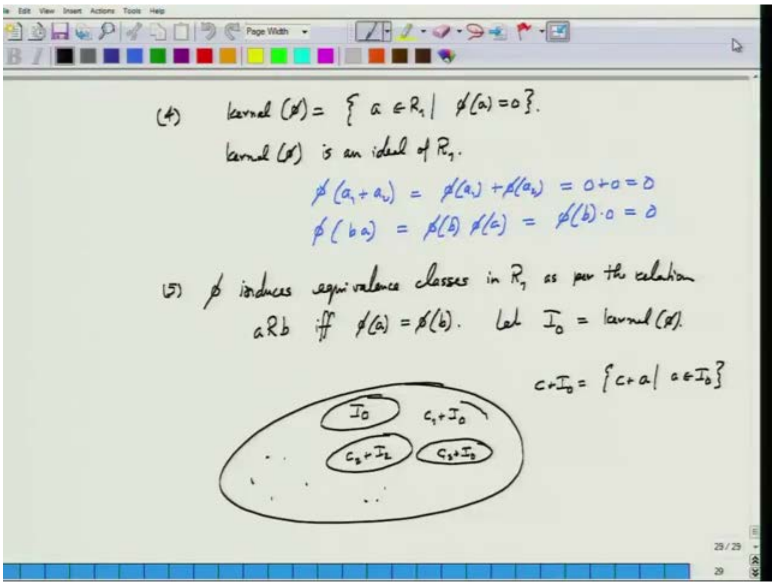
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture – 13
Rings: Quotient Rings

Let us continue from where we left off yesterday.

(Refer Slide Time: 00:17)



(4) kernel $(\phi) = \{ a \in R_1 \mid \phi(a) = 0 \}$.

kernel (ϕ) is an ideal of R_1.

$\phi(a_1 + a_2) = \phi(a_1) + \phi(a_2) = 0 + 0 = 0$

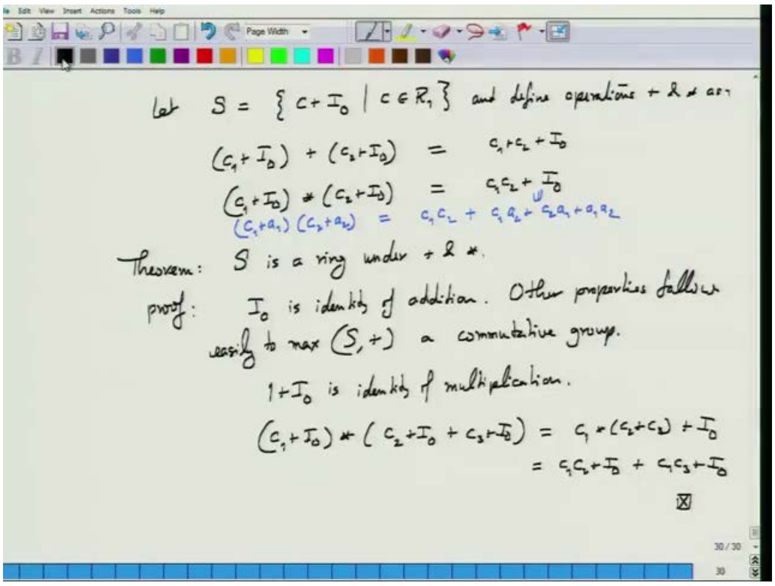
$\phi(ba) = \phi(b)\,\phi(a) = \phi(b) \cdot 0 = 0$

(5) ϕ induces equivalence classes in R_1 as per the relation aRb iff $\phi(a) = \phi(b)$. Let I_0 = kernel (ϕ).

$c + I_0 = \{ c + a \mid a \in I_0 \}$

We started with the ring and looked at the one ideal of the ring, which is in this case called the Kernel, defined by the homomorphism. And then, we realized that this ideal induces equivalence classes in the ring. And, now the question was that can we define another ring made of this equivalence classes. So, did any of you think about it? No? What would be your guess? Can we get another ring of these equivalence classes, like we got for the groups? Yes, we can actually. So, here is.

(Refer Slide Time: 01:27)



let $S = \{ c + I_0 \mid c \in R_1 \}$ and define operations + & * as:

$$(c_1 + I_0) + (c_2 + I_0) = c_1 + c_2 + I_0$$

$$(c_1 + I_0) * (c_2 + I_0) = c_1 c_2 + \overset{\cup}{I_0}$$

$$(c_1 + a_1)(c_2 + a_2) = c_1 c_2 + c_1 a_2 + c_2 a_1 + a_1 a_2$$

Theorem: S is a ring under + & *.

proof: I_0 is identity of addition. Other properties follow easily to make $(S, +)$ a commutative group.

$1 + I_0$ is identity of multiplication.

$$(c_1 + I_0) * (c_2 + I_0 + c_3 + I_0) = c_1 * (c_2 + c_3) + I_0$$
$$= c_1 c_2 + I_0 + c_1 c_3 + I_0$$

☒

If we define; let say S to be this collection of equivalence classes. And, define operations addition and multiplication as. So, this is one equivalence class; this is another equivalence class. And, I am defining their sum.

Now, although I am using plus sign here, where it is being used in two ways; one is the plus within the ring R 1; which is what is meant by this plus and this plus. And, this is the addition of the equivalence classes. So, you must keep this in mind while you are looking at such an expression. This is defined as simply C 1 plus C 2 plus I 0. So, both the pluses are within the ring R1. So, you simply add these two elements C 1 and C 2 plus I naught is whatever is the equivalence class that we get. And, similarly C 1 plus I naught multiplied with C 2 plus I naught is defined as C 1 C 2 plus I naught. So, this is the definition of these operations on the set S.

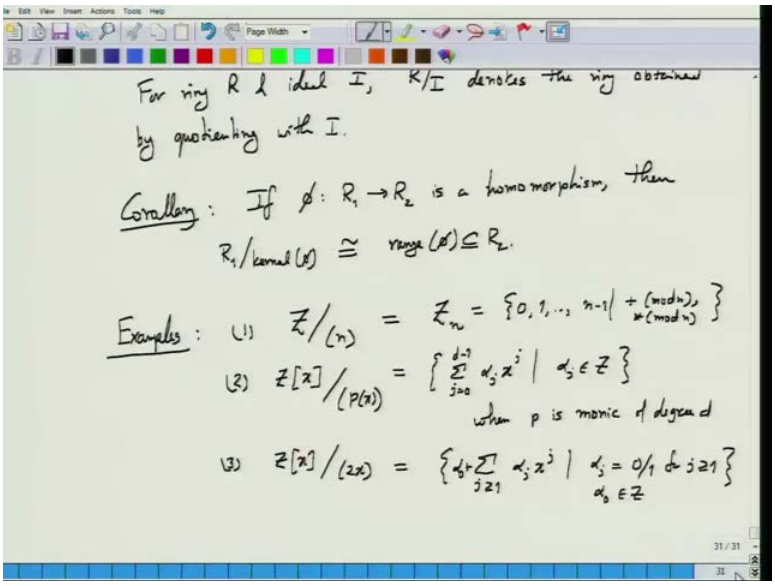
Now, we need to verify that these operations on the set S make it a ring. For that, we have to see that it is a commutative group. So, let us look under addition. So, firstly the closure under addition is by definition. With two equivalence classes, I add another; third equivalence class. Associativity is also clear, again by definition. Commutativity is clear by definition. How about the identity? Well, I naught is identity; right because if when you add I naught to any C plus I naught, by definition we will get this C plus I naught. And the inverse, while C plus I naught will have as inverse minus C plus I naught, whatever their equivalence class is.

So, here every element of the ring R 1 is in one of the equivalence classes. If you look at whatever equivalence class, the element minus C belongs to that is same as minus C plus I naught, and then you add these two. The other properties follow: now, for multiplication again the closure is clear, associativity is clear, it is also commutative, is commutative ring, it will be other. The identity is only thing one has to worry about. What is the identity? 1 plus I naught is the identity. The other properties follow: the distributivity of multiplication over addition that also follows.

You see that. Let us see. C 1 plus I naught multiplied with C 2 plus I naught plus C 3 plus I naught; this is equal to. And then, this is same as. The heart of all of this, even this might appear a little strange or funny to you. The reason why all of you go through is at its code, the following: that when you look at these two equivalence classes, take any element on this equivalence class and any element in this equivalence class. Add it. Add these two elements in the ring. That would be long to this equivalence class. C 1 plus let say a 1 in I naught plus C 2 plus a 2 in I naught is same as C 1 plus C 2 plus a 1 plus a 2 and a 1 plus a 2 is in I naught. So, clearly it belongs to this equivalence class.

So, this addition respects the equivalence classes. Two equivalence classes on the whole get added and make it third equivalence class. Similarly, in the case of multiplication when you look at C 1 plus a 1 C 2 plus a 2 here, what do you get? You get C 1 C 2 plus C 1 a 2 plus C 2 a 1 plus a 1 a 2. Now last three, they all belong to I naught. So, even plot multiplication of the equivalence classes respects this equivalence class. And that is why all these properties remaining very straight forward. So, we do get another ring by quotient. And then, we will use a very similar terminology now, for this quotienting with the ideal.

(Refer Slide Time: 08:53)



For ring R & ideal I, R/I denotes the ring obtained by quotienting with I.

Corollary: If $\phi : R_1 \to R_2$ is a homomorphism, then

$$R_1/\text{kernel}(\phi) \cong \text{range}(\phi) \subseteq R_2.$$

Examples: (1) $\mathbb{Z}/(n) = \mathbb{Z}_n = \{0, 1, \ldots, n-1 \mid +(\text{mod } n), *(\text{mod } n)\}$

(2) $\mathbb{Z}[x]/(p(x)) = \left\{ \sum_{j=0}^{d-1} \alpha_j x^j \mid \alpha_j \in \mathbb{Z} \right\}$

when p is monic of degree d

(3) $\mathbb{Z}[x]/(2x) = \left\{ \alpha_0 + \sum_{j \geq 1} \alpha_j x^j \mid \begin{array}{l} \alpha_j = 0/1 \text{ for } j \geq 1 \\ \alpha_0 \in \mathbb{Z} \end{array} \right\}$

R slash I will represent that ring. And then, it follows essentially as a corollary. That if phi R 1 to R 2 is a homomorphism; if phi is homomorphism from R 1 to R 2, then if you look at range of phi which is all elements of R 1 under phi, the elements in R 2 that they are mapped to that is a range of phi. That is also a ring.

We can just simply borrow this; that is, subring of R 2. And, this R 1 quotiented with kernel of phi is isomorphic to that subring of R 2. This is again exactly the same way as we did for groups. The same theorem extends here. So, quotienting with ideals allows us to create new rings. Again, this (Refer Time: 10:45) allowed us to create new groups.

So, let us see some examples. So, start with Z and pick an ideal of Z. Any ideal of Z is a principle ideal, which is they say multiples of n; and, you quotiented the ideal; the principle ideal n. We get another ring. What is that ring? Yes. So, this is again this will be all equivalence classes formed by this principle ideal n. And, they will precisely be n equivalence classes. And that is simply Z n; numbers between zero and n, an addition, multiplication; addition is modular n, multiplication is modular n; because in that quotient ring, you see that when it or rather I should say quotienting by the principle ideal n is equivalent to taking numbers and operating on them and quotienting modular n, dividing by n and taking the remainder.

So, this is again occurring. I mean, again in for groups also we had Z n, but there only had addition modular n, there, when this was the sub group n Z. Now, we have an ideal which is something as more structure. So, we get actually both the operations; all this right.

Let us go ahead. Some other examples, what are the rings have we come across? (Refer Time: 12:57). And, let us look at Z x. What could be an ideal in this? Take any polynomial; take any polynomial say principle ideal polynomial generated by some polynomial. And that is equal to what? See, if the polynomial p is of degree d less than d, there is a small caveat here. That it is simpler to describe if p is a monic polynomial degree of d; that is the coefficient of x to the d is 1. If it is not 1, then it becomes slightly messy. It can still be described in exactly the same way, but a bit little bit of twist.

So, in case it is monic, then it is simply; whole coefficient will have to be integer because it is a, but they are all be multiples of that whatever if the leading coefficient of p, the I would not say there will be multiples or with kind of will be become a little trickier to describe. It will still be integer, but one has to be little careful when defining that.

In fact, let us take an example when p is not monic. Just think out about that. And that is a third example we are saying. How about Z x? And, let me say divide by 2 x. What is this? See, Z x contains of arbitrary polynomials with integer coefficients, whenever their integer coefficient is even, then that will be in this ideal 2 x, except for degree zero coefficients. And then, we can take that out. But, the remaining ones can survive.

So, that would mean that this way; j alpha zero j greater than or equal to 1. That is, this you can update degree polynomials will survive here, as long as their coefficient is the terms coefficient of a power of x. If it is 0 or 1, when it does not fall in this ideal generated by 2 x. And, so those polynomials or those higher powers of the x will survive. And that is what I am writing here. So, it becomes a kind of messy to describe this ring as it goes to that ring.

Student: (Refer Time: 16: 26) 2 x or plus 1 minus.

Yes, it will be more complicated too. So, the moment it is the monic polynomial, it becomes very easy to describe. So, that is one observation that we can make.

Student: What do we make; the any one will be one. Then, we can say that it is correct quotient. We put the condition that for j greater than 1, it should be as a; coefficients will be 0.1. Put the condition that any of the coefficients is 1 then, it will not come in the forms of groups, all other group.

Any one of the coefficient, why not all coefficients?

Student: If x square plus.

Take a concrete example.

Student: x square plus 2 x.

Yes.

Student: So, according to what we have written, it will not come.

It will not come. Yes.

Student: But, which will come in the quotient.

No, why? x squared plus 2 x is same as the x square? Is it? Yes

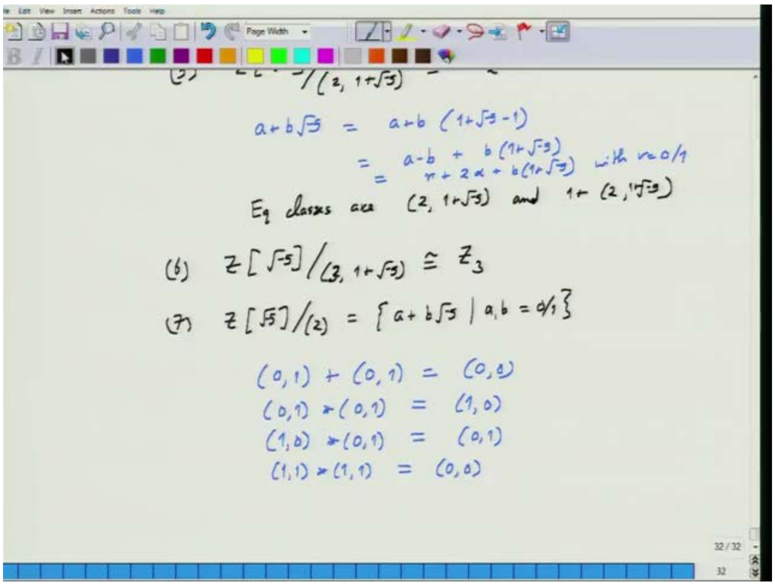
Student: If we do Z x quotient x.

Z x quotient x? Yes.

Student: Then, it is going to come Z.

That is only Z. Yes. That is right. That is nothing else. You can write that Z x quotiented with x that simply isomorphic to Z. More examples; you have seen different other types of rings as well. Yes, we have spent quite a bit of time in this larger class of integers.

(Refer Slide Time: 18:24)



$/(2, 1+\sqrt{-5})$

$a+b\sqrt{-5} = a+b(1+\sqrt{-5}-1)$

$= a-b + b(1+\sqrt{-5})$

$= r + 2\alpha + b(1+\sqrt{-5})$ with $r=0/1$

Eq classes are $(2, 1+\sqrt{-5})$ and $1+(2, 1+\sqrt{-5})$

(6) $\mathbb{Z}[\sqrt{-5}]/(3, 1+\sqrt{-5}) \cong \mathbb{Z}_3$

(7) $\mathbb{Z}[\sqrt{5}]/(2) = \{a+b\sqrt{5} \mid a,b = 0/1\}$

$(0,1)+(0,1) = (0,0)$

$(0,1)*(0,1) = (1,0)$

$(1,0)*(0,1) = (0,1)$

$(1,1)*(1,1) = (0,0)$

So, Z square root of minus 5, for example. What could be an ideal there? We have seen examples (Refer Time: 18:35). That is what? Of course we can look at a principle ideal. And, let say just a multiple of 2, 3 and that would probably not be as interesting. See, some different ideals. How about? Sorry.

Student: That is what 2, 1.

That is one possibility. Yes, we can look at 2, 1 plus square root of minus 5. This, if you remember is a prime ideal, what is this quotient equal to. Let us see what the equivalence classes we get out of this. Only quotient n takes an arbitrary element of Z a plus b square root of minus 5 with an arbitrary element of Z square root of minus 5. When you quotient with this, what happens? Firstly, there is a 2 here.

So, if we can reduce a and b modular 2. So, we can in, and with that all such multiples of two will go inside this ideal. So, what will be remaining is a can be 0 or 1 and b can be 0 or 1. Only four possibilities are left. So, there would be at most this 4 equivalence classes. No more than that 4. Further, then we have 1 plus square root of minus 5. So, we can get rid of 1 plus square root of minus 5. We can replace square root of minus 5 with minus 1 because we can, what you can say a plus b 1 plus square root of minus 5 minus 1. And, there is a minus b plus. So, this goes away in the ideal.

Now, we are just left with the integer a minus b. Now, all multiples of two of this will also going to be in the ideal. So, eventually what will be left with would be just two equivalence classes corresponding to number 0, which is the ideal itself and number 1.

So, take a general element a plus b square root of minus 5. And, I will write it as this. So, I get a minus b plus b 1 plus square root of minus 5; this in the ideal. And, I can further write this as some residue R plus 2 alpha, a minus b is an integer, so you just write it as depending on if it is even or odd as this form. So, R is either 0 or 1, this is in the ideal; 2 alphas plus b 1 plus square root of minus square. This belongs to the ideal.

Student: It will go to the 0.

This will go the 0. So, there will be only two equivalence classes left or two elements left in this quotient ring, which correspond to R being 0 and R being 1. So, these are the two equivalence classes. So, we get a ring with just these two elements; 0 and 1. And, what are the operations on this ring? Well, very naturally. 0 plus 0 is 0, 0 plus 1 is 1, 1 times 1 is 1 and so on. So, what we get really here is this is isomorphic to Z 2.

Student: Suppose, we instead of 1 plus minus 5, we did it with the (Refer Time: 22:54) minus one, then also we will get Z 2.

Z 2.

Student: But, I have these two rings different because.

The rings are different, but they are isomorphic.

Student: (Refer Time: 23:06)

Let see, let us.

Student: Plus something and that.

3, 1 plus square root of minus y z; this would be; I will go modular of a, this will be isomorphic to Z 3. Yes. Let us look at this. Although, I had initially said ignore this, but now we can come back to this and see what this means. R multiples of 2 taken out, so this will leave just 4 elements; how about the operations? This is a ring with four elements. What are the operations or the addition and multiplication? How do they go in this ring?

Student: a 1 plus a 2 (Refer Time: 24: 21)

So, the addition is simply component wise. So, a 1 plus a 2 and b 1 plus b 2 mod 2; how about multiplication? See, if I write, let say, this element has the following simpler form 0, 1; that means, a is 0, b is 1, plus 0, 1. That is 0, 0. How? What about 0, 1 multiplied with 0, 1? What is this equal to? There is square root of minus 5 multiplied with square root of minus five. There is minus 5. Minus 5 modular 2 is 1. This is a 1, 0. What is this 0, 1? 1, 0 is simply number 1. So, 1 multiplied by anything is Z. So, this is the multiplicative identity 1, 0 in the ring. 0, 0 is the additive identity. And, the how about 1, 1 multiplied with 1, 1? This is 1 plus square root of minus 5 times 1 plus square root of minus 5; that is equal to?

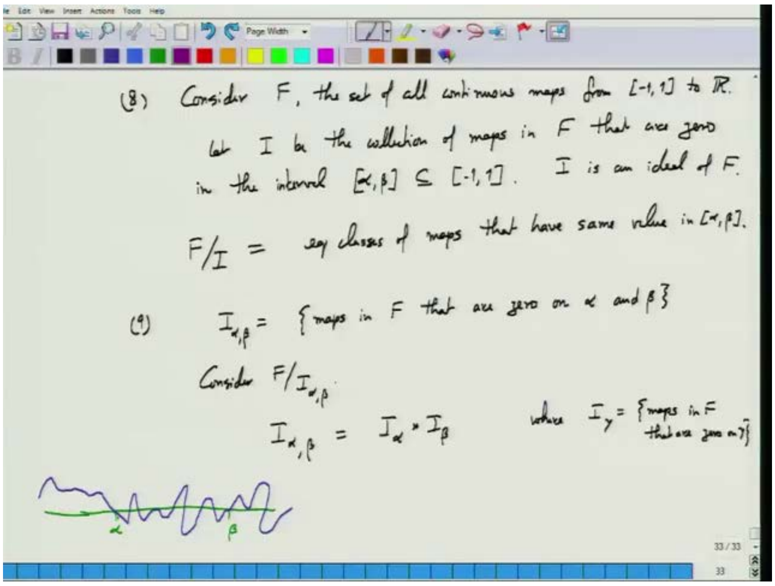
Student: 0, 0.

0, 0; so that is a funny ring. It does not look; is very simply defined. But, early you find that it is a very strange kind of a ring, which even has elements whose product or whose square is 0, non-zero element. Non?

Student: Is not an integral element.

It is not an integral element, certainly, not. Clearly it is; all right. So, it is a ring of four elements, but with a strange structure; any other example? Whether you can think of? Let me go back to this; Some lectures ago, I had created a new example; continuous map. F is a set of all continuous maps from minus 1, 1, interval to R.

(Refer Slide Time: 27:08)



(8) Consider F, the set of all continuous maps from $[-1, 1]$ to $\mathbb{R}$.

let I be the collection of maps in F that are zero in the interval $[\alpha, \beta] \subseteq [-1, 1]$. I is an ideal of F.

F/I = eq classes of maps that have same value in $[\alpha, \beta]$.

(9) $I_{\alpha,\beta}$ = {maps in F that are zero on α and β}

Consider $F/I_{\alpha,\beta}$.

$I_{\alpha,\beta} = I_\alpha * I_\beta$ where I_γ = {maps in F that are zero on γ}

Let us look at that. This, we have earlier seen already. It is a ring. What are ideals in this ring? Certainly, if you collect all maps which is 0 in its particular interval that; so, this collection totally forms an ideal. So, if you let be the collection in a given interval. In that case, I is an ideal of F because instead of two such maps lies in I multiplication of such a map with any other map in F also lies in I. What is F quotiented with I? So, you have to see what are the equivalence classes induced by this quotienting.

Student: All non-zero maps in this.

All non-zero maps in this?

Student: (Refer Time: 29:28)

Instead, what are known? So we get equivalence classes. Each equivalence class will contain a set of maps. What is the property of those set of maps? Equivalence classes will be of the form G plus I, where G is a any map. And all maps in the equivalence class will be of the kind G plus a map in I. So, what is common property of these maps?

Student: (Refer Time: 30:12)

Exactly, in the interval minus alpha, sorry, alpha to beta, they have exactly the same (Refer Time: 30:21).

Student: (Refer Time: 30:56)

Not necessarily constant. They all take on every point between alpha and beta. They take one value. For different point within alpha and beta, the values may be different.

So, the function need not be constant in the interval alpha, beta. They can be varying, but every function in equivalence class has exactly the same value sequence or value series in the interval alpha, beta. They will be infinitely (Refer Time: 31:27)

Student: (Refer Time: 31:28)

Absolutely.

Student: Each equivalence class will have infinitely (Refer Time: 31:33). So, it is a very much bigger in ring than we have seen so far. What it does is this quotienting here is trying is that as if you are saying as if that let us I am going to focus only on the interval alpha, beta. Not clear about outside this interval. Now, give me all continuous functions, which are distinct in the interval alpha, beta. So, the quotienting is just collecting all the functions and making equal all those functions that I agree on the interval alpha, beta; because for the purpose of my analysis within the interval alpha, beta, those functions do not; they are no; those functions are distinct. They have been made the same. And, then we have just looked at the different behavior within our interval alpha, beta.

This is a very important observation because this allows us to, and we will see that later, to look at the functions. Restrict; first we restrict our attention to a certain domain only and look at the functions who that behave differently within that domain. And, it is; and these functions are simply obtained by quotienting operation.

Let us stay with the same example. And, let me define a specific map I (Refer Time: 33:31) not I naught, it is a I alpha, beta. So, I collect all the maps that take zero value on these two points; alpha, beta. They may take values zero and other points. This is also an ideal. Do you agree with me? This is also an ideal. So, I can consider F quotienting this ideal.

How does this ideal look? This has all the maps that take the same value on these two points' alpha and beta. Or, rather it collects the equivalence class in this, all those maps, which have the same value on the points' alpha and beta.

Now notice that I alpha, beta, I can write as. See, this is an ideal in the ring F. And, all these three are ideals in the ring F. The product of I alpha and I beta, any element of this product has the form, and it is a finite sum of a map in I alpha and a map in I beta; finite sum of products of this form - a map in I alpha, a map in I beta. So, any such product of a map in I alpha and a map in I beta would be 0 on both alpha and beta. So every function, every map in this would be 0 and alpha and beta. But, there only shows one ring. How about taking a map which is 0 on both alpha and beta? Can I write it as product in this form?

Student: (Refer Time: 36:35)

If a map is 0 on both alpha and beta, can I write it as a product of two continuous maps? One of them is 0 on alpha and other is 0 on beta. What is an ideal is? So, you just write. Yes, if you look at a map F in I alpha beta which is 0 on both alpha and beta, you write it as, let say, map is g. And, look at the map; square root of g. That is also 0 on both alpha and beta. It is also continuous. G is continuous, and then square root of G is also continuous. So, G is square of G times square root of g. Where?

student: (Refer Time: 37:25) was negative.

Yes, then there is a problem. So, square root of G will not always work.

Student: See (Refer Time: 37:32).

But, what about R? You can do something simple enough actually. You know suppose F is a map, so you have an alpha, you have alpha here and beta here. And, for F what we know is what? Wherever F is coming from F is 0 to alpha, not F, some G here. Then, it just goes all over. But, it stays 0 on beta. And then, it again goes over.

So, if you define a map which is continuous, so let us say takes this simple map. This one, this may not work. I think it is a very good home exercise. So, instead of me doing it let me give it you to work out an example. It is very simple. This, you do not have to try anything complicated, just construct. See, you have a lot of flexibility. You have to define any two maps; whose product is equal to this map.

One of them should vanish on alpha, other should vanish on beta. Make one of them vanish on alpha, make one of them vanish on beta. And, define this value on the remaining, on the remaining point, so that the product is the values that we want. You just have to ensure that there is continuity.

Fine, so I will leave it at that and have you work it out. So, that is it for today.