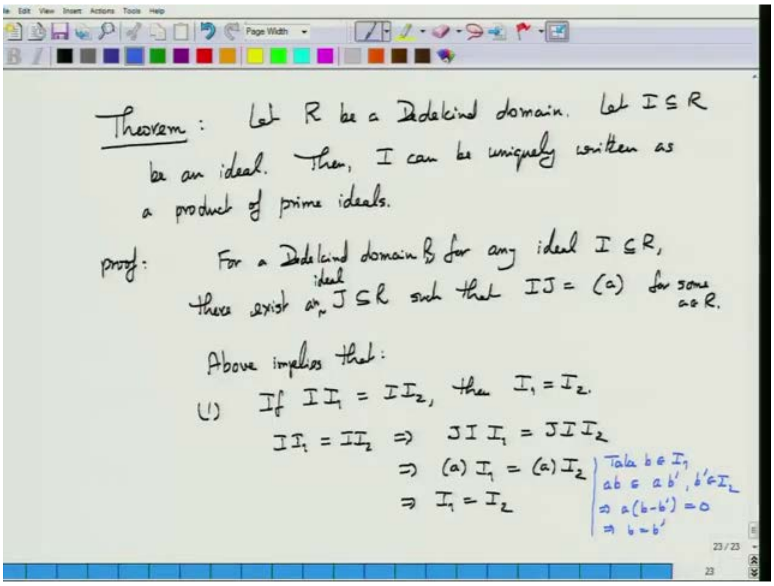
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture – 12
Rings: Dedekind Domains

Today, we partially prove this theorem.

(Refer Slide Time: 00:18)

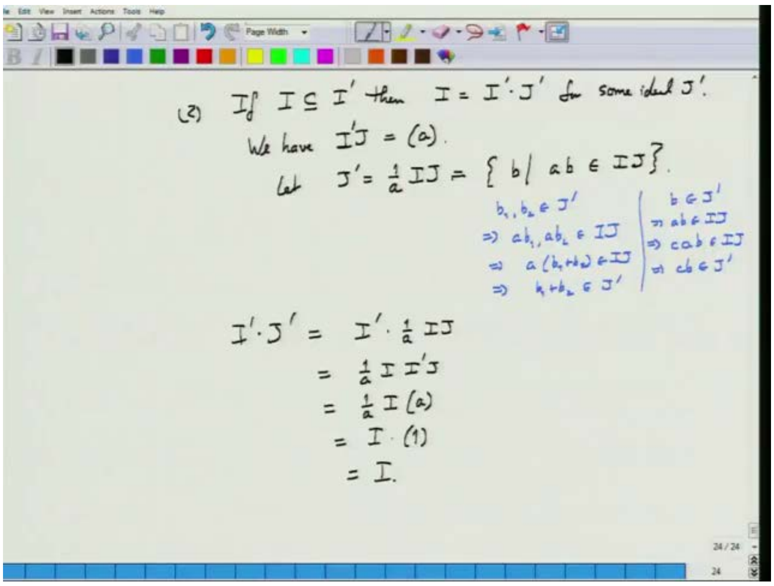


Let R be a Dedekind domain, and let R, sorry, I be any ideal in the ring; then, I can be uniquely written as a product of prime ideals. I will not give you the complete proof of this, because, that requires a… It is not very difficult, but it requires some efforts. So, and I want you to make that effort on your own. So, instead, what I will do is, I will give a partial proof, and leave the rest to you. So, the key property that we are going to make use of is the following. This is the property I am going to make use of. I will not prove this property, and it is a very interesting statement; says that, 'if you have any ideal I in a Dedekind domain, and there exists another ideal J in the ring, such that, I times J is a principal ideal.

So, let us assume this to be true, and proceed with proof. One very interesting consequence of this is the following. In fact, I will show you two consequences. First one is, cancellation; there is 2 products, I I 1 and I I 2 are equal, and these are, of course, all three are ideals; then, I 1 equals I 2. Essentially, it says that, I can cancel I from both sides of the equation; works out exactly the same way as we can cancel numbers. This is not at all obvious, but, we, by using the property above we can make sure of that; how? Well, if you have I I 1 equals I I 2, and corresponding to ideal I, we have an ideal J, such that, I times J is a principal ideal. So, I I 1 equals I I 2 implies, J I I 1 equals J I I 2. This implies, J I is principal ideal a I 1 equals principal ideal a I 2. And, this implies, I 1 equals to I 2, because, you can easily cancel principal ideal multiplication. Why? Take any element b of I 1; then, a b of I 1 is in, a times I 2, ok.

Let us see that; let me write it in a different thing. Correct? Now, a Dedekind domain has the property that, it is an integral domain, which is that, a times c is zero, then either a is zero, or c is zero. In this case, a is surely not zero. This is, of course, follows from this fact, and so, b minus b prime is zero. So, this shows that, b prime, whatever is in I 1 is in I 2; b was in I 2, and b is in, sorry; b was in I 1, and b, therefore, is in I 2 also. and (Refer Time: 06:34). So, that is the first interesting consequence.

(Refer Slide Time: 06:49)

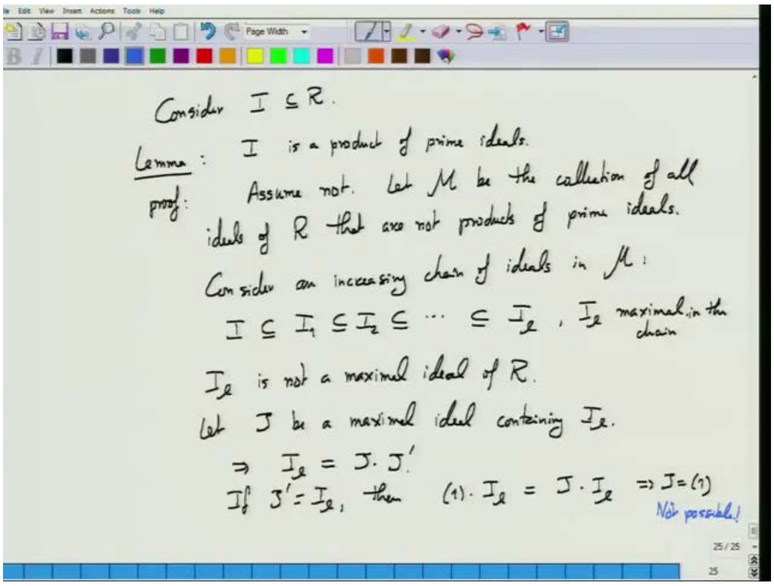


The second one is that, if I is contained in I dash, then, if ideal I is contained in ideal I dash, then I, actually, can be written as a product of I dash with another ideal J dash. The converse of this is always (Refer Time: 07:23); we have seen that; that, if I is the product of two ideals, then, I is contained in both the ideals. In fact, I is contained in the intersection of these two ideals. This, we solve all the time. This shows the converse set.

In case, I are with Dedekind domain, then, containment is sufficient to imply that, I can be factorized as I dash (Refer Time: 07:49). How does this work? So, let us start with this that, we have I times J is a principal ideal; no. In fact, let us, we should use the J corresponding to I dash. So, I dash times J is the principal ideal. So, let now, this requires some explanation, but, before that, let me see if this is working out, yes. I think it has. So, I dash J is a principal ideal, generated by a non-defining J dash, to be I times J divided by a; and I need to explain that. See, I is contained in I dash, which is I dash times J is a principal, equals principal ideal, generated by a. This is another way of saying that, all elements of I dash J are multiples of a. So, since I is contained in I dash, all elements of I J are also multiples of a. And, one by a, simply means that, they just divide all those elements by a. So, the elements in here are multiples of a. So, just cancel out, or take out a from this, and you get elements of I J divided by a. I am not saying that, these are invert, a is invertible; I am simply saying that if a times b is in I J, then b is in J dash.

So, this is defined as set of all b s, such that, a b is in I J. And, since we know that, every element of I J is of the form a time b, so, this definition makes sense. J dash is an ideal; because, if b 1 and b 2 are in J dash, then b 1 plus b 2 b 1 b 2 in J dash means, a b 1, a b 2 is in I J. This implies that, there is in, I J is an ideal; a b 1, plus b 2 is in I J. And, this implies that, b 1 plus b 2 is in J dash. And, similarly, if you have b is in J dash, then, a b is in I J, implies some, any times c a b is also in I J, this being the, I J being an ideal; this implies that c b is in J dash. So, that shows that. So, J dash is an ideal of R. And now, let us look at what is I dash times J dash. What is this equal to? Is it I dash times 1 by a I J? Is this? Just rearranging, because this is commutative multiplication, I dash J, by definition is, yes, what is 1 by a times principal ideal a? This has all multiples of a. Sorry, is R itself; or, this is just one, principal ideal 1. And, any ideal times principal ideal 1 is just I; because this shows that, I factors as I dash J dash. Two very interesting properties follow by that result, and we will make use of both of these.

(Refer Slide Time: 12:38)

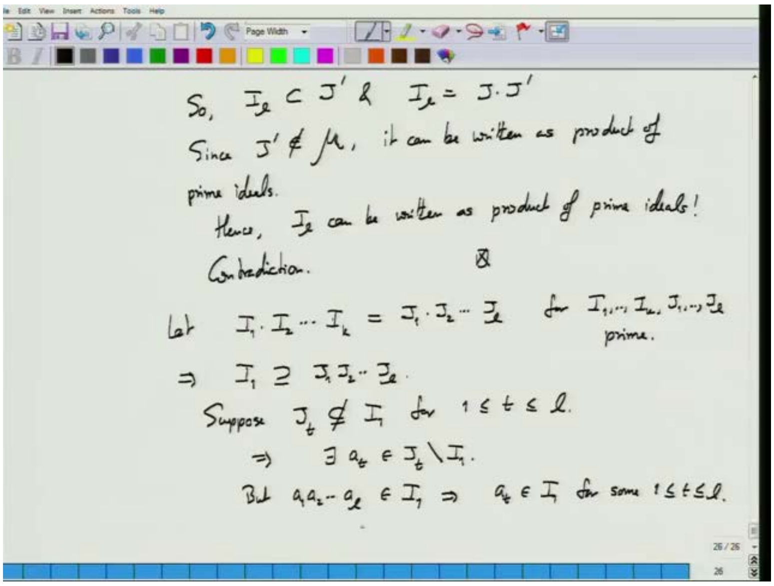


Ok. So, now, let us consider I and R; it is an arbitrary ideal in the Dedekind domain. First, I will show that, I is a product of prime ideals. Let us assume, for the sake of contradiction that it is not. In fact, I will say that, let. Let us collect all ideals of R, which are not products of prime ideals. Let this collection be (Refer Time: 14:05) as M. I am going to show that, this collection is empty; and, that will prove the (Refer Time: 14:12). Well, since our assumption is that, it is, M is not a, I is not a product of prime ideals, then, M is not empty; theoretically, because I is in M.

Now, consider a maximal element in M; that is, start with I; see if this collection M has an ideal, which is a super set of ideals; and, keep taking larger and larger sets, containing the previous ideals; larger and larger ideals. And, by the fact that the ring is (Refer Time: 14:55), one of the consequence of that is that, any such chain of increasing ideals is going to be finite; because, you can realize that quickly, because, all ideals are finitely generated. When you look at an increasing chain of ideals, you are basically saying that, you are increasing the number of generators, essentially, one by one. And, since there are only finitely many generators in the ideal, total, any ideal is only finitely generated. So, there will not be many, or only a finitely many ideals in this chain. That is a bit of a intuitive proof, not a formal proof, but we can formalize it along these lines.

So, consider an increasing chain of ideals, which starts with I contained in I 1 contained in I 2, I l; and, I l being the maximal in this chain. So, any ideal that strictly contains I l is outside. Now, I l cannot be, it is not a maximal ideal of R; I l is maximal in the chain. There is, there is no ideal bigger than I l in this chain, but if you look at the ideal I l, it is not a maximal ideal in the ring R; because of the property we proved that, every maximal ideal is prime. So, if an ideal is a prime ideal, then, of course, it can be written as a product of prime ideals. So, I l cannot be maximal. So, let us say, let J be a maximal ideal, containing I l; fine. So, J contains I l. Now, invoke the property number two, which we just showed; that means, and I l can be written as J times some J dash, where J dash and J both, of course, J contains I l; J dash will also contain I l. Yes, can J dash be equal to I l? Then, one times I l equals J times I l, J dash being equal to I l; and, I l equal to J dash I l, this implies… All J s are non-trivial, of course; why, because of the cancellation. Of course, so, yes. J as a maximal ideal, by definition is non-trivial; in the sense, it is not equal to the full ideal; then, by cancellation, J equal to 1 not possible. Therefore, J dash is not equal to I l.

(Refer Slide Time: 19:02)

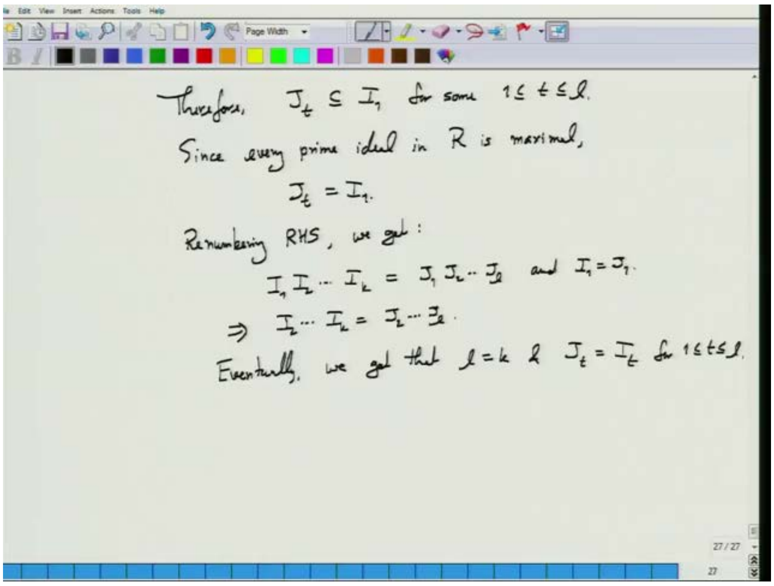


So, I l is strictly contained in J dash, and I l equals J times J dash. Now, J is a prime ideal in itself; J dash is a strictly larger ideal than I l. So, it is not in M, which means, J dash can be written as a product of prime ideals; which means, I l can also be written as a product of prime ideals; all the prime ideals of J dash times J, which is a prime ideal. It is a clever proof.

And, this is a contradiction. So, that is the proof of the lemma, which shows that, every ideal can be written as a product of prime ideals. And now, we need to show that, this expression is unique. And, that is also, now, will follow pretty simply; which is, let us say, I 1, I 2, dot, dot, dot, I k be equal to J 1, J 2, J l for. So, let us consider two products of prime ideals which are equal. This implies that, I 1 contain this product. So, I 1 is a prime ideal, and it contains product of prime ideals. What would this imply? I claim, this implies that, I 1 equals one of these J i s. Suppose, J t is not a subset of I 1, for 1, less than equal t, less than equal to l. This implies that, there exists a t in J t minus I 1 I should use the correct symbol here.

So, if J t is not in I 1, then, there is an element of J t which is not in I 1. But, this product, a 1, a 2 to a t is in I 1. Now, I 1 is a prime ideal. What is the property of prime ideal? By definition, an ideal is a prime, if whenever, a b is in the ideal, one of a or b is in the ideal. So, if this product a 1 to a t is in the ideal, one of a, not a t, it is a l, one of a t s must be in I l. And, that shows that, whichever, I mean, this assumption that none of the J t s are contained in I 1 was wrong. So, what we have managed to show after this is that, if a prime ideal I 1 contains a product of prime ideals, then, this prime ideal is actually contains one of those prime ideals itself; not just a product, but one of the prime ideals.

(Refer Slide Time: 24:20)



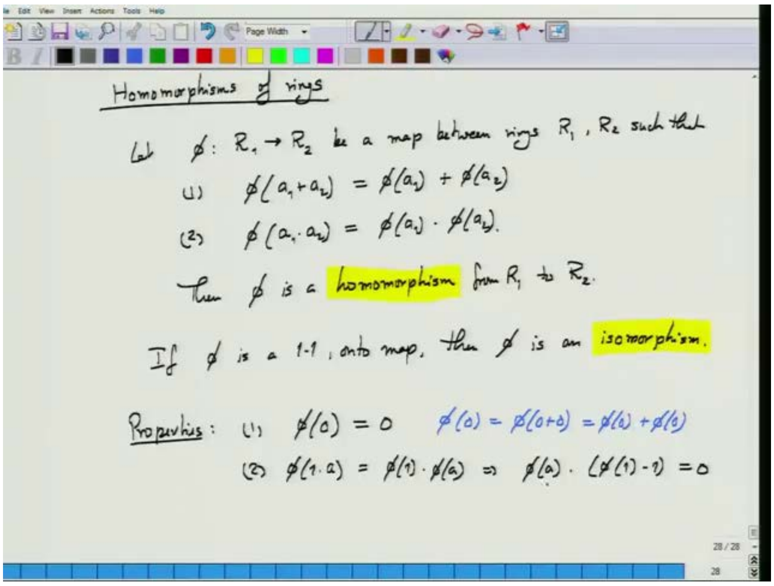
Now, J t is also a prime ideal; I 1 is a prime ideal, and J t is contained in I 1. Now, we use another property of Dedekind domains, which is that, those conditions that I listed for Dedekind domains imply that, every prime ideal is maximal. In fact, the three definition of prime ideals that I gave, I think I mentioned this last time; the three definitions of the prime ideal I gave earlier, all of the three coincide for Dedekind domains. So, every prime ideal in particular is maximal. J t is a prime ideal, and which is contained in ideal I 1, which is also a prime ideal. So, J t has to be maximal; I 1 also have to be maximal; which means J t is equal to I 1. And now, go back to the product. So, we have… Now, from this reasoning, what we learn is that, I 1 occur on the right hand side also. And now, I can renumber, or rearrange the right hand side, so that, J t is J 1. Now, use the cancellation property. This implies that I 2 to I k is equal to J 2 to J l, and repeat. So, you just keep canceling the identical ideals from both sides, and eventually, we get that, firstly, l equals k, and J t equals I t because. So, this gives you a flavor of the arguments that one can use, working with this abstract ideals. The key thing, I mean, I showed you the entire proof except this key lemma, because, where was that, for every ideal I, there is an ideal J, such that I J is a principal ideal. This really provides the heart of the proof, and proof of this is a little tricky, but, completely elementary; that is, you can follow it from the conceptual output. So, try to think about it.

Any questions on this? This is probably the longest proof I have done in this course, and quite abstract also. This seems like, this manipulation of symbols without much intuition; if you think about it, you will find, there is a clear intuition there. Basically, when one is trying to use the, you know, you just, cancellation is a very powerful tool of ideals, which you can use to, use to prove the uniqueness. And, the containment being equivalent to factorization, we use to show that, there exists a prime factorization of every ideal. Any questions? So, this is a story of the development by Kumar, and then, Dedekind. So, after... So, you know, significant amount of effort, which I just outlined earlier, they were able to restore this unique factorization property, for, of course, a limited class of rings. And, if you recall, this entire thing originated from that Fermat’s last theorem that, and the proof of Fermat’s last theorem used unique factorization implicitly, which broke down in a, that particular ring. And, but now that we have restored unique factorization, we can try going back to the proof, and see how it works out. Unfortunately, that proof now breaks down. Because, that proof used, I mean, it does not work when you are using ideals; it only works when you are using numbers, (Refer Time: 29:59).

So, of course, when the attempts continued, to prove Fermat’s last theorem for another

100 plus years. But, what we got in place of proof was this notion of ideals. Now, they have certain utility in terms of what I just showed, but it has turned out that, they have far more reaching utility, than just this. So, let us discuss that aspect of ideals. And for that, I will again go back to the group theory we developed. We had this notion of subgroups, in groups, and then, we defined the notion of quotienting a group with a subgroup, which corresponded with a homomorphism between groups. And, you have, there is a nice correspondence between quotienting a group with a subgroup and the homomorphism from that group to another group. And, we established something very similar for rings, and we will see that, the ideals play the role of subgroups.

(Refer Slide Time: 31:50)



So, let us first work, or define, the notation of a homomorphism for rings. So the notion of homomorphism generalizes very naturally into rings. In groups, we have one operation, and homomorphism preserved that operation. And in rings, we have two operations. So, we want homomorphism to preserve both the operations. So, if we say phi of a 1 plus a 2 is phi of a 1 plus phi of a 2 and phi of a 1 times a 2 equals to phi of a 1 times phi of a 2. All such mappings are homomorphisms. And the, further, if phi is a 1 1 onto map, then, phi is an isomorphism; that is, again, exactly the same as for groups. And, the notion of isomorphism allows us to deduce which rings are identical; if two rings are isomorphic, then, essentially, they are the same ring, ok.

Now, some properties of homomorphisms, for rings. Firstly, you should expect that, since it has preserved two operations, then, it should satisfy more properties, than the properties of homomorphisms for groups. And, that is certainly true. For example, what is homomorphism of zero? If phi is a homomorphism, what is phi of zero? This is always zero. Why? Yes, it follows, because, phi of zero is phi of zero plus zero, which is phi of zero, plus phi of zero. And then, you can cancel one of them, and then, deduce phi of zero itself. Phi of 1 is 1; second property, phi 1 of a 1 dot a 2 equals?

Student: (Refer Time: 35:59).

Let us see that. What you are saying is that, phi of 1 dot a is phi of 1 dot phi of a. And, this implies, phi of a times phi of 1 minus 1 is zero. Is this is what you are saying?

Student: So, phi of 1 dot a is equal to phi of a.

Phi of 1 dot a is equal to phi of a, yes.

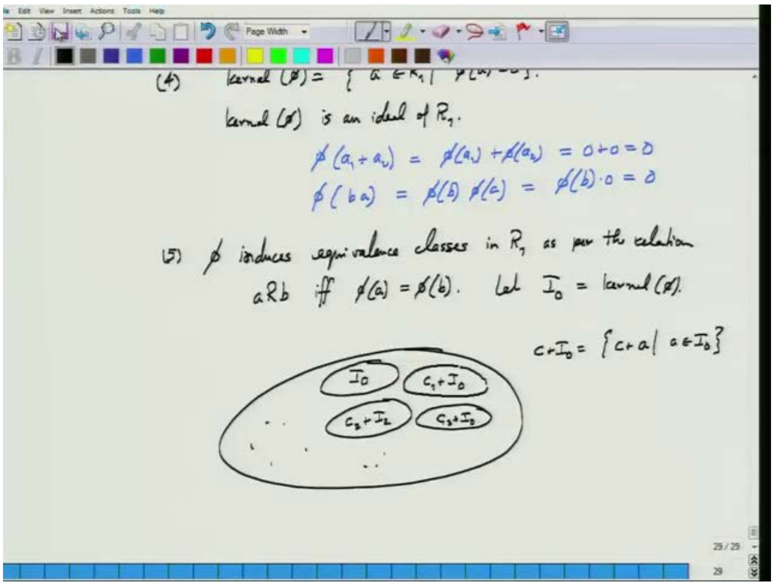
Student: So, we have phi members (Refer Time: 36:53).

Yes. So, that is what, I am taking the right hand side to the left, and writing that in this fashion. Now, does it imply that phi of 1 is 1?

Student: can zero one (Refer Time: 37:11).

For integral 1, yes: very right. If ring is a integral domain, then, one of them must be zero. So, either phi of a is zero, for all a s. So, that is the homomorphism; that is a trivial homomorphism; every element is mapped to zero; or, phi of 1 is zero. Even if it is not an integral domain, if for any element a, it is mapped by phi, to a unit of the ring R 2, then also, we can say that, phi of 1 is 1. Recall the definition of a unit. Unit was an element, which is, which has an inverse within the ring. So, we will so, for most of the rings, phi of 1 is 1; rings, and map; it is a, it is fine. So, we will stick to this assumption that, for homomorphism, phi of 1 is 1, because, that just simplifies certain things.

(Refer Slide Time: 38:35)



How about phi of a unit? What happens to this, when a is a unit of R 2, is phi of a is also a unit of R 2?

Student: (Refer Time: 39:00).

Phi, we assume phi of minus 1, yes; yes, why?

Student: (Refer Time: 39:10) inverse of a b is 1.

a b is 1, yes.

Student:. So, phi of a b is

So, phi of 1 is, phi of a b; so, 1 is so, yes, which is phi of a times phi of b, and that shows that, phi of a is also a unit. So, this is a nice property, which follows just by, you know, the fact that, phi of a is 1 is 1. Now, consider kernel. Again, exactly as defined as for groups; consider all elements of the ring R 1, which are sent to zero. (Refer Time: 40:14) This was same as, same definition as. Actually, here, we can define it in probably two different ways. So, if there are two units, or two identity elements, send phi of everything to zero, or send all those a s which are sent to 1. But, defining it for zero makes a lot more sense, as you will see. What can we say about kernel of phi. There, kernel of phi for groups was a subgroup. Here, it is an ideal. Why? See, if phi of a 1 plus a 2 is phi of a 1 plus phi of a 2, if phi of a 1 and phi of a 2 both are zero, then, that is all; phi of a 1 plus a 2 is also zero; phi of b times a, is phi of b, times phi of a; then, if phi of a is zero, then, this is phi of b times zero. So, that implies that the kernel is an ideal f the ring R 1. And, what does the kernel do, or rather, what does the map phi do? It takes the ideal I, or ideal kernel of I within R 1, and sends precisely that ideal to zero; other elements, it does not set to zero. So, this is again, defining that notation of quotienting, in a very natural way. And again, we can look at the equivalence classes that are created by phi within R 1. And, what are those equivalence classes like? Use the relation R which is… say that, a and b are related, if phi of a equals phi of b. And, if you look at the set R, or, you will have the equivalence classes; one would be the kernel.

Let us give a name to the kernel. Let I naught be kernel phi; then, there will be an I naught, one equivalence class; other equivalence classes would be of the kind… Every equivalence class can be written in this form that, sum c plus I naught, which means, this has elements of the form c plus a, whenever a is in I naught. And, you can see that easily; phi of c plus a, is phi c plus phi a; phi a is zero. So, it is same as phi c. And, whenever phi c is equal to phi d, then, phi c minus d is zero. And, therefore, this R is precisely the equivalence class (Refer Time: 44:43), ok.

Now, once you get these equivalence classes, let us again continue with our analogy with groups, and try to define a quotient ring. If you recall, the quotient groups, we defined by taking these equivalence classes, and defining a group operation on these equivalence classes. And, we showed that, that is a quotient group. Can we do the same here? Let me stop here, and leave this for the next class. You think it over. It is very natural, we can define the quotient class very easily; but I want you to give it some thought, and we will continue tomorrow.