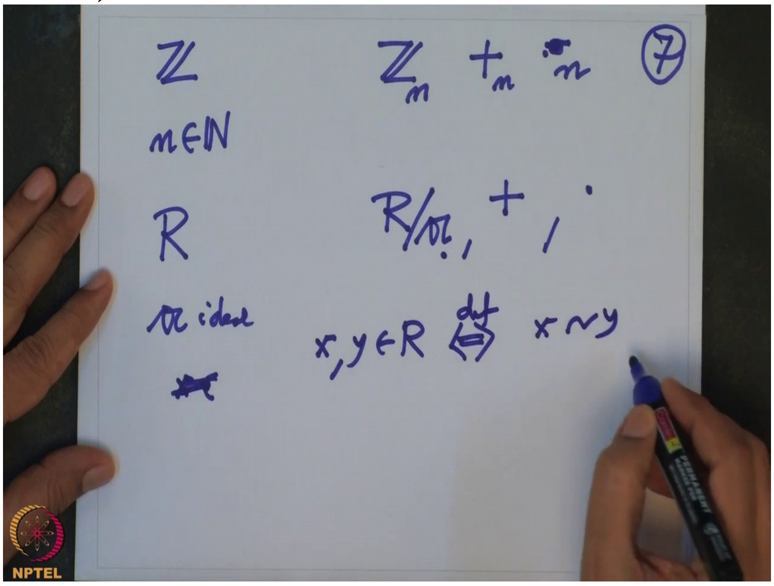
That means I will introduce an equivalence relation which will be defined by A and take the equivalence classes and on the equivalence classes I define addition and multiplication.

(Refer Slide Time 24:28)



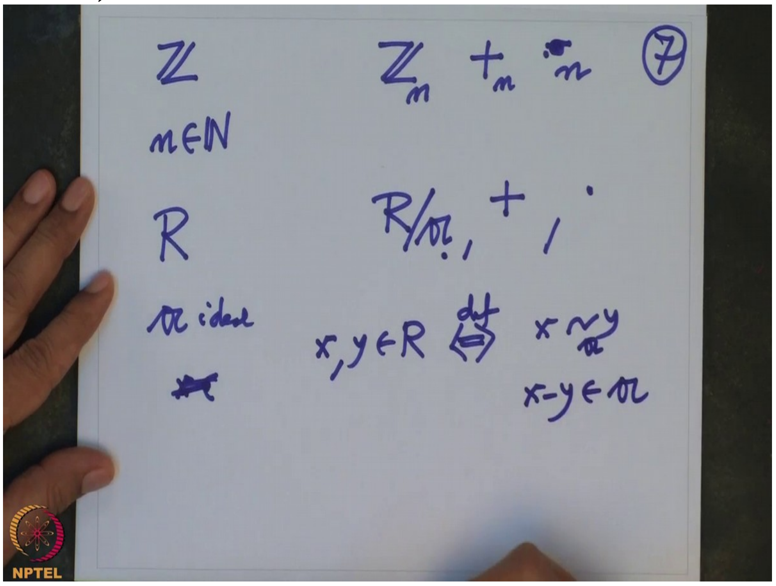
And how do I do that? It is very simple. Take any x in, take, define an equivalence relation by x, y in R then we say that this is a definition. x is related to y

(Refer Slide Time 24:50)



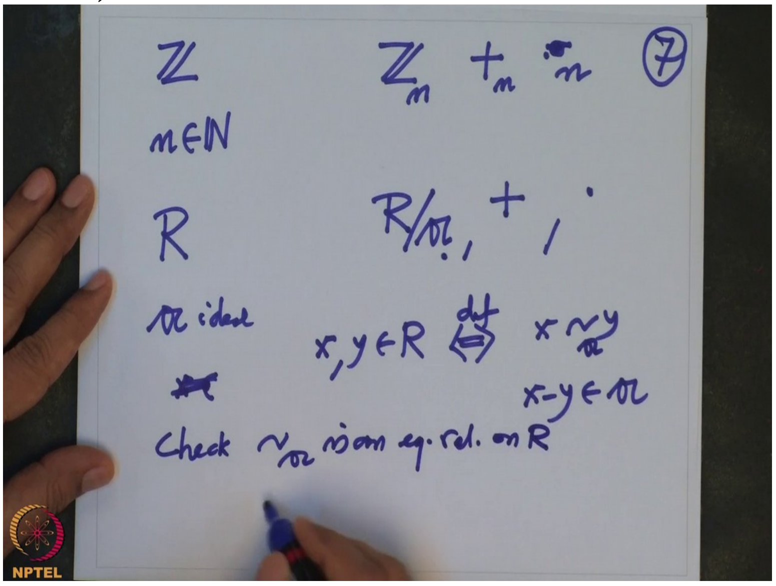
under, A should come somewhere notation, so I will just write simply this. So this means x minus y should belong to the ideal A.

(Refer Slide Time 25:02)



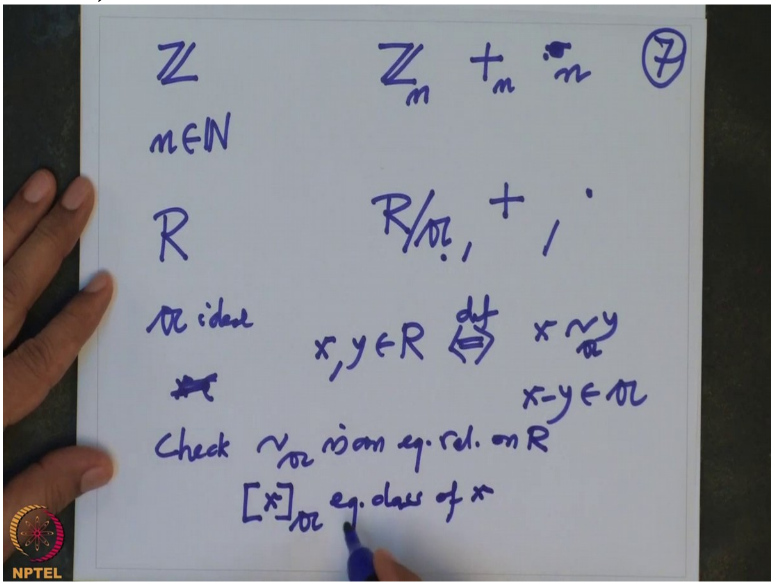
And now we will check that, check I will just say that check that this is an equivalence relation on R

(Refer Slide Time 25:15)



and let us denote the equivalence classes x suffix A here, equivalence classes, class of x and obviously you have to add

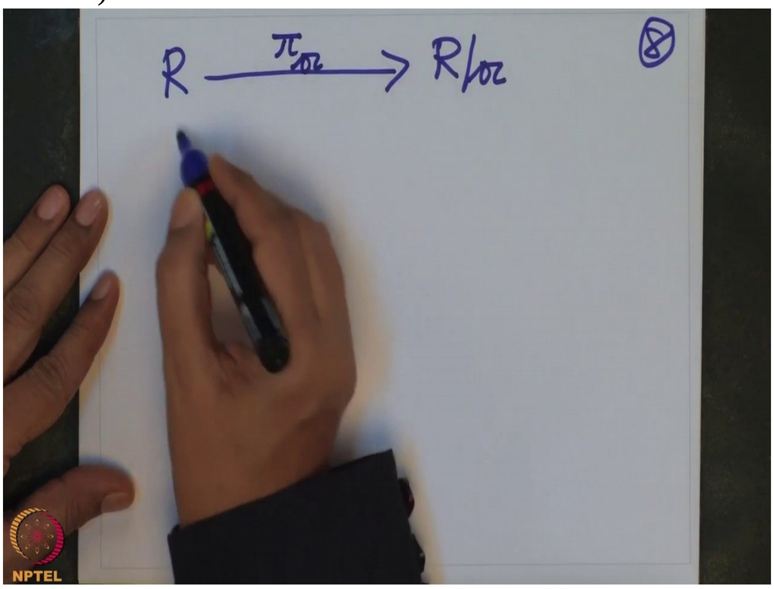
(Refer Slide Time 25:27)



these, add as usual and take its equivalence class under A and then you check that these operations are well-defined and same, everything is same. If one gets stuck, go back to study the example.

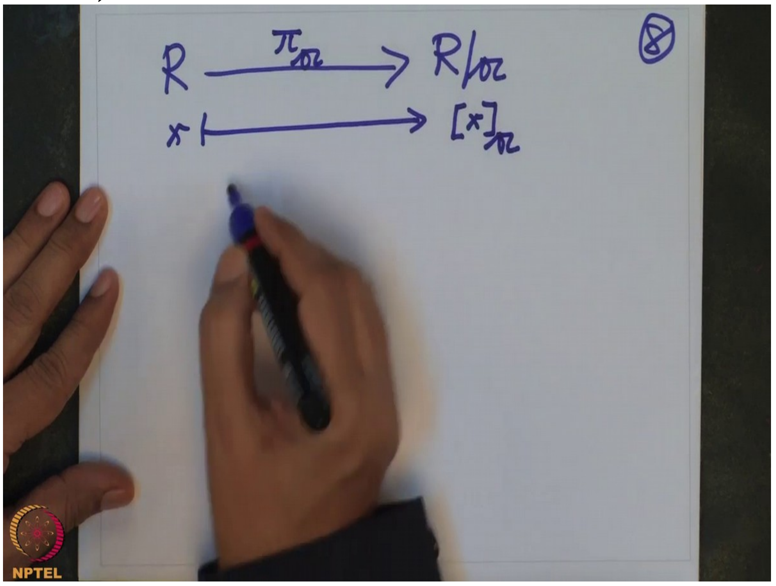
So from this ring R we have this new ring. So R we have passed on to this new ring R by A and also we have a natural map here. This is, I denote by π_A ,

(Refer Slide Time 25:55)



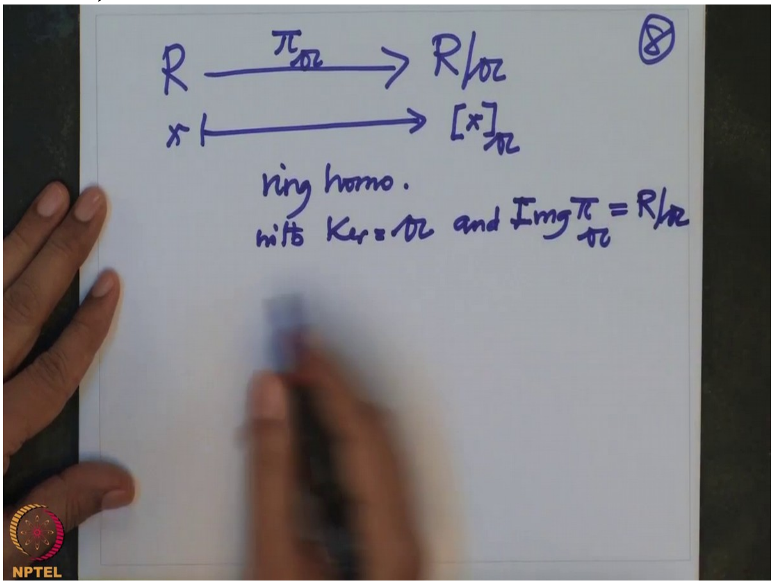
this is x going to equivalence class of x under A

(Refer Slide Time 26:01)



and also I will leave it for you to check that this is a ring homomorphism, ring homomorphism with kernel, the given ideal A and image, image of π_A is the whole R by A, that means

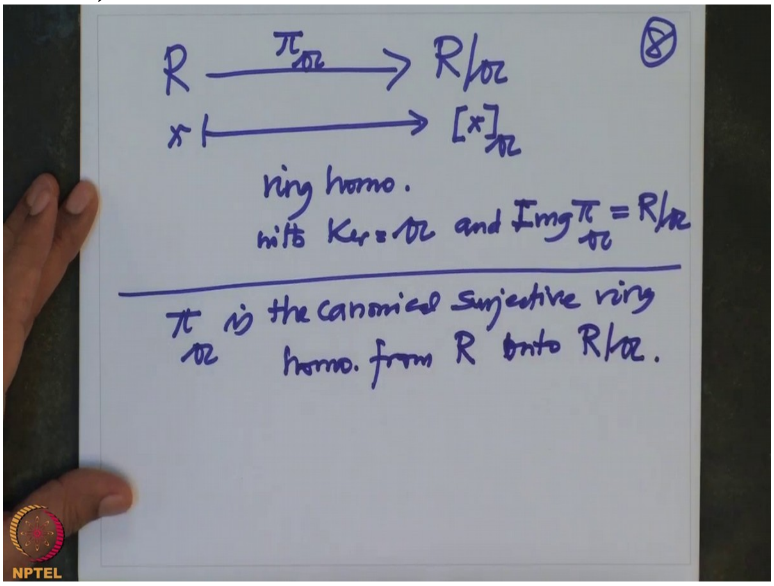
(Refer Slide Time 26:26)



this.

In other words, this π_A is the canonical surjective ring homomorphism from R on to R by A.

(Refer Slide Time 26:54)



So that is a kernel. Now we are in much better position to describe what algebraic element means and what algebraic extensions are.

But this program I am going to carry out in the next lecture. And just to summarize what we have seen today's lecture is rings, ring homomorphisms, algebras, algebra homomorphisms, kernel, image and so on.

And now in the next lecture we will introduce the concept of algebraic elements. We will introduce the concept of field extensions which are algebraic and also define transcendental elements and so on. And use this further to one of our main step, the beginning step that given a polynomial over arbitrary field, we extend the field in such a way that all the

(Refer Slide Time 27:54)

zeroes of this polynomial lie in the bigger field.

This we do it for single polynomial first and then we do it for many polynomials and as a consequence we will deduce the fundamental theorem of algebra namely that is the field $\mathbb{C}$ is algebraically closed. With this I will stop today, thank you.