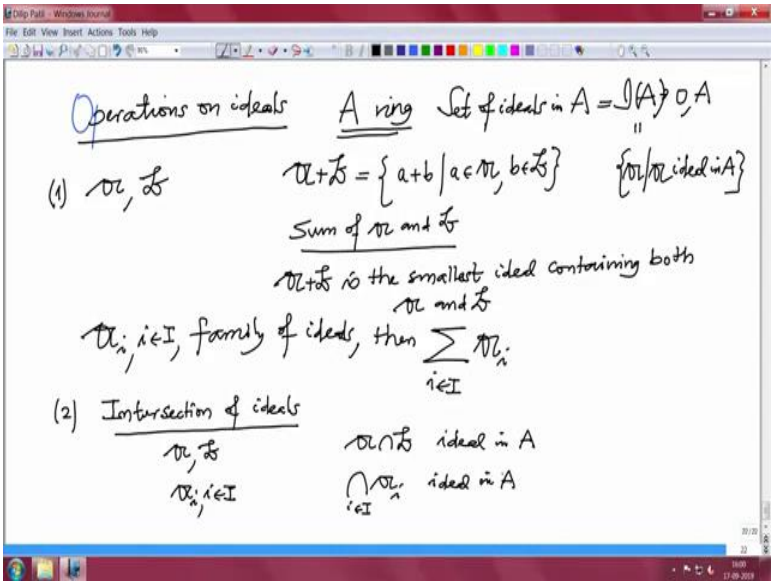
Introduction to Algebraic Geometry and Commutative Algebra
Indian Institute of Science, Bengaluru,
Dr. Dillip P. Patil
Department of Mathematics

(Refer Slide Time: 00:44)



Coming back to this latter half of this lecture, we will continue with the study of ideals. Now we should construct new ideals from the given ideals. So this is comes under the subsection called operations on ideals. So first is if I have 2 ideals a and b, then I can define their sum, and how do I define the sum obviously, what you can do is you take elements from here and elements from here and add them a plus b as a where is in a and b where is in b.

And now you check that this is an ideal, this is obvious because what you can take is it is a subgroup and it is closed under arbitrary multiplication by an element in the ring a. So here, our ring is fixed A is a ring, and we are considering ideals in that ring. So sometimes, the set of ideals in A, I will denote by this IA script IA. So, this is (())(02:10) such that A is ideal in A and definitely this is a non empty set because 0 belongs here ideals 0 belongs here and also the unit ideal belong here.

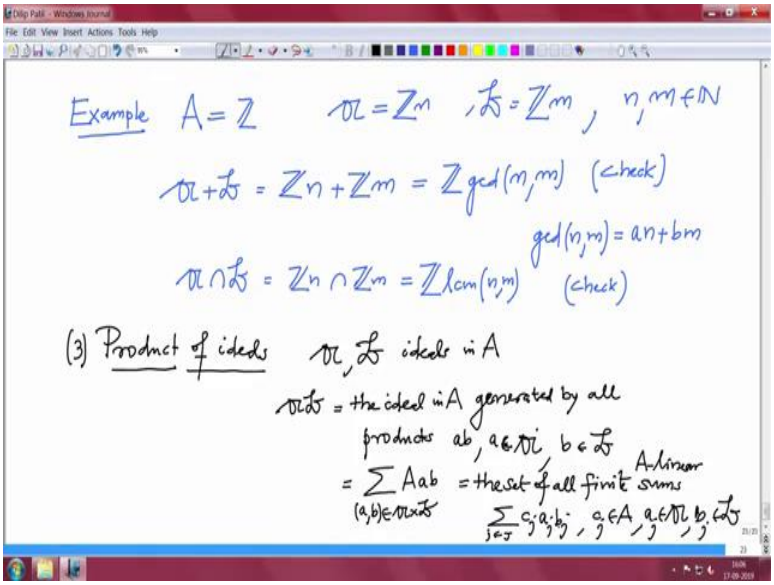
So, there are at least 2 elements there and this set on the set I have defined edition by using the addition in the original ring. If I have 2 ideals then you take their sum or sum elements from the those ideals and check that this is an ideal this is called a sum ideal sum of a and b, and you see you observed that like earlier, you it is it may be sometimes better to define this is smallest ideal which contain both. So, this is a smallest a plus b is the smallest ideal containing both a and b.

And see this observation will allow us to define if I have arbitrary family of ideals ai, i n i family of ideals. Then we can define these some i n i ai. Remember we are not taking infinite, the infinite sums this is just a notation for the smallest ideal which contains all of the ideals and definitely there is 1 ideal which contain all of them namely the unit ideal a. So, it makes sense.

So, this was the first operation on ideal to sum operation. So this was 1, 2 this was a bit easier, but now let us take another one the intersection. So, intersection of ideals, so if I have 2 ideal a and b then I look at the intersection a intersection b and check that this is also an ideal in a this is obvious because intersection of subgroups is a subgroup, you would have learned in a group theory and also it is closed under arbitrary multiplication by an element from the ring, because both are satisfy that property.

And similarly, we can actually define these for arbitrary intersection, arbitrary family, if I have a family of ideals ai, then intersection ai this also is an ideal in a, now, it is let me just pause here and look at example.

(Refer Slide Time: 05:45)



So, in the ring A equal to Z, let us see what happens? So, we know that all ideals in the ring Z their principle, and they are unique they unique generator is the natural number. So A is Z n all Z multiples of this n and B is, all Z multiples of m where these n and m are natural numbers. If I have take two such ideals, what will be a plus b, a plus b is in these notation, all multiples of n plus all multiples of m and what is this?

These is always we know this again has to be principal, because we know every ideal in in there Z is principles. So they should be also principle and what will be with the unique generator that is precisely the gcd of n and m, these I would say check this. That is clear because how do you write gcd how do you compute gcd of n and m gcd of n and m is a combination Z linear combination of n and m. So, that is a times n plus b times m.

So, when you multiply this and so on. So, please check this, but this is very very special true in case of Z it is not true in arbitrary ring because this gcd does not make sense in the arbitrary rings. And what will be the multiplication or intersection? Intersection first this will be Zn intersections Zm. And again now you might have guessed this is nothing but ideal generated by the lcm of n and m.

Again check this, this is not so difficult this is the school arithmetic gets converted into these language of rings and ideals on divisibility and so on. So, this was 1 now it intersection now, the next definition about operations on ideals is that is a third one and is a product. You may have

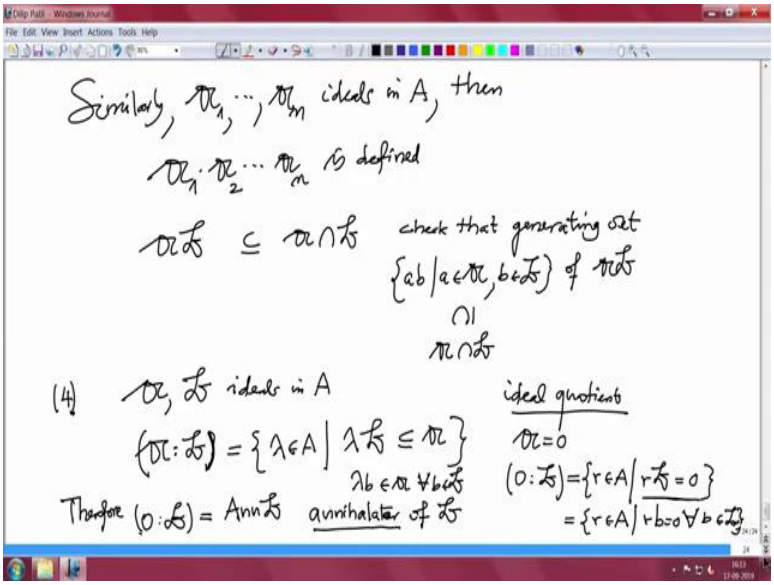
notice that whatever we have studied in arithmetic in the school now we are trying to study that arithmetic for ideals but obviously the ring Z has a special property it has a Euclidean algorithm etc. Arbitrary ring will not have that.

So, whatever machinery we have for Z that may not be available for arbitrary ring. So, things will not go as it goes for the ring Z. So, suppose again for 2 ideals if a and b are 2 ideals in a the ring a, what will be the product ideal? Obviously it suggest that all product should be there, but then the difficulty that it may not form in subgroup.

So then, the right way to say is take this is the ideal in A generated by all products a times b where a is in a and b, a is in the ()(10:19) and B is in ()(10:29) b. So, take the ideal generated by that. So, in our notation it will be like this. So, this is same thing as summation A times ab and the submission is running over ab in a cross b.

These are formal notation. Now these are all principal ideals generated by ab a is a and b is in b. So this means what this we know this is finite sums the set of all finite sums finite a linear sums like this j in j aj. Now I need some other cj aj, pj. Where cj elements are in the ring a aj are in the ideal, a and bj are in ideal b. So, that is a product and again nothing special about to, but now we can go only for the finite ()(12:12) because product of, if you are a finite arbitrary family then product will not make sense.

(Refer Slide Time: 12:23)



So, similarly I will just say similarly if a1 to an are ideals in a then the product a 1 times a 2 times an this is defined. And what is obvious is, so I forgot to mention for 2 ideals a and b, what is the relation between a times b, a intersection b see this is generated by the products and each product is in a as well as in b. Therefore, each generator of these ideal is contained in this ideals and therefore, this ideal is one of the ideal which contains all the generators here therefore, this is increasing.

So, again check that each generator each did not very good to write like this each generator generating said ab a in a, b in b this is generating set of the product ideal is contained in a intersection b and therefore this is increasing. Now one more operation which I want to introduce now only because later on we do not may not have appropriate place.

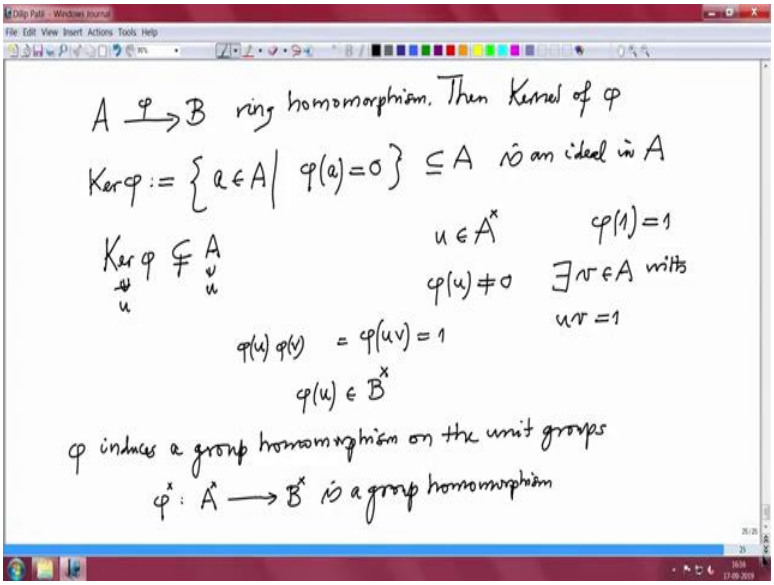
So if I have 2 ideals a and b, this definition which I am making, it is analog to the division. It is analog. We cannot write a divides b but this is similar to that. So, for ideals 2 ideals in a I am going to define colon ideal a colon b this is the notation a colon b this is equal to all those elements lambda in the ring a such that lambda times b is contained in a.

So what does this mean? This means for any b in b lambda times b is an element in the ring a element in the ideal a for every b in b. So this is called a colon ideal or ideal quotient, ideal quotient. This is ideal quotient alright, and obviously this definition is so super so restrictive that we cannot define it for arbitrary ideals, arbitrary many ideals.

So, we will special case where it will be very interesting is when ideal is 0 then what is this? This is 0 colon b means what? Let us write down this definition. This means all those elements let me not use a little lambda word let me use the letter r in a, such that r times b is containing a but a zero. So, r times b is 0 that means what? That means these are all r elements a in a such that r times any b is 0 for every b in b this for every.

This might remind you this is precisely the definition of. So, in 0 colon b therefore 0 colon b is nothing but annihilator of b what is annihilator of b that is all those elements in the ring which kills b see this it annihilates? So this is called a n n ia latter of b lator this is o of b alright. So, that is all about the operations about ideal. I will come back to this again improve this with more observations and examples.

(Refer Slide Time: 18:32)

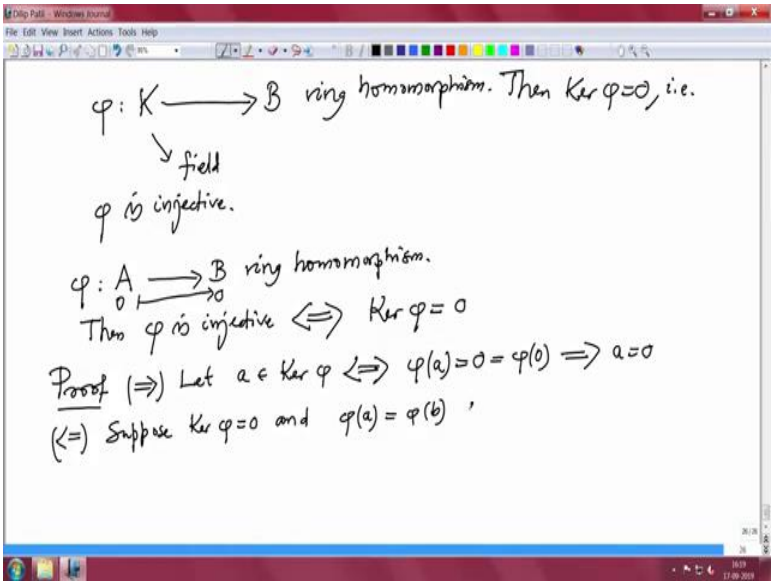


But right now also I want to remind that whenever I have a ring of homomorphism if A to B it is a ring of homomorphism then kernel of phi which is by definition I will write in the notation kernel phi this is by definition all those elements a in a such that phi of a is 0 this is a subset of a is an ideal in a. And note that this is kernel is always a proper ideal kernel of phi is not equal to a because it never contains a unit if you have a unit so, if I have a unit u in a then I just have to check that phi of u is not 0.

That is because, so then this u will not be u will be an element here which u will not be here and why that because I know phi of 1 is 1. This is 1a and this is 1b. So, if I multiply it is a unit therefore, there exist a v in a with u v equal to 1, but when you apply phi to these you get phi of u equal to 1 which is phi of u phi of v. So, therefore, we can conclude phi of u is also unit in B now. So ring (())(20:46) maps units to units.

So that mean this u will induce phi induce, and this is a group of homomorphism on the unit groups. So that means, we have a map which is I will denote by phi cross which is a map from a cross to b cross and this is a group of homomorphism. With respect to the multiplication in a and with respect to the multiplication in b. Now kernel we have noted kernel gives a proper ideal. So, in particular if a were a field then the kernel is not the whole field k therefore, your only chance that it is 0.

(Refer Slide Time: 22:10)



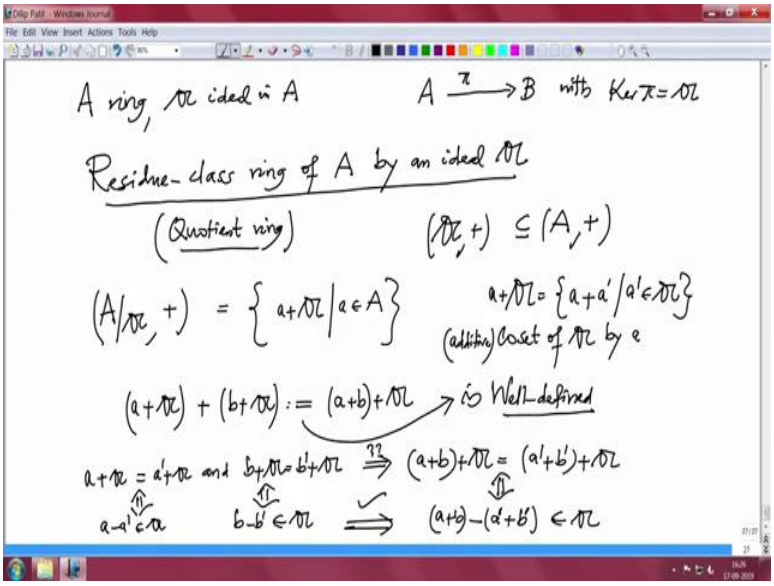
So, therefore, I should note that phi is a map from a field to somewhere b arbitrating and K is the field. This is a field this is a ring homomorphism then kernel of phi is 0 that means that is the map phi is injective. So, more generally I should have noted if I have a ring homomorphism from a to b ring homomorphism, then phi is injective if and only if kernel of y is the ideal 0. So let us write a short proof this is first.

Suppose e is injected and I want to prove the kernel phi 0 so let some element a v in the kernel by but that is equivalent to saying phi of a is 0 but phi is injective. So and also we know it is homomorphism of 0 will go to 0, 0 goes to 0 that is again very easy to prove in in more generally if you have a group homomorphism then the identity in a group should go to identity in the other group.

So but this 0 is phi of 0 but injective phi is injective. So that will imply a equal to 0. So we approved this way conversely suppose kernel of I is 0 and suppose the 2 elements gives the same image in under phi and I want to prove a equal to b for injectivity. But this is equal which saying phi of a minus phi b is 0 but this is same thing as because it is a ring of homomorphism addition etc. This phi of a minus b this is 0 but that is equivalent to saying a minus b is in the kernel phi that is equivalent to saying this is 0.

So a equal to b so that is one way to test. So in this case then a will be a sub ring of b. So now we have seen the kernel is an ideal in general conversely we will now check that if I have any ideal then it is kernel of sum of ring homomorphism.

(Refer Slide Time: 25:34)



Now I am trying to take check conversely that means what I am trying to check I am trying to check suppose if we have a ring A, A is a ring and A is an ideal in A then I want to define ring homomorphism from A to some other ring. So let me write this ring homomorphism special name let me write this name is pi.

So, we are looking for some other ring b and ring homomorphism with kernel of pi is precisely A. So you want to construct pi you want to construct ring be, we want to construct a ring homomorphism phi such that kernel of phi precisely and this is precisely called construction of residue class rings of A by an ideal boutique. This is also called quotient ring of A by an ideal this one.

So, this is similar this you will already have seen the construction in groups, if you have a group and you have a arbitrary sub group will not work because something I should be well defined and then you lead a normal condition there, but we have advantage here our rings are accommodative. So that will help us to go quickly.

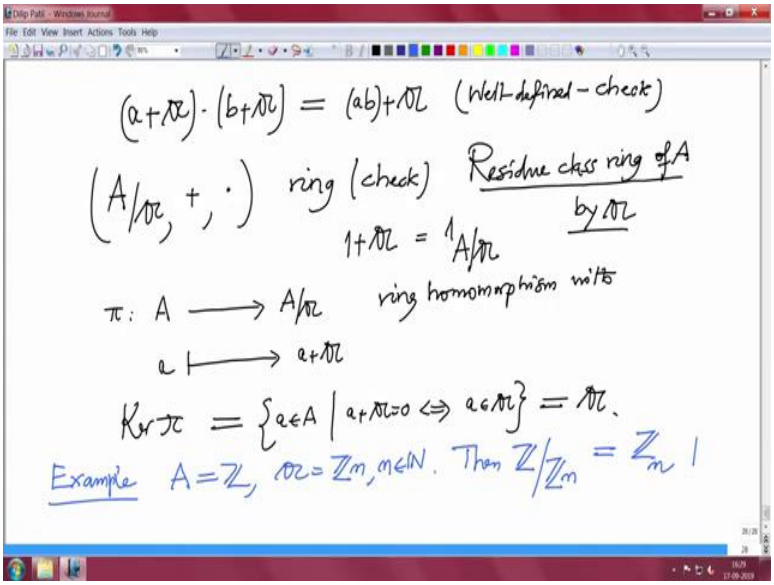
So, this ring what am I doing? So, remember these the (())(27:32) ideal A under addition, this is a subgroup of A plus. So, this is a group a billion group and this is a sub group. Therefore, this quotient group makes sense this is a quotient group. So, what are the elements? The elements are the cosets so, a plus a this is a co-sets and then you look at this co-sets. So, as a where is in a but obviously 2 cosets can be equal for 2 different elements.

So, and what is the co-set a plus a, a plus a by definition this is the small a plus arbitrary element of a. So, that is plus a prime let me write it a prime in a. This is a co-set additive co-set of the ideal a by this element a. And you know then how do you define a group structure here? We have a plus a that is 1 co-set another co-set, another co-set b plus a. Then you define these as a plus b co-set of this (())(29:14) by the sum a plus b. And now we will have to check that this definition is well defined. That means, this definition does not depend on the representative of a representative of be.

So, I will only write down the problem and I will leave it for you to check this is correct. So if that means if a plus a equal to a prime plus a and b plus a equal to b prime plus a that means the co-sets these representatives are the co-set representatives of this of co-sets, they may be different but 2 co-sets are equal, then a plus b plus a is also same thing as a prime plus b prime plus a. And now, how do you prove once you write down this what does this mean then it will be clear.

So, this is equivalent to saying a minus a prime belongs to a and this is equivalent to saying b minus b prime belongs to a and this is similarly, this is equivalent to saying a plus b minus a prime plus b prime belongs to a. This is what we want to check this what we want to check, that means equivalent we want to check this but we have given this. So when you add it you get this so, that is obvious So, therefore, this operation is well defined.

(Refer Slide Time: 31:14)

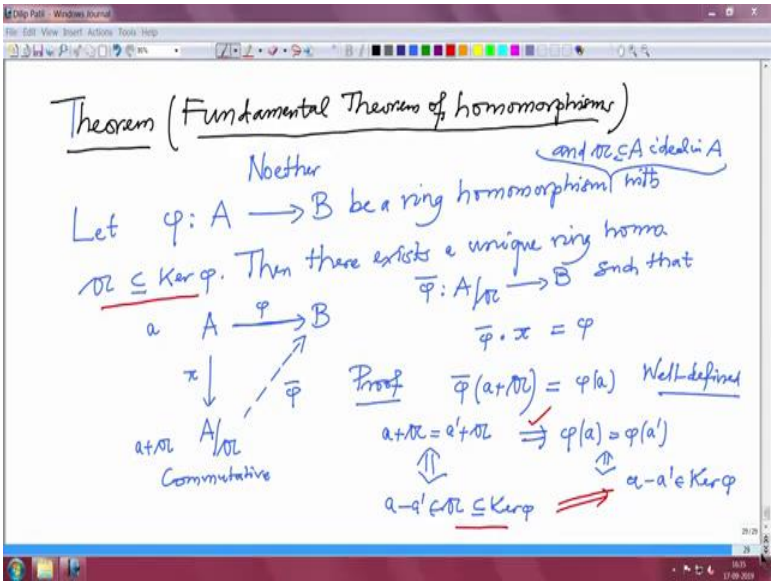


Now, I want to define the multiplication and that gives you a clue how to define a multiplication also. So, if I have 1 co-set a plus a, another is b plus a, then multiply them by just writing ab plus a. And now again we have to check it is well defined, I will just say check. So, therefore, and with this 2 definitions, this quotient group will become with this multiplication, this will become a ring that you have to check.

Again check that means, it a (())(31:36) group it is monoid and there is an identity element and what is the identity element identity element if precisely 1 plus a. This is identity element this is, 1 of the quotient ring all right and therefore and also the pie map is obvious now. That is a going to a by a this map is defined simply an element a goes to the element the coset by a. Now, this is the way we have defined this is a ring of homomorphism with kernel of pie equal to you see what all those elements a in a such that a plus a is 0 part which is equivalent to saying a belongs to the ideal a.

So, this kernel precisely the ideal a. So, what do I object is given an ideal a there is a ring of homomorphism from a to some other ring. These is not the only ring where a will be the kernel but there may be some other also. But this is a very natural contrition, this ring a is called a residue of class ring. Ring of A y the ideal A for example, if you take A to be Z and ideal a to be the principal ideal generated by these n and natural number then Z this quotient ring is nothing but z modular n this. So, I will come back to some more.

(Refer Slide Time: 34:40)



The last proposition here is about this is called usually the fundamental homomorphism theorem fundamental theorem homomorphism. So what does it say? So this theorem this is fundamental theorem of homomorphism. This is usually when the writes in the first books on the ring, but I must mention this is actually proved by Noether's these are also called Noether's still Noether's theorem.

So, what is it? So let phi from A to B be a ring homeomorphisms then there exist, let me be a little bit more general then if it is ring homeomorphisms with and A is an ideal in with the ideal A is contained in the kernel phi. So I should have said in the beginning, let and a in a ideal in a with ideal a is contained in the kernel phi.

Then there exist a unique ring homeomorphisms from, so A is here this A quotient to A by A is here and this b is here, this is our given phi this from the ring a and from the ideal a we have this residue class ring and this pie ring homeomorphisms there exist a map from this that leads denoted by a phi bar there exists a unique homomorphism phi bar from the quotient ring A by A to B such that this diagram is commutative that is when I say this diagram is commutative.

That means, you see, usually there will be one point where you can go this way and then from this point you can go this second way. So, this should be same, such that phi equal to, so that is

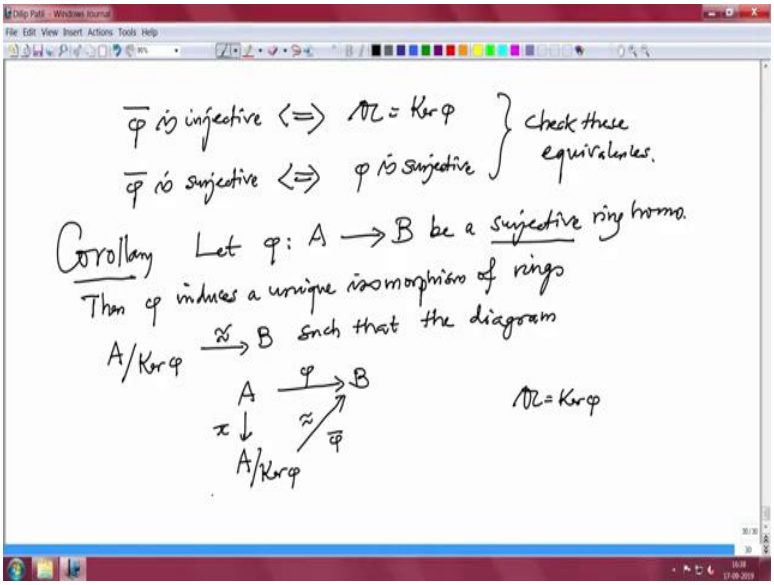
this equal to pie followed by phi bar pie compose phi bar. So, proof, let us write quick proof, I want to define what is we want to define this, we want to define phi bar that means, I want to define what is phi bar of the co-set? But then this commutative demand will dictate what to do this a plus this co-set is here, this is a co-set of this a and this a will go somewhere here phi b and we want this equality.

So, we are forced not b sorry a this is a and we can define this now, as usual we have to check that this definition is well defined. Simply whenever we are defining a map from a quotient set to somewhere you always have to check that map is well defined and what does that mean that means, if I have another co-set a plus a and a prime plus a these 2 co-sets are equal then I have to check this side is equal then this map will be well defined and in the commutative it will be obvious because that is how we have. We are force, but what does this mean.

This means the difference a minus a prime will be a and what does this mean? This mean a minus a prime belong to the to the kernel pie because when we shift to this and then use the ring homeomorphisms. So, it is in the kernel pie and what is a given the relation between this and the kernel that this is contained in the kernel that is given see, this is given to us.

So, this is given to us, and then that will mean this and that is equivalent to say this we have checked this. So, well defined is checked and ring homeomorphisms we have to check it is a ring homeomorphisms that is again I leave it to you and commutative is force so, that it is it is clear. So, I will just drive one corollary from this

(Refer Slide Time: 40:58)



So, because 1 corollary I will define this. So when is this phi bar injective phi bar is injective if and only if is precisely the kernel and phi bar is surjective if and only if phi is surjective. This is again I would say obviously you check these check these equivalences and then therefore I can state the corollary. So corollary, let phi be a ring homeomorphisms from A to B be a surjective ring homeomorphisms then there exists then phi induces a unique isomorphism of rings a mod kernel of phi to B such that the diagram A here b here phi this A by kernel phi.

This is a residue class ring by this ideal kernel phi this is our pie such that this map, this is phi bar and this is an isomorphism. Isomorphism of ring means it is a bijective ring morpohism or you equivalent their existing morpohism in the other direction so that both composites are identity. This is just this observation because C is surjective given here.

Therefore, this map phi bar surjective from the corollary I am applying the theorem to the ideal A equal to the kernel phi and then first we will tell you the cyber is injective and second of the ration will tell you this cyber is surjective therefore it is bijective. Therefore, this is a ring of isomorphism.

So, I will now stop here and the next lecture now I will have to digress a little bit about special kind of ideals, namely prime ideals and maximal ideals. And after that, we will also go a little bit basics about the modules. With this I will stop here and we shall continue it in the next lecture. Thank you.