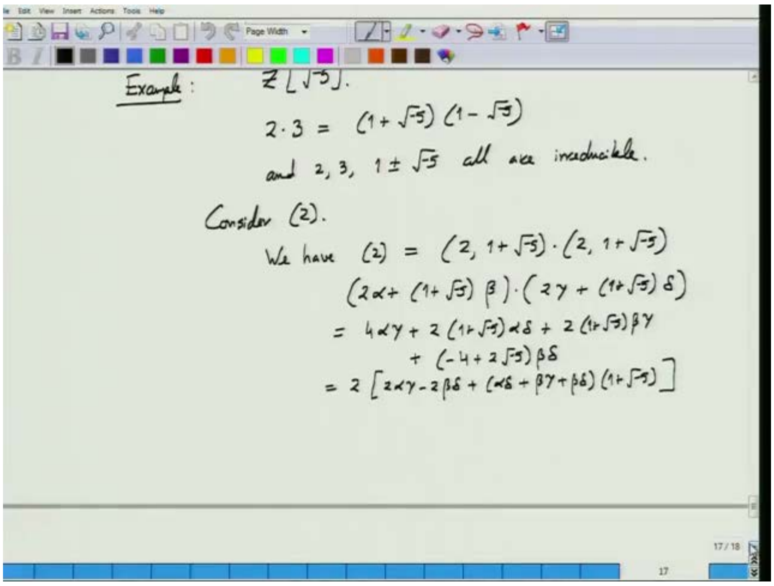
Modern Algebra

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

Lecture - 11
Rings: Special Ideals

(Refer Slide Time: 00:19)

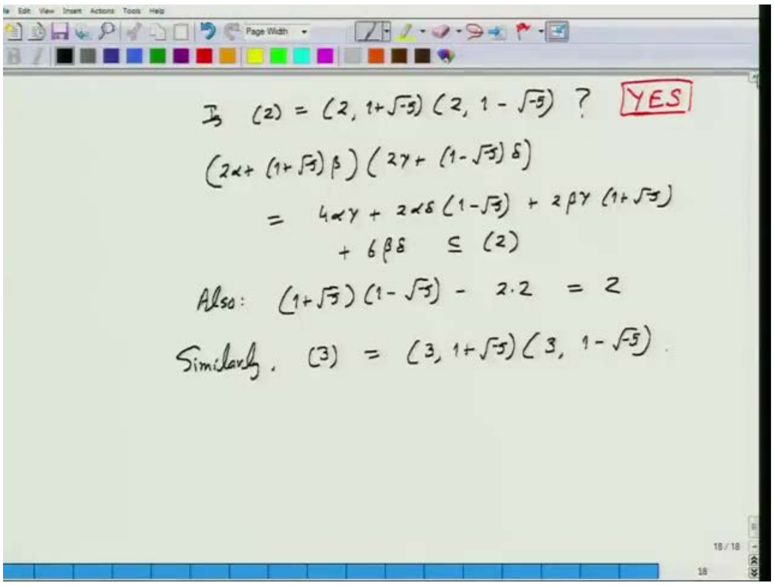


So, did anyone work this out, this place we got stuck yesterday?

Student: We have worked out it (Refer Time: 00:22).

What? Is that possible to write principle ideal 2 as a factor of 2, is what you can prove that?

(Refer Slide Time: 00:39)



Then that is contrary to what I can show, so let us see who is right.

Student: Equation is somewhat wrong, last equation.

That is wrong, that is clearly wrong that you showed last time and that cannot be, how about this?

Student: (Refer Time: 00:59).

Is this true?

Student: (Refer Time: 01:08).

Let us see that I think this should be true. So, we have to show inclusions two ways. Firstly, any element of this, which is in fact, we can go back to yesterday's calculation and make use of it. We have an arbitrary element which is here of course this is not quite what we would have. So, let us see just do it fresh today. So, an element here which is 2 alpha plus 1 plus square root of minus 5 beta times 2 gamma plus 1 minus square root of minus 5 delta that is a general element of this product.

Of course, there are some solves of what each product each term of the sum has this wrong. And if you multiply this out is equals 4 alpha gamma plus 2 alpha delta 1 minus square root of minus 5 plus 2 beta gamma 1 plus square root of minus 5 plus this would be 6 beta delta. And this is in principle ideal 2 because each term if you see is a multiple of 2 and also belongs to (Refer Time: 03:01) that is it now specifically each of it is 2 times some element of the ring so that is it.

Student: (Refer Time: 03:10).

Well, ring is z square root of minus 5 so that is one way it is clear. How about the other way like I said last time it is enough to show that 2 belong to this product. Do 2 belong to this product?

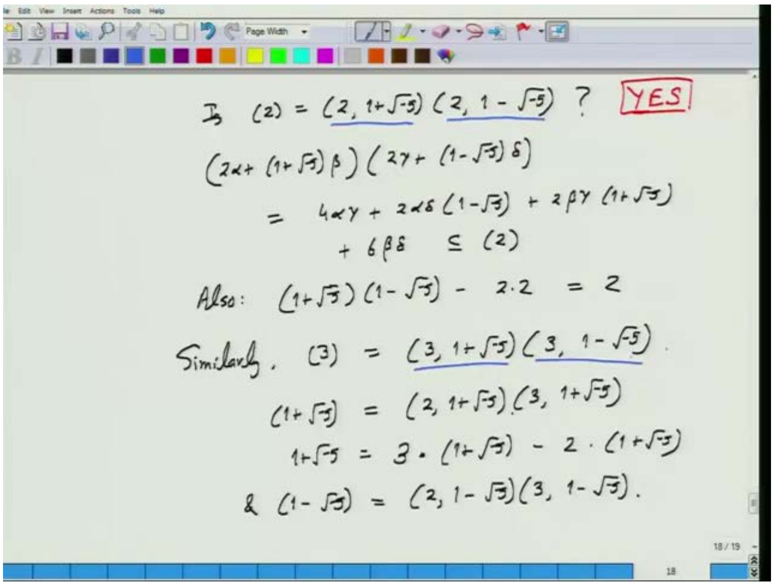
Student: (Refer Time: 03:36).

Just multiply 1 plus square root of minus 5 is 2. So, this sum of products is an element of this product ideal, because this is an element of the first ideal, this is an element of the second ideal, this is an element of the first ideal, this is an element of second ideal. And in the product ideal the elements are finite sums of pair wise product and this is 6 and this is 4 then difference is 2. So, therefore, the answer to this question is yes. So, the proof that you worked out there it is not factorisable there is a problem in that proof I guess.

Similarly, the principle ideal 3 factors as in a very similar way in this question, and you can see almost identically the connection or why this is happening. If you take a generic element of this product, which will be of the same kind expect that instead of 2 will have 3. And you multiply this out instead of four 4, we have 9, 3, 3and this 6 will remain.

So, in all of this multiple of 3, so this any element of this belongs to the principle ideal generated by 3; and conversely, I can generate 3 in this basically the same thing 3 into 3 minus this, this product is 3, so that is it. So, that also shows that the principle ideal of 3 also factors so that is the factorization of 2 and 3. And if recall, we had this equation, so let us see the right hand side of this equation, how about 1 plus square root of minus 5 and 1 minus square root of minus 5.

(Refer Slide Time: 06:28)



1 plus square root of minus 5, I will claim factors as yes, it is again look at the general element of this. What is that, go back to the same picture, in the general event there will be 2 here and 3 here 1 plus square root of minus 5 1 plus square root of minus 5. When you multiply them out 2 times 3 would be 6, all other terms will be multiples of 1 plus square root of minus 5, and 6 is a is 1 plus square root of minus 5 times 1 minus square root of minus 5, this 6 is also multiple of 1 plus square root of minus. So, this therefore, contained in this principle ideal that adversely is 1 plus square root of minus 5 contained in this.

Student: (Refer Time: 07:36).

Yes, why?

Student: 3 into 5 (Refer Time: 07:40).

3 into.

Student: 1 plus 2 square root of minus 2 into (Refer Time: 07:51).

Wait a minute. Now we have to show an element of a here times an element of a here, and may be some finite sums of such elements is equal to 1 plus square root of minus 5. So, what is that equation you are saying?

Student: 2 into 1 plus square root of minus 5 (Refer Time: 08:10).

1 plus square root of minus 5 equals 3 into.

Student: (Refer Time: 08:18).

Minus 2 into 1 plus, yes, so that is an element. This is an element here and this is an element here, so this times this minus this times this, and 1 minus square root of minus 5 in a very similar way will factor as and now you we can explain this seemingly different factorizations. Because these when you look at these in terms of principle ideals they will factor as non-principle ideals and I have not discussed it. In fact, we are still yet to decide on the definition of what if prime ideal is, but whatever that definition these are prime ideals as it turns out I will not show that I will leave it for you to work out. And then 2 into 3 is this two ideals time these two ideals and 1 plus square root of minus 5 into 1 minus square root of minus 5 is these are ideals times these ideal both the product are same.

Student: (Refer Time: 09:51).

2 comma 1 plus square root of minus 5, so this is a prime ideal, this is a prime ideal, this is a prime ideal, this all these four are prime ideals. And now you see that you can write the reason why we get distinct this equality that I 2 times 3 is 1 plus square root of 5 minus time 1 minus square root of minus 5 is that just a rearrangement of this prime ideal factorization. So that is an example of how this unique factorization property gets

restored once we look at the ideals.

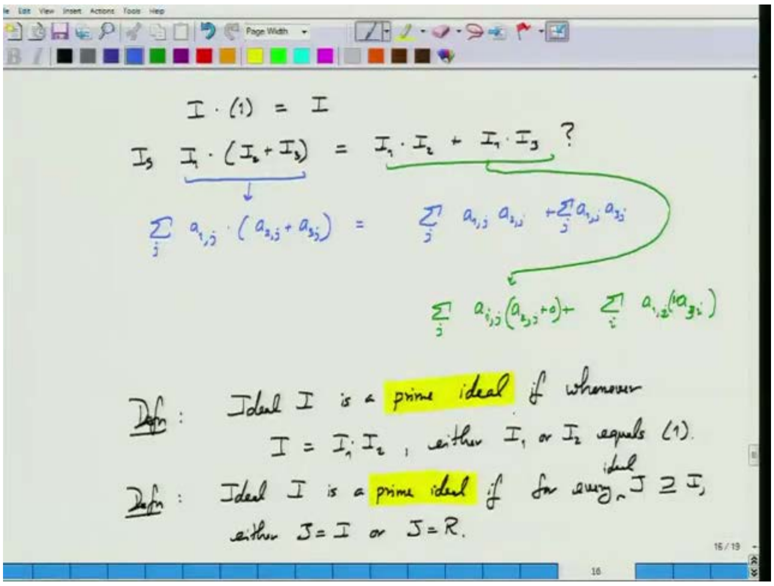
Student: (Refer Time: 10:44).

So, if you see this equation in the ring does not admit unique factorization 2, 3, 1 plus square root of minus 5, 1 minus square root of minus 5, they are all irreducible elements in this ring so you cannot be factored further, but there are 2 different ways of factorizing the number 6. So, unique factorization property in this sense does not hold in the ring. Now when instead of looking at these as numbers if you look at these as principle ideals then we have unique factorization property again. As principle ideals this is the principle ideal 6 is same as principle ideal 2 times principle ideal 3. Similarly, it is same as principle ideal 1 plus square root of minus 5 times 1 minus square root of minus 5. Now moving to the ideal world allows us to further factor these principle ideals into prime ideals which is what happening here, here and here and more over here as this, this, this, this.

And now in terms of these principle ideals being factored as prime ideals, the unique factorization property is restored, so that was an original motivation why the ideals were defined. I can say Kumar who was the mathematician who identified the problem and then tried to resolve it by defining ideal numbers, which were some hypothetical numbers, which helped resolve this reinstate the unique factorization property.

And then later on Dedekind said these ideal numbers instead of forcing them in if we just look at ideals just by changing the view like I said earlier that do not look at a number as a number itself or if look at a number or view the number as all multiples of that that are. In terms of now notation of thermology we have defined look at the principle ideals corresponding to that number. And then this unique factorization properties brought in throughout these ideal numbers of (Refer Time: 13:32) are at least in this case are these prime ideals. So, their presence brings about the unique factorization. So, this resolves this example, but we are still have not looked at the general case.

(Refer Slide Time: 13:51)



But before we look at the general case, we still have to resolve that certain amount of confusion about the definition of what a prime ideal is. I gave two definitions last time. Did you think about this? The first one is quite natural. The second one seems strange, but let me suggest to you why this is also a possible definition of a prime ideal. We defined ideals as at least principle ideals as multiples of numbers.

So, in case of ring of integers, if you look at a principle ideal, all ideals there are principles, look at a prime number, look at the principle ideal of that prime number which are all multiples of that prime number that ideal is a prime ideal in this second definition sense. Because there is if there is an ideal which contains this so let us look at number 7 look at all multiples of number 7 that is a principle ideal if there is any ideal that contains all multiples of 7 what could that be?

Student: (Refer Time: 15:21).

It has to be ideal principle ideal 7 or principle ideal 1, cannot be anything else because 7 is a prime so that is this definition this is second one, that is if you have a there is no ideal between a prime ideal and the whole ring. So, it does make sense the second one also. So, any comments about or thoughts about these two possible definitions are they equivalent?

Student: (Refer Time: 15:56).

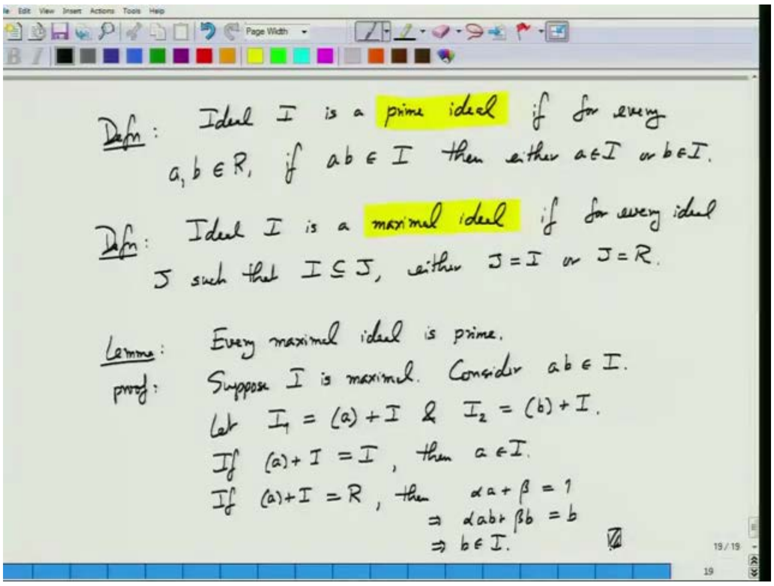
Sorry.

Student: Could not prove that equivalent.

Could not prove that equivalent actually, they are not equivalent in general; in fact, this factorization of ideals itself gets messy if the rings are not of certain kinds you know somewhat nice kind. And similarly this I may or rather I should say that if the rings are not nicely behaved or not of a particular kind, then these two definition become different, even factorization of ideal itself is kind of not very nice.

So, we would see from prime ideal they are such basic concepts when we would like a definition that is universal, it holds for all rings, and then it can be done in a nice enough way. Since factorization is of ideals is not very nice for certain rings, we will not use this factorization definition of prime ideals, so that brings us to the second definition. The second definition also becomes restricted for certain rings, certain types of rings; we will see examples of this later not now. For now, you just have to believe me. So, we cannot use the first definition we would not want to use second definition, so which definition do we use, we use a third definition.

(Refer Slide Time: 17:51)



This is a new way of stating the definition ideal I is a prime ideal if for every a b in the ring, if the product a b is in the ideal then either a is the ideal or b is in the ideal. Now again if you go back to the definition of or the setting of ring of integers, this is also very sensible definition.

Look at a principle ideal generated by a prime number, and we are saying that if two numbers a, b where the product of two number a and b is in that principle ideal then either a or b is in that principle ideal which is equivalent to the fact that if a product is divisible by prime number then one of the two elements in the product must be divisible by a prime number so that is one of the fundamental properties of prime number. And this definition captures that property, so hence this can be also used as a reasonably good definition of the prime ideal, and this is the one that we used across all the rings.

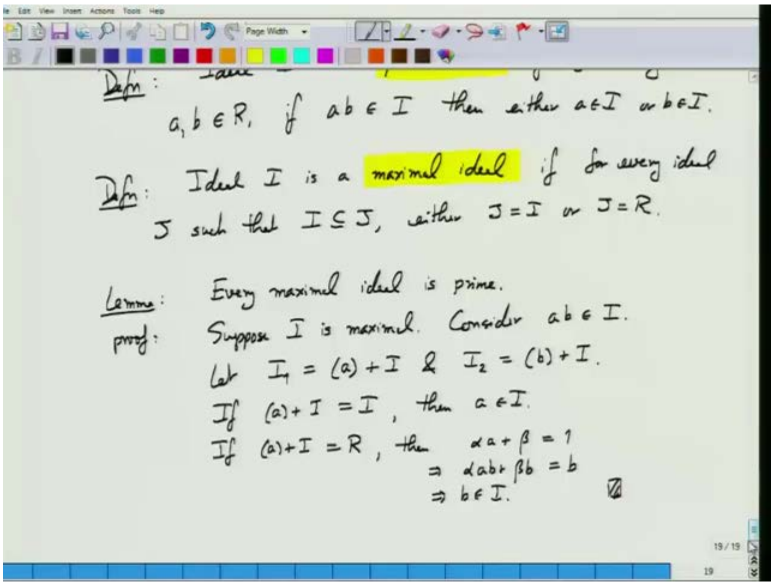
Now, it turns out that for certain types of rings, all the three definitions are equivalent. I will not show it, but I will just kind of highlight a bit, but the second definition that I had earlier given that is still interesting enough or it can be generally defined for all rings. So, I will give it a different name not call those prime ideals, but call them with a different name. Same definition expect the name I give to such ideals is not the different, these are called maximum ideals.

And there is let me just shows one connection that can be proven very easily for all rings, which is that every maximal ideal is prime ideal. And this is good to know because this tells us that the our definition of prime ideals is a more general one then the initial one that I given that you know (Refer Time: 22:04) more ideals, so why they are very maximal ideal prime

Well, suppose I is maximal, and we want to show that I is prime. So, consider a, b this product in I. Now let us create two ideals I 1 being principle ideal of a plus I, I 2 being principle ideal of b plus I, both are ideals. Both contain the ideal I, and since I is maximal, what is it mean? It means that they are either equal to I or they are equal to R. If any of them is suppose if this equal to I, what does it mean that a is an I, and if there is a case and we have already done.

On the other hand, if a plus I equals R, then we have alpha a plus beta is 1, R contains 1 and this some of ideal is R, so there would be alpha in the ring R, beta in the ideal I such that alpha I plus beta is one. Multiply this equation with b; now this implies that b is an ideal, because beta is in I, so beta is in I; a b is in I by assumption, so alpha a b is in I therefore, b is in I, as a pretty straight-forward proof showing that every maximal ideal must be prime.

(Refer Slide Time: 25:01)



Now let us come to this situation, where the definition that I gave see eventually I want right now the target is to be able express uniquely every ideal as a product of prime ideals. And I have been saying that this only holds for certain types of rings, and the types of rings were to this holds is the are the once where all, but at least these definitions go insight for the prime ideals. So, let us define those settings. And in order to define those settings, if you recall going back to the our discussion on groups, we were able to express certain types of groups as a sum of copies of set Z n plus some finite number.

What was the limitation or what was the condition impose on those groups? Finitely generated, see if you go back to your that result about groups the structure of groups, there are theorems stating that every finitely generated group can be expressed as sum of copies of Z plus a finite part of it a finite group part of it which further can be expressed as sum of Z p to the alphas, so that structure theorem only was true for finitely generated groups not for other kinds of groups. And I have been saying it is this structure theorem for rings that I have been aiming for only hold for certain types of rings and returns out that finitely generated rings is an not rings only finite generation is an important component of that restrictions.

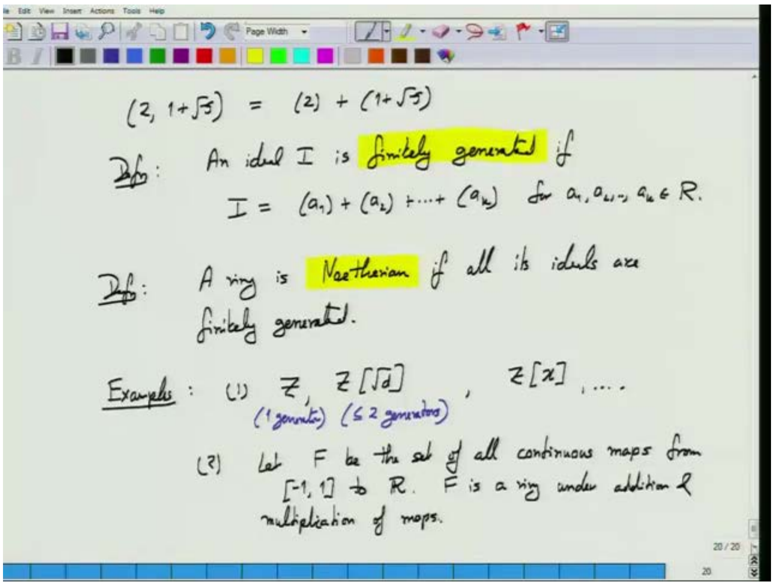
So, for rings, how do we say that now how do we connect this notion of finite generation with rings, with groups we had seen? What is the simplest finitely generated group the one with just one generator, and then you all powers of that generator generate that group, so in case of the group in finites, so finite it is a cyclic otherwise it is a just a copy of Z. So, what could be analogues notion of rings, a finitely generated ring let say a ring with one generator?

Student: Principle (Refer Time: 28:23).

A principle ideal, a principle ideal like yes that is seems like a natural thing, principle ideal there is just one generator right, all multiples of one element are make the principle ideal. But then every ring has one generator only, because every ring is equal to whatever the ring that we are talking about is equal to principle ideal of one. So, we cannot limit our attention to saying that a ring is finitely generated or not.

Well, in all rings in this sense are finitely generated it was very simplest as possible once. So, what we will have to do and this is slight relief of imagination that instead of looking at whether rings are finitely generated, we look at whether ideals are all finitely generated. A principle ideal is surely finitely generated it is just a single generated by a single element not all ideals are finitely are principles we have seen that.

(Refer Slide Time: 29:51)



In fact, if you look at this ideal, this is not principle by it is sum of two principle ideals. In fact, this was just a short hand to write this. So, this ideal is also finitely generated. So, in general, we can say an ideal we say is finitely generated, if it can be written as a sum of finitely only principle ideals and that is a very natural definition. And then we say a ring is a ring is called a noetherian ring, if all its ideals are finitely generated.

Now the name noetherian is as often the case is named after the mathematician, who first studied these kinds of rings. The unique part of this name is that it is a woman Emmy Noether, she was one of the earliest woman mathematicians known at least probably amongst the prominent mathematician, and she was probably the earliest woman mathematician. So examples of Noetherian rings, you have seen examples of many ring yes, yes, go through them.

Student: Integers.

Integers surely noetherian right, all ideals are principle, so they are the extreme example of noetherian rings. How about these extensions?

Student: (Refer Time: 33:05).

Z square root of d 1 comma root d will generate everything, but what we need to show is that every ideal is finitely generated. Every element of this is of the form an integer plus an integer times square root of d. So, if an ideal has two generators of this kind then by taking appropriate differences, we will get in that ideal an integer and one element being pure integer and other element being an integers times square root of d.

And now individually on these you can apply this property of z. So, there are two integers - pure integers in that ideal, and then their gcd will also be in the ideal. So, there will be a unique minimum integer in that ideal; and every integer in that ideal will be written as a multiple of this. Similarly, if d s times square root of d, and then with you know just put all these arguments together, you will find that any ideal in this ring can have at most two generators.

How about this Z x, this will behave exactly the same way as this. See this square root of d is so 1 and x are the two natural components right, yes even not even 1 and x, it is let say if you have an ideal so elements of these are polynomials, if you have an ideal with two polynomials inside that ideal the gcd of those polynomial will also be in that ideal.

Of course, taking gcd, we have to be a little careful, because we have coefficient are integers, so we have to show that there is an integral, I mean all of like coefficients are integers, but you can work this out. I will leave this small exercise to you, and you can work this out and find that this will also have maximum two generators I believe. I am not sure, it may also have there is every ideal here may also be principle. This is you need to just check this out so either one or two, no more than two generators are needed for this, so that is you know very interesting.

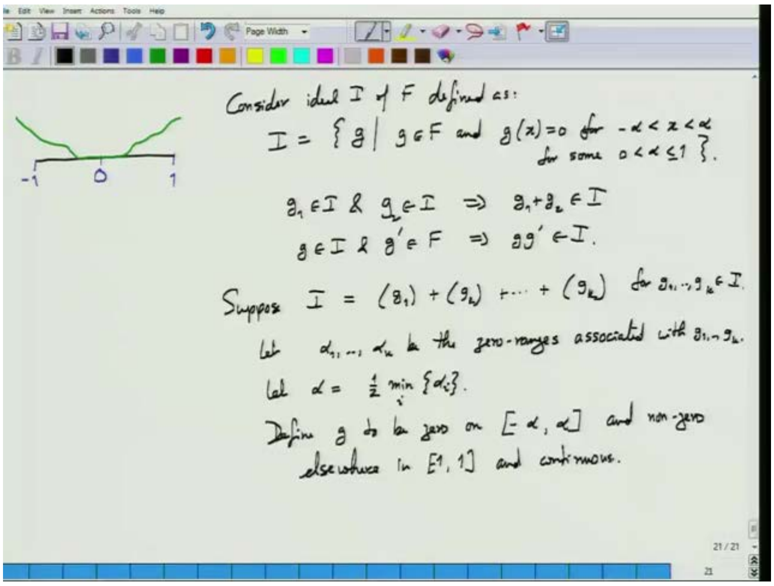
How about any other example of a ring that you know of we are reading out non-commutative rings, we are just focusing on commutative rings; in fact, lot of examples exists which have this property that this rings are noetherian. So, instead of giving more example of this let me give you an example of a non-noetherian ring. And this example is also of quite bit of interest, because we will develop on this subsequently.

So, let us define an interval let say minus 1 to 1. We are considering continuous mappings from the interval minus 1 to 1 to real numbers collect all continuous mappings in the set f. I will define arithmetic on this set and claim that under that arithmetic, it forms a ring. What is the arithmetic, very simple, addition take two mappings and define the sum of those two mappings as a new mapping.

Will that be continuous, yes, that will be continuous, what is this is also commutative and associative this of summation. How about the identity of this operation, the zero map which maps everything to zero plus the identity of this operation. Then inverse, if you have mapped g then minus g is the inverse map because g plus minus g this map will map the entire interval to zero. So, this forms a group under addition commutative (Refer Time: 39:33) addition

Now, you defined multiplication of mapping also. So, g 1 times g 2 is also a continuous map from the same interval. The identity of multiplication exists which is the map, which sends everything to all ones, this is commutative, and it is associative. So, it is and then distributive property of multiplication also for addition. All this follows on trivially essential so that means, f is a ring under addition and multiplication, multiplication of maps. Now I claim that this ring is not noetherian and to prove that what would I need to do I would need to show an ideal in this ring which is not finitely generated. Let us do that.

(Refer Slide Time: 40:53)



Consider ideal I of f defined as I contains all mappings g, g is in F, so I contains all the maps, which are continuous on the interval minus 1 to 1, and g of x is 0 on certain interval around the number 0 around the origin. So, essentially you have this is the origin, this is minus 1, this is plus 1. And your maps any map which is of this kind whether it is 0, and this part and then it is continuous whichever way everywhere else that is fine.

There must be a non-trivial interval around origin on which this map must take the value 0. There will be lot of such maps continuous this is a continuous map is an ideal. If g 1 in I, and g 2 in I, this implies that g 1 plus g 2 is an I because if there is a interval around origin on which g 1 vanishes and interval around I on which around origin of a g 2 vanishes then intersection of those intervals on that g 1 plus g 2 will vanish so that is fine. Now g in I, and g prime in f implies g g prime in I, because if there is a interval on which g is 0, then g times g prime is also 0 on that interval it may be zero on a larger interval, but certainly 0 on that interval. So, I is an ideal certainly.

Student: Should make the equivalent interval (Refer Time: 43:29).

It could make the full interval trivial that is also possible, yes.

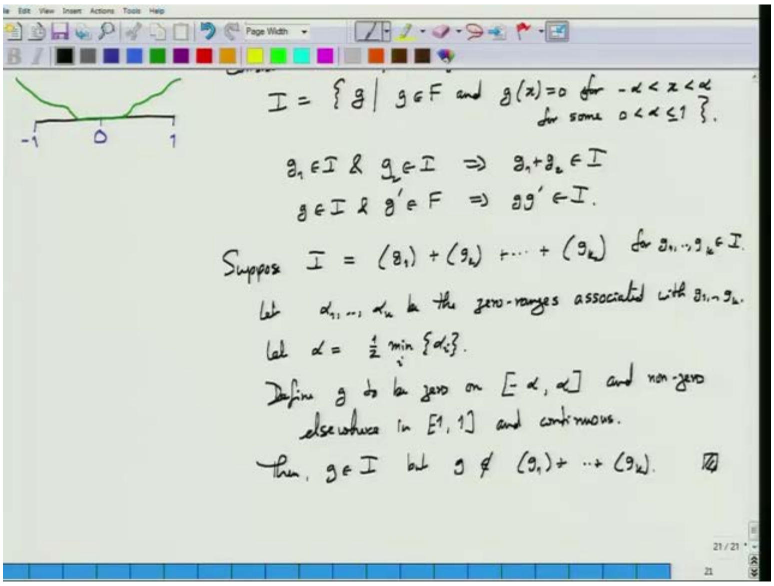
Student: (Refer Time: 43:32).

Let us make it one, good point, now I is an ideal of the ring F and this ideal is not finitely generated, why, well suppose I, I can write as g 1 g 2 plus g k or some g 1 to g k in f in fact g 1 to g k not only would be in f it would be each 1 of them would be in I also has to be by the very definition, then look at the there is an interval on which g 1 vanishes there is an interval on which g 1 g 2 vanishes there is an interval on each 1 of them vanish take the intersection of all those intervals and half it.

Student: (Refer Time: 44:42).

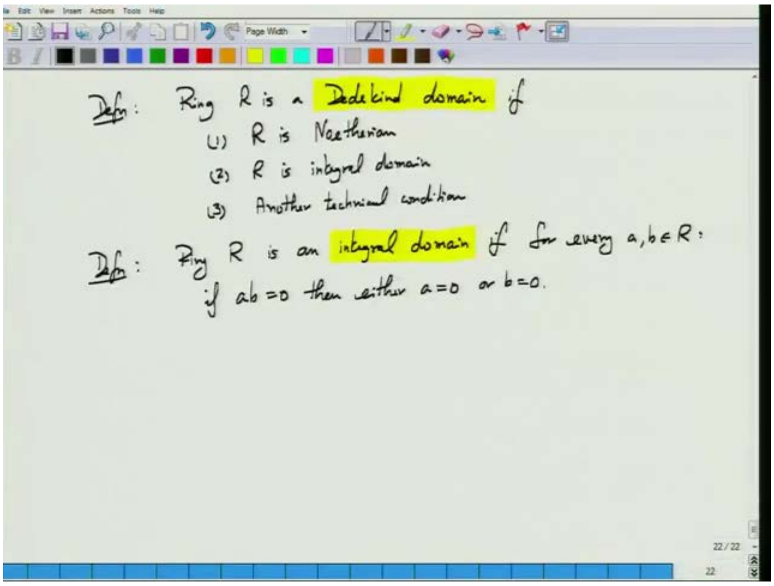
And cut it down by half or reduce it further basically. Now define a continuous map which is 0 only on that reduced interval and nonzero everywhere else. There will exist such a map in f and that map will be on I also, but this on this sum, the sum of these any mapping in this sum is going to be 0 on a larger interval around 0. Whereas, that in new map that I have defined will be 0 only on a smaller interval, so it is not possible.

(Refer Slide Time: 46:45)



So, these are the rings which will cause problems to us if you are looking for that structured theorem. So, we will not be able to prove any as nice as structured theorem about such rings, so for now we will let us just focus on noetherian rings, where is not unfortunately sufficient that will be we are able to prove that we rather noetherian rings are not sufficient for us to prove that structured theorem. We have to bring in some additional conditions.

(Refer Slide Time: 47:45)



So we say that ring R is a Dedekind domain if R is noetherian, two R is an integral domain I have not defined what integral domain is which I will do (Refer Time: 48:48), but unfortunately even these two are not sufficient, we have to push in one more condition which I do not even want to write down. So, you just keep in mind if some small technical condition which is almost always true, so it is not something very limiting or problematic.

It is just that you know if I want to write down that condition fully I will have to define two more things, which I do not want to do, but I do want to define what integral domains are. So, we call a ring R integral domain, if whenever a product a times b is 0 in the ring then either a is 0 or b is 0, this is a very obvious looking condition. Of course, this should be true certainly is true for integers or numbers in general, but this is not true for all rings. In fact, go back to the ring I just defined above this one this is not true for this. Why?

Student: In a noetherian (Refer Time: 50:54).

That the product it vanishes everywhere, and that is a 0. So, again in non integral domains are very funny kind of a strange kind of a rings which are very interesting also, but not useful for.

Student: Can be mean matrix also.

Can be matrix also, very right.

Student: (Refer Time: 51:32).

Yes.

Student: (Refer Time: 51:34).

Yeah, that is right absolutely. So, while such rings are non-integral domains are interesting rings and we will come across some later, but as far as numbers and their factorization are concerned, we do not want them around, because that is cant really handle factorization there. So, that is why we bring in this condition also and then there is additional technical condition all put together the rings that satisfy them are called Dedekind domains and then we have the theorem for Dedekind domains. Now we can prove the theorem about Dedekind domains, which I will do next time.