Commutative Algebra
Prof. A. V Jayanthan
Department of Mathematics
Indian Institute of Technology, Madras

Lecture – 2
Review of Ring Theory (Continued)

(Refer Slide Time: 00:22)

Suppose we take the set of all 0 divisors of a ring. If this is only 0 then such rings are called integral domains. If the only 0 divisor of, so first we should say let A be a commutative ring with identity. If the only 0 divisor of A is 0 then A is called an integral domain. We have an almost all of the examples that we were looking at, they are all integral domains; so Q R C Z all of them. What about this set? Can you say something about this set? Is this an integral domain? Why it is not an integral domain.

Student: You take any (Refer Time: 02:19).

Can you can you give me an example where this is not an integral domain.

Student: Take s equal to R.

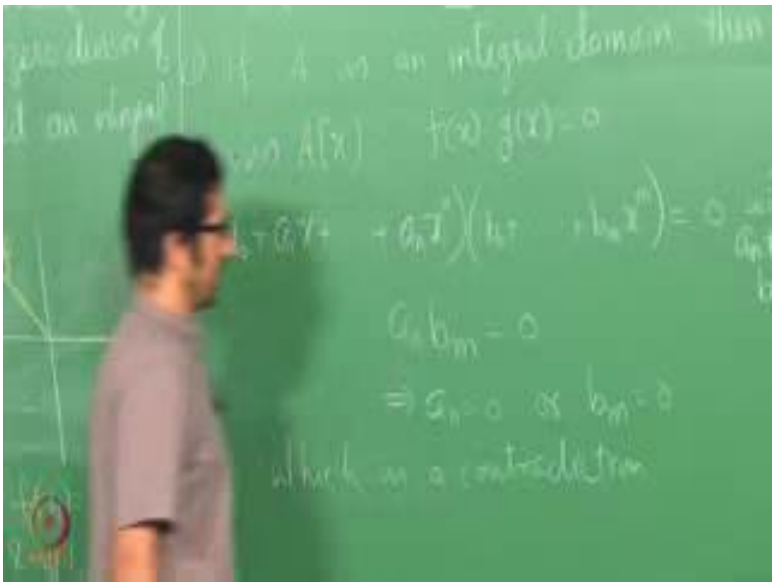
Take s equal to R fine.

Student: Constructs are standard functions.

So you want to say construct this kind of functions. You understand the difference, so if you take so this is your, if this is f and if this is g then f times g is 0 neither this is f and this is g then f g is 0, but neither f nor g is 0.

I mean you do not really have to go that far if we just take s to be 2 points set right. And take f f a to be one f of b to be 0 g of a to be 0 and g of b to be 1 then f g is always 0, but neither f nor is g is, so this is not an integral domain, so F s is not an integral domain.

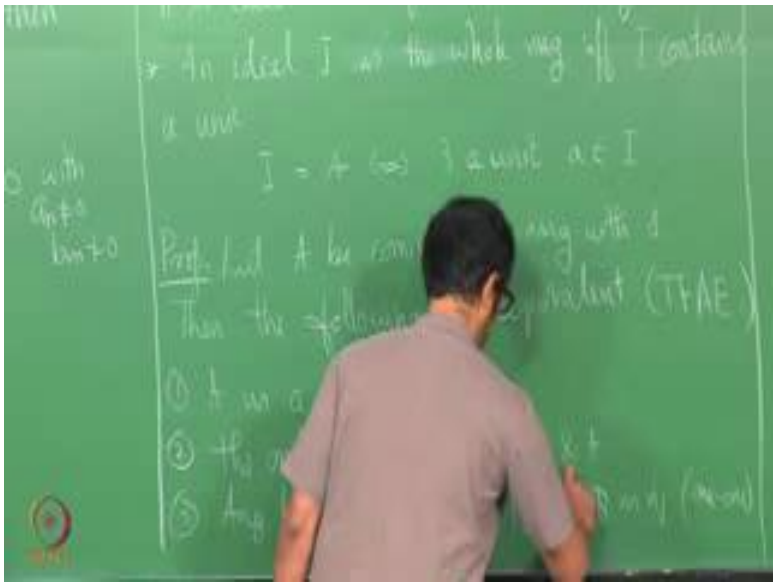
(Refer Slide Time: 04:12)



Another important example, class of examples in this direction that you will see often is, polynomials ring of polynomials over integral domains. If A is an integral domain then what can you says about A x? There is also an integral domain. So this is you know the proof is easy. One has to look at product like this a naught plus a 1 x plus etcetera a n x power n b naught plus b m x power m. Suppose this is 0 we want to say that one of them is 0. Suppose both of them are non 0; that means, I can get suppose I have f x times g x is 0. F x is non 0 g x is non 0. Then I can get an n and an m such that a n the leading coefficient of this f x this is non 0 and this is non 0.

Now, the product is 0. When do you say polynomial is 0? When each coefficient is 0 which means a n b m is 0, but our assumption is that neither a n is 0 with, so here with a n not equal to 0 b m not equal to 0, but our assumption is that A is an integral domain this will imply that a n is 0 or b m is 0. That is a contradiction. So therefore, we see that if a is an integral domain then so is A x

(Refer Slide Time: 07:19)



Now, if a is a unit implies there exists b such that a b is equal to one. So there this b is denoted b is called inverse of a. And denoted by a inverse. First simple observation again comes from your first course in algebra. An ideal I is ideal I is equal to as the whole ring if and only if I contains a unit. So this is in our situation that we are considering commutative rings with identity. So I is equal to A if and only if there exists A unit i. Of course, this easily implies this, but if a contains a unit which means you can multiply by it is inverse and then multiply with all elements of A.

Now, this brings a nice characterization of fields. Let A be a commutative ring with identity then the following R equivalent, hence forth I will be simply writing it like this. The following are equivalent will be denoted like this. A is a field the only ideals of A are 0 and a any homomorphism from A to a ring B is injective; so any to a non 0 ring. So as I mentioned earlier whenever I say a ring in our context it will be commutative ring with identity. I will not always repeat it, but so can we see one implies 2, A is a field.

(Refer Slide Time: 11:11)

If A is a field you want to say the only ideal is 0 and the whole ring. So if I take an ideal I take a non 0 suppose it is non 0 ideal take any non 0 element there it says that our assumptions that is a field therefore, it is a unit which means I contains a unit therefore, it is the whole. So any non 0 element non 0 ideal has to be whole ring is an ideal. Then there exists a unit in I and that implies I is A. So any non 0 ideal is the whole ring. Now how do you prove 2 implies 3 the only ideals of a R 0 and A. You want to show that any homomorphism from A to B any again any non 0 homomorphism any non 0 homomorphism from A to non 0 ring B is injective.

Student: (Refer Time: 12:40).

You look at kernel phi, so I have supposed phi is from A to B be a non 0 homomorphism. Then kernel phi is an ideal of A. Now kernel phi has only 2 options, kernel phi can be either 0 or the whole of A, but can it be the whole of a because we are assuming that phi is A.

Student: Non 0 ring homomorphism.

Non 0 ring homomorphism, therefore, kernel phi is non 0 kernel phi has to be equal to 0. So, that implies phi is injective. And how do you imply a proof 3 implies one. You are given that you define any homomorphism non 0 homomorphism from a to any non 0 ring B. Then it has to be injective you need to prove that B is a field A is a field. So a is given

to be a commutative ring with identity. What you need to prove is that every non 0 element has an inverse. So let us start with an element. Let a be a non 0, x be a non 0 element in A, I want to show that x this a unit. How do you show that x is a unit here? What are the information given? I mean if you have what are the hypothesis if you can define a homomorphism involving x then we can get hold of it. Can you think of a homomorphism like that?

Student: (Refer Time: 15:10).

Yeah.

Student: (Refer Time: 15:12).

If x is not a unit then then this is a proper ideal, ideal generated by x has to be a proper ideal, because this is not a unit implies for any y in a x y cannot be 1, or x y cannot be a unit. So therefore, the in this ideal you cannot have a unit. So therefore, this has to be a proper ideal now define a map from, so this is a proper ideal implies that this is non 0. So I have a ring homomorphism the natural map, ring homomorphism from A to A mod x. And what is the kernel of this homomorphism?

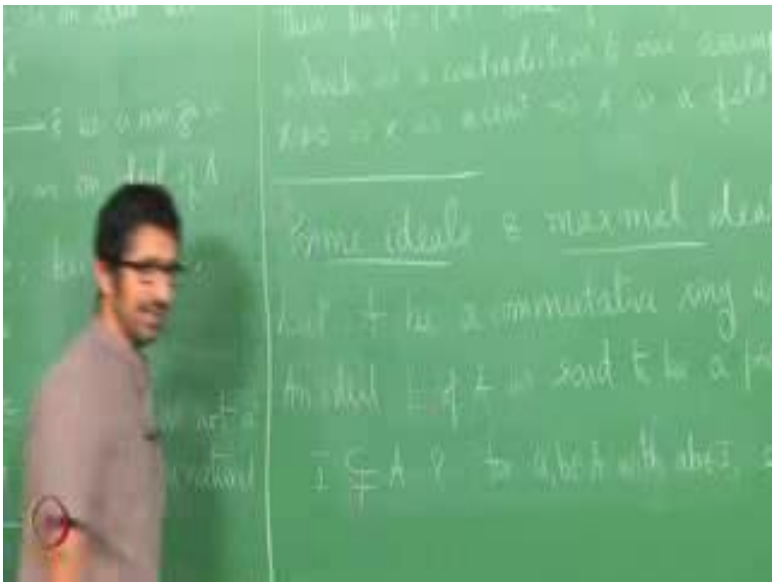
Student: (Refer Time: 16:18).

Ideal generated by.

Student: X.

X, now again there are 2 options. We are saying that it is injective; our hypothesis is that any homomorphism is injective, but then this has a kernel. Unless this is 0 this has a kernel. Therefore, so consider the homomorphism consider the natural homomorphism.

(Refer Slide Time: 17:02)



Phi from A to A mod x, then kernel of phi is equal to x, by hypothesis it is injective therefore, x has to be 0. That is a contradiction see here we have assumed that x is neither 0 nor unit. It is a contradiction. X is 0 this since phi is injective x is 0 which is a contradiction, to our assumption that x is a non 0. So therefore, we have made an assumption which is wrong; with so after this we have made an assumption that x is not a unit. So therefore, this is wrong here x has to be unit this implies x is unit and that implies a is a field.

So, now this characterizes fields. So now, let us look for you know slightly bigger class of rings, for that we require another tool, which are called prime ideals and maximal ideals. So again our standard assumption is that A is a commutative ring with identity, A be a commutative ring with identity. For the definition of prime ideals, you do not really require ring to be commutative with identity, but for some properties we need that. An ideal I of a is said to be a prime ideal if I guess you have seen the definition if.

Student: (Refer Time: 18:55).

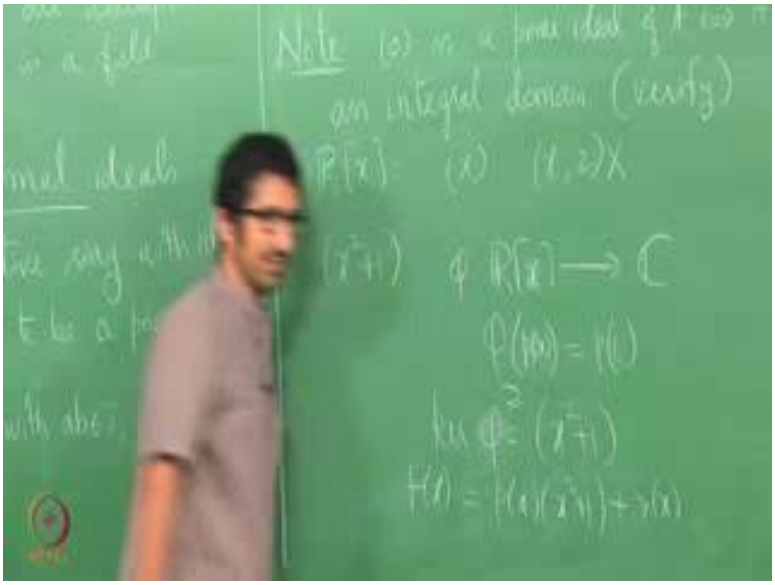
Yeah.

Student: (Refer Time: 18:57).

If for a comma b belongs to A with a b in I either a belong to I or b belong to I, this is; obviously, satisfied by the whole ring right and it is it is an ideal, but we are not bothered

about the whole ring. When we are studying about prime ideals we avoid the whole ring and say that prime ideal if I am a proper ideal of A and these conditions are satisfied. Or in other words a proper ideal is said to be prime ideal if for any product a b belong to a belong to I either a is in I or b is in I. Can you give me some simple examples of prime ideals?

(Refer Slide Time: 21:09)



So, p Z in Z some slightly better in Z do you know only these kind of prime ideals in Z.

Student: (Refer Time: 21:43).

In Z do you know only these types of prime ideals?

Student: (Refer Time: 21:06).

0 right 0 is primary ideals in Z.

Student: (Refer Time: 21:56) proper ideal.

Yes, I is a proper ideal right in Z 0 is a proper ideal right. It is properly contained in A. So this is very important that you know this is indeed a prime ideal. In fact, can you make a more general statement?

Student: (Refer Time: 22:19).

Is 0 is a primary ideal of any ring?

Student: (Refer Time: 22:25) integral domain.

Integral domain because a product has to be is 0 if and only if one of them is 0. So therefore, we should say a note 0 is a prime ideal of A if only if a is an integral domain. So this is try to write down a proof it is very easy, but you should write down; so some more examples of prime ideals. Can you give me an example of a prime ideal in let us say in R x. Ideal generated by x, more?

Student: x comma 2.

X coma x coma 2; will this be a prime ideal in R x?

Student: 2 is an unit.

What can you say about 2? 2 is a 2 is a unit in R x right. It is a unit in R, therefore, it is a unit in R x, therefore, what will this be the whole of R x so this is not a prime ideal. So can you give me some other examples of prime ideals in R x. Can you think of an ideal say other some other linear generated by linear polynomials, can you think of another example with generated by linear polynomials not only x?

Student: (Refer Time: 25:09).

Student: x square plus 1.

Well, x square plus 1. Is this a prime ideal? Why is the prime ideal?

Student: (Refer Time: 25:28).

Well, that is no, we can say that it is fine, but this is you will have to justify that. Ultimately it comes down to one particular property of R x. So we are saying R x, so R x to C this is what you were mentioning, like you can define a map phi of x going to I or phi of p x going to p of I and the kernel is generated by x square plus 1, why is the kernel generated by x square plus 1? Kernel of p x kernel of phi is generated by x square plus 1 why is it so?

Student: (Refer Time: 26:41).

I mean my question is 1. X squared plus 1 certainly belongs to the kernel right. I can understand. So this inclusion is fine, why is it true that you take any element of kernel phi it is in this ideal.

Student: (Refer Time: 27:09).

So, this is what I said this is a very particular property of R x or even more generally f x for any field the property of division algorithm right. This is exactly what we use it boils down to that see if you take any F x here, I can write this as p x times x squared plus 1 plus R x. So to first of all you have to say that no linear polynomials belong here. Because a x a x plus b is in kernel implies a I plus b is 0 which means a I is equal to b, but a is real b is real and I is complex that is a basic property of complex numbers.

So therefore, no linear polynomial is in kernel now if I take any anything bigger than into degree 2 I can write it like this with R x having degrees to p x will be non 0 and R x having strictly degree less than strictly less than 2. Now put x equal to I you see that this is 0 this is 0 therefore, R of I is 0, but that is a linear polynomial at most of degree one therefore, it has to be 0 therefore, f x belongs to so that it is the division algorithm that we are using.

Now, in R x can you give me more prime ideals, can you give me a prime ideal of degree 3, can you give me a primary ideal R x of degree 3 generated by degree 3 polynomial I mean why.

Student: in R p equities data prime ideal R x is a p I is equal to maximum ideal.

No it is much simpler argument.

Student: (Refer Time: 29:36).

Can you.

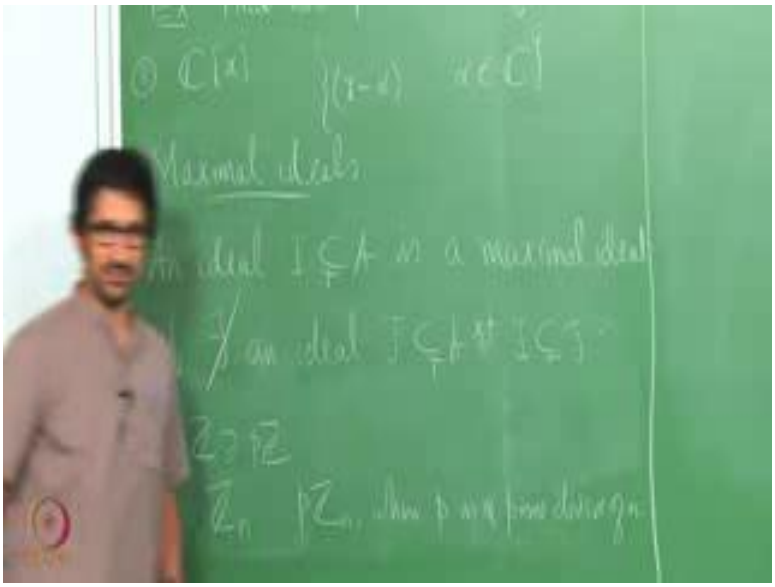
Student: (Refer Time: 29:36) as a root.

Yes.

Student: (Refer Time: 29:51).

It is intermediate value theorem if you take a degree 3 polynomial it has a root in R, therefore, it factorizes in you know so therefore, you cannot have a polynomials of polynomials of degree 3 generate generating a prime ideal.

(Refer Slide Time: 30:14)



So, I will leave this find all prime ideals of R x. Now let us move on what would C x? Quickly tell me, what are the prime ideals of C x ideal generated by x?

Student: X minus alpha.

X minus.

Student: Alpha.

Alpha so the prime ideal is alpha belongs to C. I will leave to you to justify this is what is the reason behind it, what is the reason behind these are the only prime ideals.

Student: fundamental theorem of algebra.

Fundamental theorem of algebra C is algebraically closed right, is that clear to you every polynomial will factorize into linear factors so this is a PID C x is a PID. So every ideal will be generated by a polynomial if it is of degree bigger than equal to 2 you can write it as a product of 2 distinct polynomials. Now it cannot be prime if these 2 factors one of them is not here right. So therefore, if it is of degree 2 or above generated I mean an ideal is generated by a polynomial of degree 2 or above, this can be split into 2 factors of

smaller powers which have not there, so it cannot be a prime ideal. So now, let us let us move on to maximal ideals. So the name suggests what should it be an ideal I is a maximal ideal if there exists a proper ideal an ideal J strictly contained in a and containing I.

If you cannot find a proper ideal containing, the proper ideal properly containing I then I is called a maximal ideal. So let us make some observations first before looking into some examples. Maybe let us take up one or 2 examples; quick examples from the known rings. Let us say Q R 0, Z maximal ideals in Z p Z maximal ideals in Z n. What are the maximal ideals in Z.?

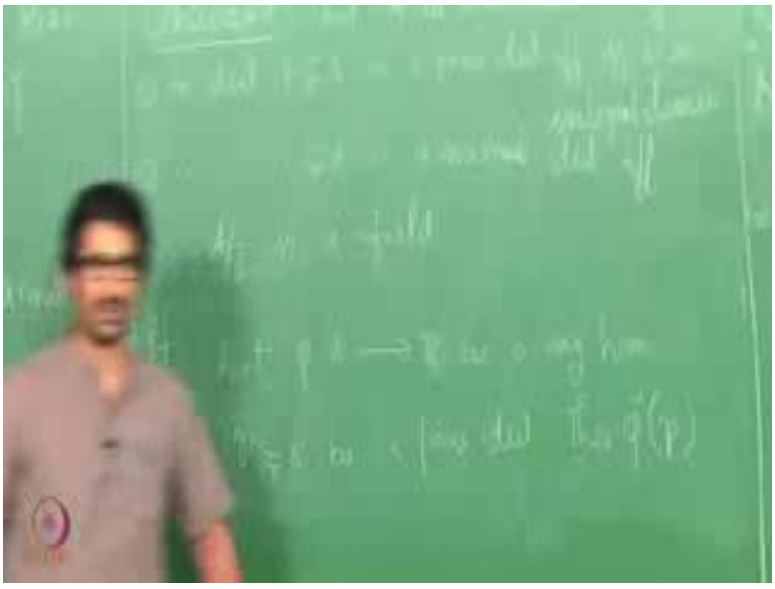
Student: I think prime is equal to 0.

N is prime then 0 if n is not a prime.

Student: P Z in where p is a prime divisor (Refer Time: 35:02).

P Z in where p is a prime divisor. How do you get this? Can you think of a proof? Why is this a maximal ideal? We will come back to this. So first I mean one can of course, in this case it is I mean this is a set that is known to you this is a set that is known to you one can immediately prove it.

(Refer Slide Time: 36:01)



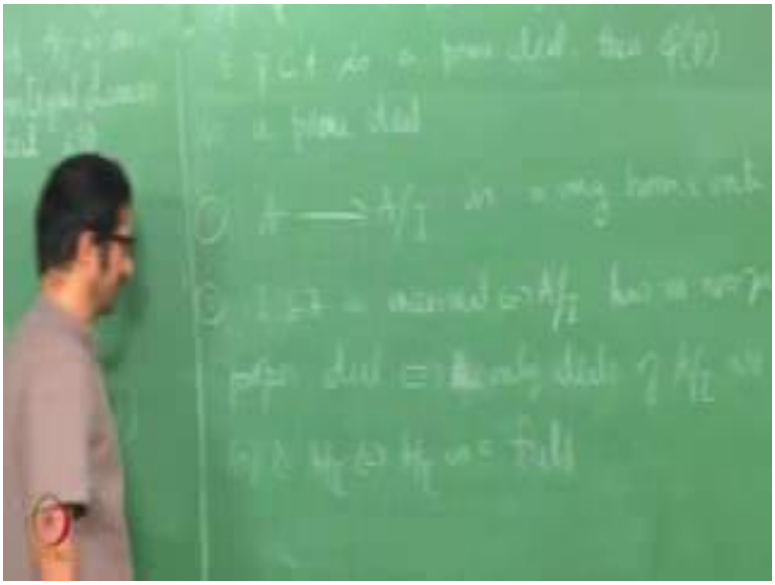
But there is a much simpler way to tackle this which is more general a tool that is more general again observation or remark or note. Let a be a commutative ring with identity and an ideal I is a prime ideal if an only if a mode I is an integral domain. And an ideal I in a is a maximal ideal if and only if a mode I is a field.

This we already saw in a slightly different manner here. So for this we need one more simple observation. Suppose I have a so this is sketch of the proof. If I have let phi from A to B bearing homomorphism, if I take an ideal here it is inverse images an ideal here. This we saw in the last class. Now I you know restrict it to slightly smaller class. Suppose I take a prime ideal then what can you say about phi inverse of p.

It is certainly an ideal. So the question is this a prime ideal, is it? Yes. If you take a product suppose you have A B is in this one, which means phi of A B is in p phi of a b is nothing, but phi of A times phi of B that is in p, but p is prime therefore, either phi of A is in B in p or phi of B is in p or in other words A is in phi inverse of p or B is in phi inverse. So therefore, this is a prime ideal. Now do you see a proof of the first part using the observation the note that we wrote here. 0 is prime ideal in A if and only if a is an integral domain. Now I start with a prime ideal I want to say that A mode I is integral domain.

So 0 you want to say that no here we need slightly, if p is if this is one observation this we require for converse.

(Refer Slide Time: 40:28)



Another observation is that if I have phi from A to B I have a ring homomorphism. If I take A prime ideal in A phi of the prime ideal I mean we have seen that it need not necessarily even be an ideal, but if you put some conditions this becomes an ideal. What are the can you think of a condition for which this becomes. If it is a surjective map then for any ideal I in a phi of I is an ideal in B, now if phi of if p is a prime ideal in A is it true that phi of p is a prime ideal in B. So be a surjective homomorphism and is a prime ideal. Then what can you say about this. Again let us look at I take A B belongs to phi of p. This is a surj, so therefore, I have some a 1 b 1 in a such that phi of a 1 b 1 belongs to a 1 b 1 belongs to a phi of a 1 b 1 belongs here, but then a 1 b 1 belongs to p therefore, a 1 belongs to p b 1 belongs to p either a 1 belongs p or b 1 belongs to therefore, phi of a 1 belongs to p a phi of p or b 1 a phi of b 1 belongs to phi of p.

So therefore, this is a prime ideal now we are ready to see a complete proof of the first part. A is I start with the prime ideal this is the say A to A mod I so for the first one A to m mod I is ring homomorphism, surjective ring homomorphism. I start with ideal I it is a prime ideal. Therefore, it is image is a prime ideal which means it is images 0 here. 0 is a prime ideal here therefore, this is integral domain. So that is the first part. Now assume phi of A mod I A mod I is an integral domain therefore, the 0 ideal is prime ideal here. Now it is inverse image is nothing, but I 0 is prime here therefore, it is inverse image which is I is a prime ideal and that is exactly what we have to prove.

Now, for the second part I is maximal ideal if and only if A mod I is a field. For this one can use the equivalent conditions that we used earlier. So I is maximal suppose this is maximal ideal. If this is maximal ideal how do you say it is a field?

Student: (Refer Time: 44:34).

Yeah.

Student: (Refer Time: 44:41).

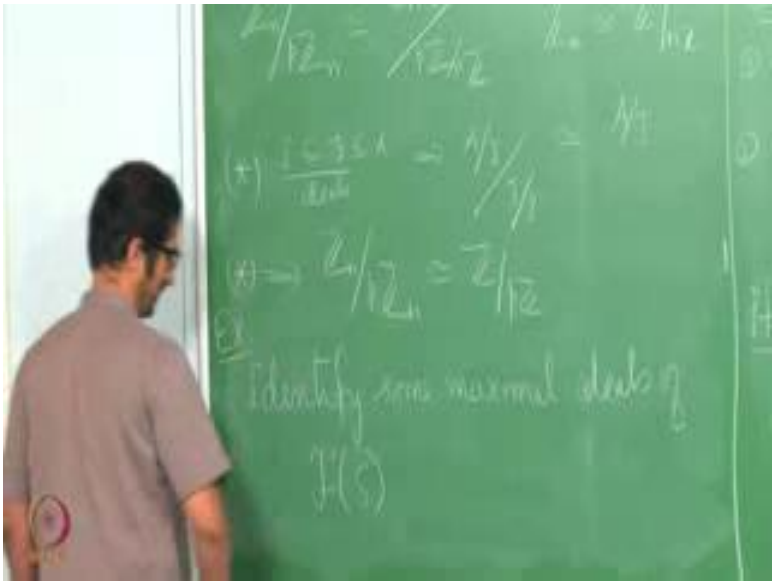
Yes, so you look at this A mod I A mod I has no non 0 proper ideal which implies a mod the only ideals of A mod I are 0 and A mod i; that means, a mod I is a field. Now you can just go back. If a mod I is a field then the only ideals of a mod I are these 2 which means a mod I has no non 0 proper ideals; that means, there are no proper a now again we use the correspondence theorem that we looked at yesterday. Using that we can say

that any ideal here any ideal in this one is in one-one correspondence with ideals of A containing i. So this says that there are no proper ideal containing I and contained in A which means I is a maximal ideal.

Now, let us see few more examples. Now can you tell me why p Z n is maximal, why p Z n x is maximal?

Student: (Refer Time: 46:35).

(Refer Slide Time: 46:33)



Z n mod p Z n; so here we have to use isomorphism theorem. See Z n is isomorphic to Z mod n Z. So this is nothing, but Z mod n Z modulo p Z mod n Z. If I i contained in J contained in a these are ideals of a then a mod I mod J mod I this is isomorphic to A mod J. The second isomorphism theorem again you know you can prove this using the first isomorphism theorem from here send the map to a mod J x plus I say map to x plus J it is kernel will precisely be this therefore, by first isomorphism theorem. This is true, so using this star implies that Z n mod p Z n is isomorphic to Z mod p Z which is a field. And you should in fact prove that any maximal idea of Z n is of this form, you cannot have any other maximal ideals.

Let me conclude today by asking a question, identify some maximal ideals, of we will come and start from here tomorrow.