Introduction To Rings And Fields

Prof. Krishna Hanumanthu

Department of Mathematics

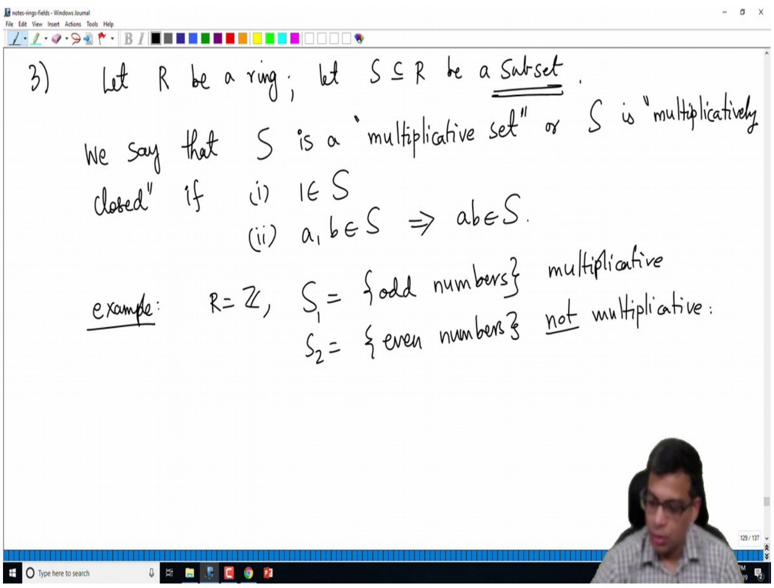
Chennai Mathematical Institute

Lecture - 32

Problems 9

In the last video I did a few problems on rings and let us continue. Now, I am going to do some more problems in this video.

(Refer Slide Time: 00:24)



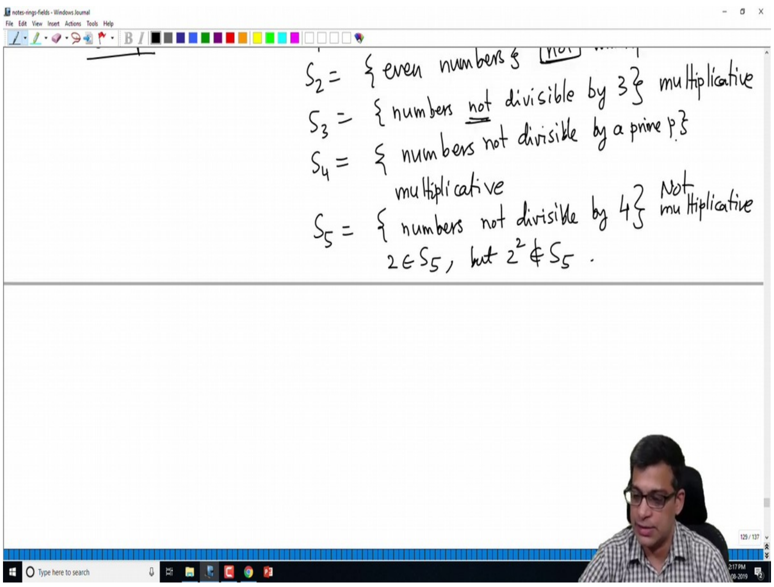
In the third problem now, last time we did two problems. Let us introduce a very important construction in ring theory, this is this will be useful if you continue studying ring theory. So, I will introduce it to you and do some simple properties. So, let R be a ring and let me remind you again that in this course, a ring for us means a commutative ring with unit.

Let S be a sub set of R, I am not asking for it to be a sub ring, only a sub set. So, we say that S is a multiplicative set or a more suggestive name is multiplicatively closed or S is multiplicatively closed. So, that is the another term for this, if the following happens, if two things happen; one is in S the identity element multiplicative identity element of R is in S, the other is if a and b are two elements in S, for any ring elements that are both in S their product is in S. So, it is multiplicatively closed, the as a name suggests if two things are in S it is product their product is also S, that is all no other condition.

So, immediately you know that for example, it cannot be an ideal if it is an ideal it has to be the unit ideal, because one is there, if this property if it is an ideal also, then it must be equal to R. So, most of the time these are not ideals or any kind of closure under addition will not be there. So, a quick example to you so, if R is Z, you can take S to be odd numbers right, S 1 is odd number.

So, 1 is an odd number product of 2, odd numbers is odd number. So, this is multiplicative, S 2 even numbers, this is not multiplicative, because even though the product condition holds, if two even numbers multiply to an even number, but 1 is not there. So, that is an important condition for us. So, it is not multiplicative.

(Refer Slide Time: 03:04)

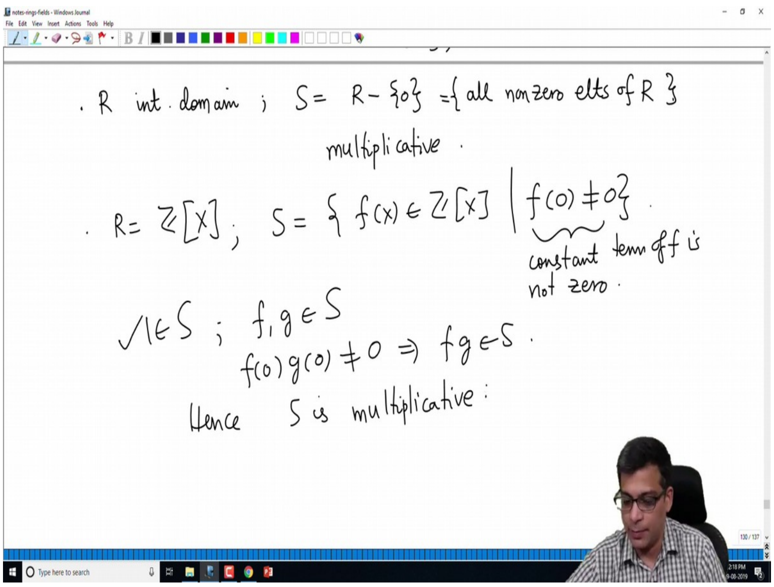


Let me just one more example; numbers not divisible by 3 or this is multiplicative. This requires a little bit of thinking, but you can show that this is a multiplicative set, because 1 is in this set, because 1 is not divisible by 3, it is in the set whereas, and if two numbers are not divisible by 3 for example, 5 and 7 are not both divisible by 3, 5 times 3 7 is not divisible by 3. Here, the important fact is 3 is a prime number.

If 3 does not divide a, 3 does not divide b, then 3 does not divide a b. Remember, that is the property of prime numbers, because if 3 divides a b, 3 divides either a or b, 3 divides b. So, this is multiplicative in general, we can define S 4 to be numbers not divisible by; not divisible by a prime p.

This is multiplicative right, because exactly the same idea as before 3 is a prime number, you can replace it by any prime number. What about numbers not divisible by 4? Say this is not multiplicative, because 1 is there, that is fine, but 2 is there in S 5, but 2 square is not in S 5, because 2 is not divisible by 4; however, 2 squared is 2 times 2 is divisible by 4. So, it is not in S 5. So, this is why you need a prime number in this case ok. So, 4 is not prime. So, this is not going to work.

(Refer Slide Time: 05:06)



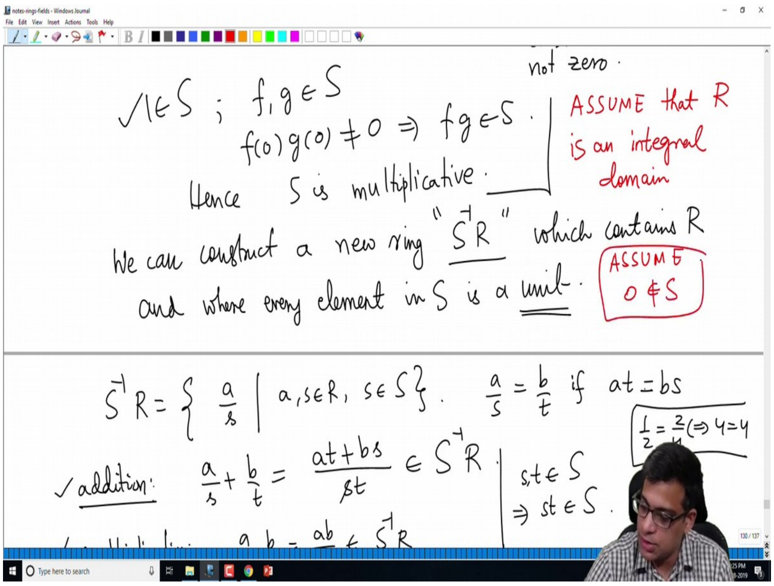
More generally if you have an integral domain, you can take S to be R minus 0; so, all non-zero elements of R right. This is multiplicative also, because you multiply two non-zero numbers the product is non-zero. So, if two elements are in R minus 0 the product is also in R minus 0, this is multiplicative. Remember, that this will not be a multiplicative, if R is not an integral domain, there will be two non-zero elements, whose product is 0.

So, that will not be multiplicative one, more example I will do before continuing. Let us take Z X, let us take f to be all polynomials in Z X such that f of 0 is not 0. This simply means the constant term is non-zero right, because f of 0 is the constant term of any polynomial suppose it is not 0 1 is certainly in S, because constant of 1 is 1 which is not 0.

If f and g are in S, then f of 0 times g of 0 is non-zero, because f of 0 is non-zero integer g of 0 is a non-zero integer; that means, the constant terms of f and g are non-zero integers, their product is non-zero. So, f g is in S ok.

So, this hence S is multiplicative. So, this is another example of a multiplicative set. So, these are some examples of multiplicative sets. Now, the point of the problem is not this, the problem is to show that there is a new ring.

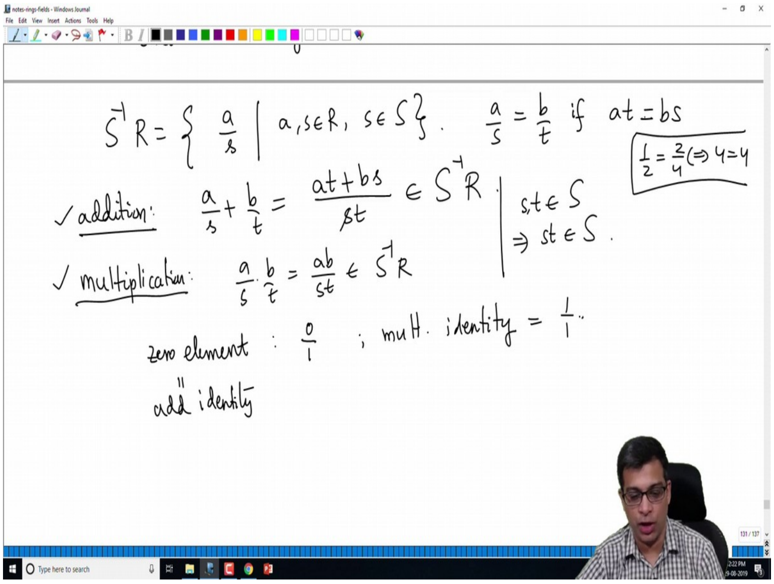
(Refer Slide Time: 06:53)



We can construct a new ring. So, actually now I will assume that. So, I should have said this before, assume for simplicity this can done in general, but as a first introduction to this we can assume that R is an integral domain, from now on in this problem, we will assume that R is a integral domain. We can construct a new ring, which we denote by S inverse R, where, which contains R and where every element in R, in S is a unit. So, I will explain what this means.

So, more generally there will be a function from R to S inverse R, which is injective, image of an element of S is a unit in S inverse R. So, this process is called localization and what we are doing is; we are forcing every element of S to be a unit. In general of course, when you take a multiplicative set the elements are not units in this examples you can see that odd numbers are not units 3 is not a unit in S 1 so; however, we can construct a new ring where it becomes unit.

(Refer Slide Time: 08:20)



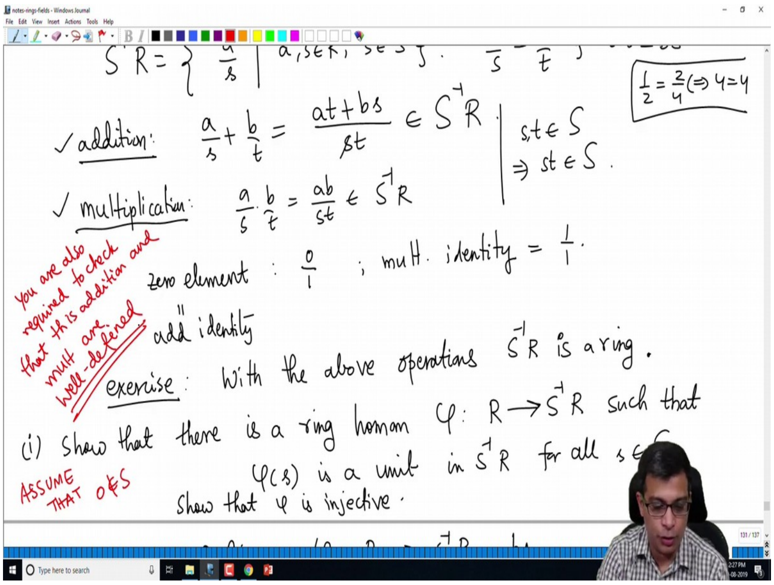
So, we define S inverse R to be. So, please keep in mind, when I am doing this the example of how we construct rational numbers from integers, we have integers and we take ratios in S inverse R, we take ratios where denominator is in s. So, simply it is defined like this a by s. They are just symbols at this point a in R a and s are both in R to begin with and s is also an S.

So, we define this and as equality will be a by s will be considered equal to t if a t is equal to b s, just like we have two rational numbers 1 by 2 is equal to 2 by 4, because 4 equal to 4 the same idea I am applying. So, two ratios are considered equal, if their cross products are equal. This is the set, addition on this again, we are exactly mimicking the construction of rational numbers.

So, addition is a by s plus b by t is at plus bs by st. Here is where the multiplicative property of S is important s and t are in S, because and hence their product is in s. So, this is in S inverse R in my notation. So, multiplication is also defined in the same way, a by s times b by t is a by b times s t which is in S inverse R. So, important two point is if s t R and s s comma t is in S, s t is in S. So, that is what we are using one can check that this has all the required properties.

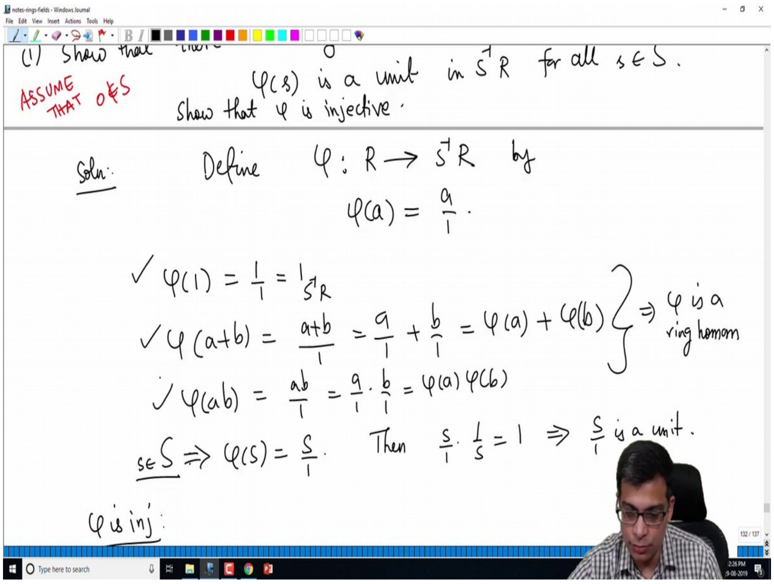
0 element is 0 by 1 or 0 by any other element, multiplicative identity 0 element remember is the additive identity, multiplicative identity is just 1 by 1 1 is an s remember. So, we can put 1 in the denominator.

(Refer Slide Time: 10:34)



So, with this and this I will let you solve as an exercise this part I will not do, with the above operations S inverse R is a ring show that now, the problem is show that there is a function, there is a ring homomorphism phi from R to S inverse R such that. So, this is I can think of the first problem there on this such that phi of s is a unit in S inverse R for all s in S ok. So, how do we show this solution? The map is very easy to define. So, define phi from R to S inverse R by sending phi of a to be phi of a to be a by 1. So, why is it a ring homomorphism?

(Refer Slide Time: 11:44)

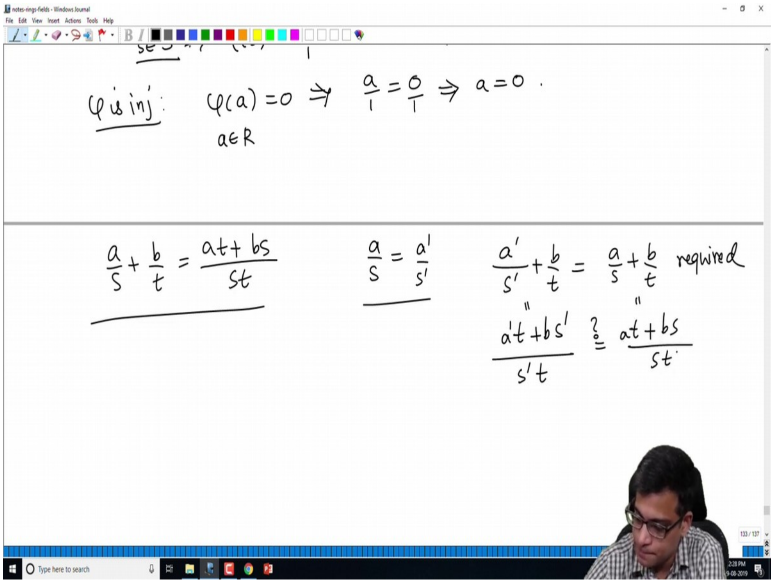


What is phi of 1? This is 1 by 1, which is the 1 in S inverse R. So, this is what is phi of a plus b? This is a plus b by 1, which is a by 1 plus b by 1 which is phi of a plus phi of b. So, this is what is phi of a b? This is a b by one this is a by 1 times b by 1. Remember, the definition of multiplication at addition in this ring, a by s plus b by t is a t plus b s by s t a by s times b t b by t is a b by s t. So, this is phi a times phi b ok. So, this is also so, this shows that phi is a ring homomorphism I am leaving a verification that phi is a S inverse R is a ring to you. So, this is an exercise for you.

Now, suppose small s is in capital S, then phi s is s by 1; I want to show it is a unit note that 1 by s is an element of phi inverse R S inverse R, because s is an element of capital S. So, this implies S by 1 is a unit. So, this is the other statement here that we are asked to show. So, phi of S is a unit for every s in S. So, also show that I should also left it should have written it here show that phi is injective phi is injective.

Actually, I should have said this so, maybe I should write it here most of the time we are going to assume that S does not contain 0, some where I wrote this also assume that otherwise, I get into problems assume that 0 is not in S. So, assume that every where 0 is not an S. So, show now that phi is injective.

(Refer Slide Time: 14:08)

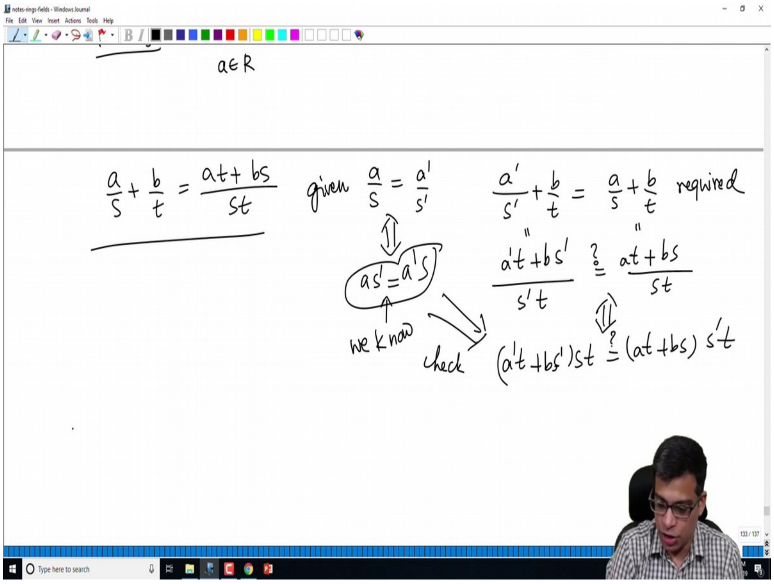


So, why is that phi is injective, because suppose, phi of a is 0 for some a in R this implies a by 1 is 0, because that is the meaning of phi of a phi of a is a by 1. So, a by 1 is 0; that means, 0 can be thought of a 0 by 1; that means, actually is yeah so, this is 0 element is 0 by 1 so; that means, a is 0 ok. So, to do well define so, actually one think that I did not that is hidden in this exercise, you want to show that this is well define, this addition, because a by s may be equal to a prime by s prime, but then when you replace that by a prime by s prime you want to check that what you get is same.

So, hidden in this exercise is you are also required to check that this addition and multiplication are well defined. So, that is hidden in here, only after you check that they are well defined you can start verifying that the ring axioms are satisfied. So, just to may be start the verification, I will let you, I will do the following. So, remember, what we are doing is a by s plus b by t is at plus bs by s t this is the definition, but suppose, a by s is equal to a prime by s prime that can happen right, because rational numbers have various representation 1 by 2 is same as 2 by 4. So, then we want to check that a prime by s prime plus b by t is equal to a by s plus b by t.

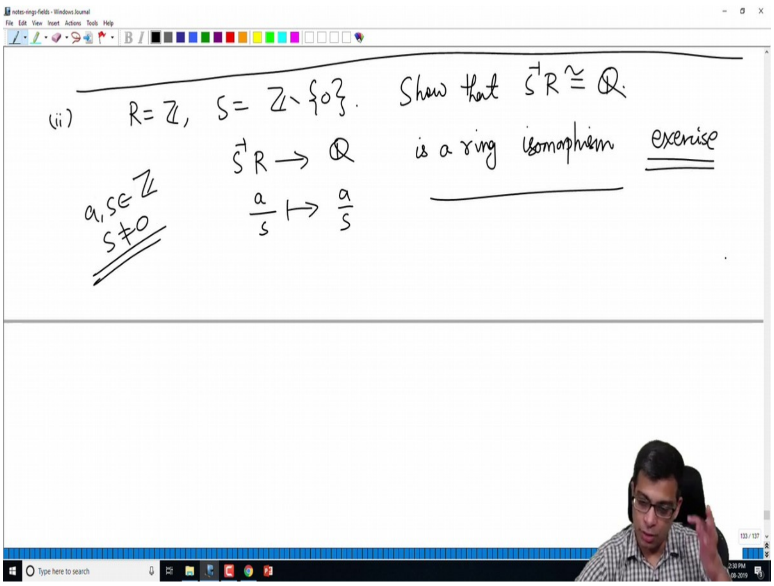
This is required for well definiteness, but what is this is a prime t plus b s prime by s prime t, this is and the question is whether these are equal a t plus b s by s t.

(Refer Slide Time: 16:24)



Remember, this happens if and only if a prime t plus b s prime times s t is equal to a t plus b s times s prime t this is what we want to check, but we are given this a s by a by s is equal to a prime by s prime; that means,. So, we are given this; that means, a s prime equal to a prime s so; that means, this we know and now, you can just expand this out and you see that using this fact, we can get this fact. So, we you check this. All you need to do is multiply this out and cancel for some common terms and you will get what you want so, that I will leave you to check. So, this shows that it is well defined.

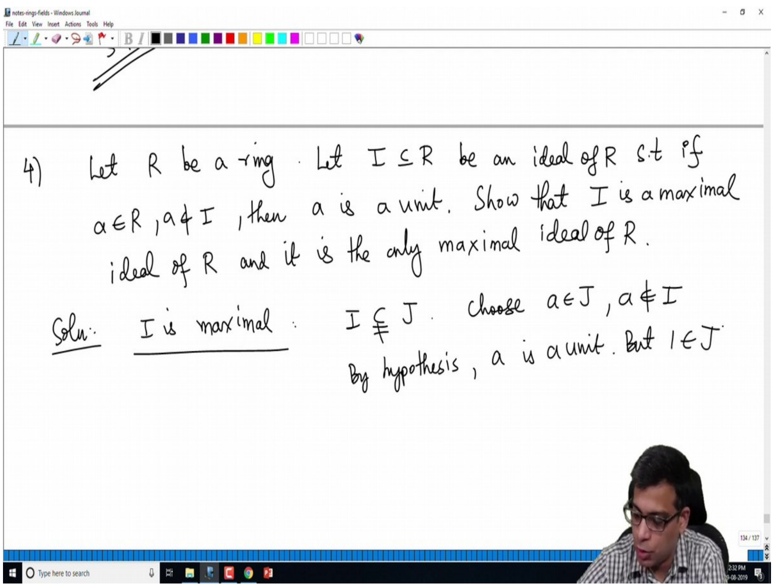
(Refer Slide Time: 17:14)



Now, the second part of the exercise I want to check is let us take R to be Z and S to be Z minus 0; this is our model for the localization, then we have to verify that actually what we get is S inverse R is equal to Q ok. This I will not do all the details, but it is clear what the map should be send S inverse R to Q in the following way a by s should go to a by s.

Remember a and s are integers here right and s is not 0. So, s a by s is actually a rational number is a ring and so, this map is a ring isomorphism. So, the more general process that we define now, for any integral domain and any multiplicative set in it, contains with in it as a special case, the well known construction of rational numbers from integers. So, this I will leave as an exercise for you, not very difficult. So, that is not surprise, it is not surprising that it generalizes the well known construction of rational numbers from integer.

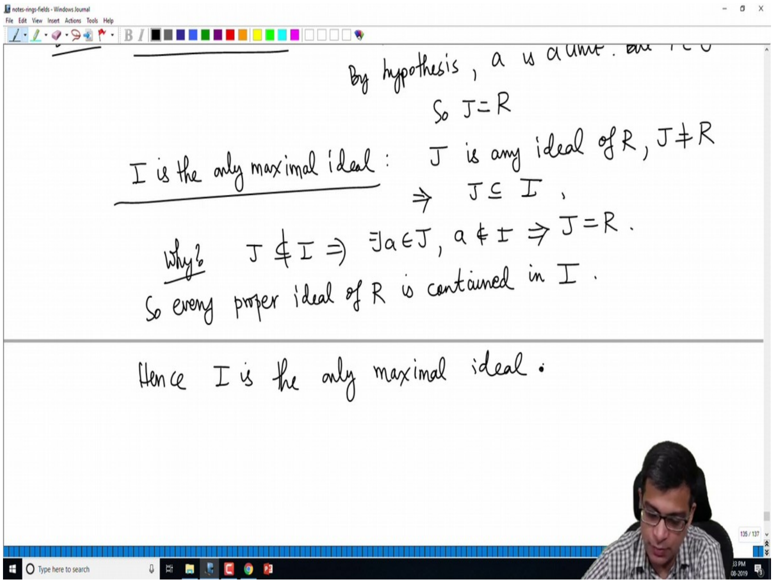
(Refer Slide Time: 18:27)



So, let me do now one more problem and then we will connect it to the localization this and this is a very simple problem. So, let us write it here, let R be a ring, let I be an ideal of R such that if a is in R and a is not in I, then a is a unit, show that I is the only, I is a maximal ideal and it is a only maximal ideal and it is the only maximal ideal of R.

So, such rings are called local rings. So, it is an ideal it is a maximal ideal and it is the only maximal ideal. So, let us prove this, very easy. First of all I is maximal, why? Suppose, I is contained in J and it is not equal to J. So, choose a in J a not in I right, if J is strictly bigger ideal, it must contain an element which is not in I, but by hypothesis, what is a hypothesis? Every element of the ring which is not in I is a unit. So, a is a unit, but then one belongs to J because a times something is 1 a is in J. So, 1 is in J. So, J is R.

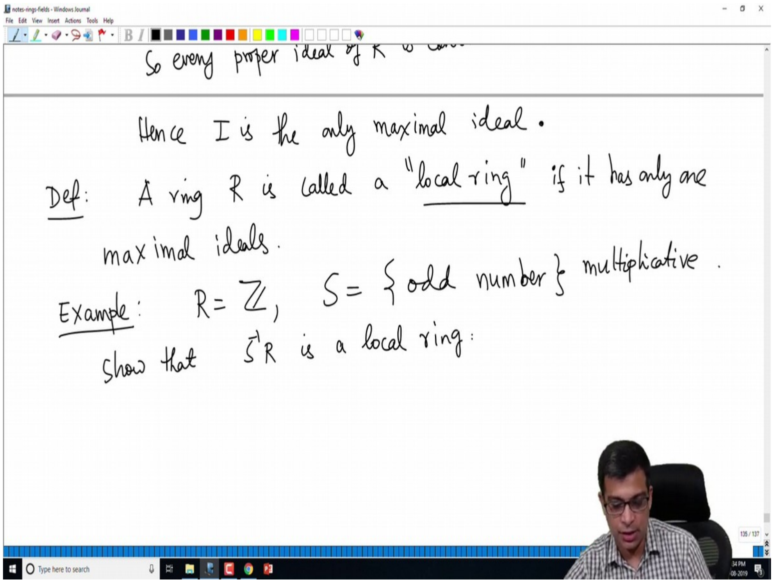
(Refer Slide Time: 20:16)



So, any ideal that strictly contains I must be equal to R. The next part is I is the only maximal ideal. Why is this? Suppose, J is any ideal of R implies I claim J is contained in I. I claim that every ideal of proper ideal of R is contained in I, why is this? So, if suppose, J is not contained in I; that means, there exist a in J, a not in I by definition if J is not contained in I; that means, J is not a sub set of I, it must contain something that is not in I.

By the above argument; that means, J is in R ok, but we are assuming J is not in R. So, every proper ideal of R is contained in I, but this means I must be the only maximal ideal right. Hence, I is the only maximal ideal, why is this? This is, because if there is another maximal ideal, we known it is a proper ideal, but then it must be contained in I, but a maximal ideal cannot be contained in I, a bigger ideal so, unless it equal to I. So, it is equal to I. So, in no other maximal ideal can exist. So, there is an important definition for you a ring R is called a local ring.

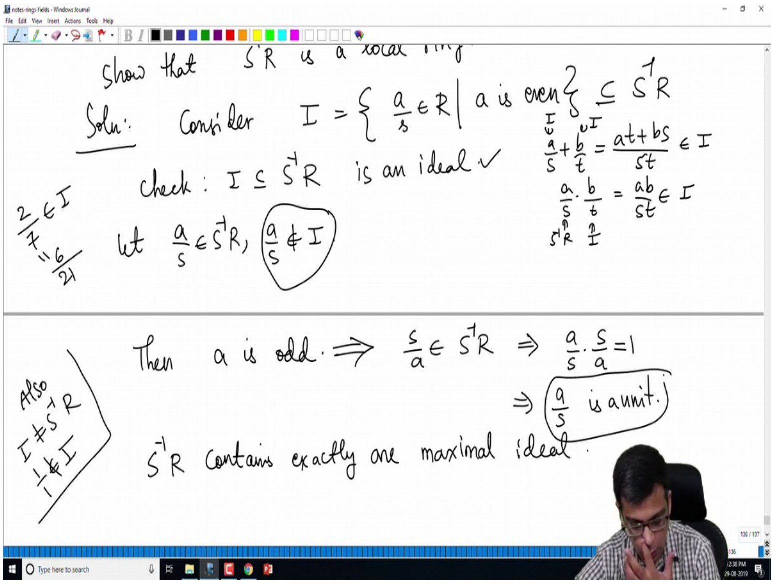
(Refer Slide Time: 21:56)



So, this notation is related to algebraic geometry, where this is such things are studied, R is a local ring if it has only one maximal ideal. Every ring has a maximal ideal by Zorn's Lemma we proved earlier. If there is exactly one maximal ideal, it is called a local ring. What are examples of this? So, this is part of the exercise that I will do and in fact, I will leave many details to you.

Let us take R to be Z and S to be the set of odd numbers in the first beginning of this video. We showed that this is multiplicative show that S inverse R is a local ring, using the previous exercise. Why is this?

(Refer Slide Time: 23:00)



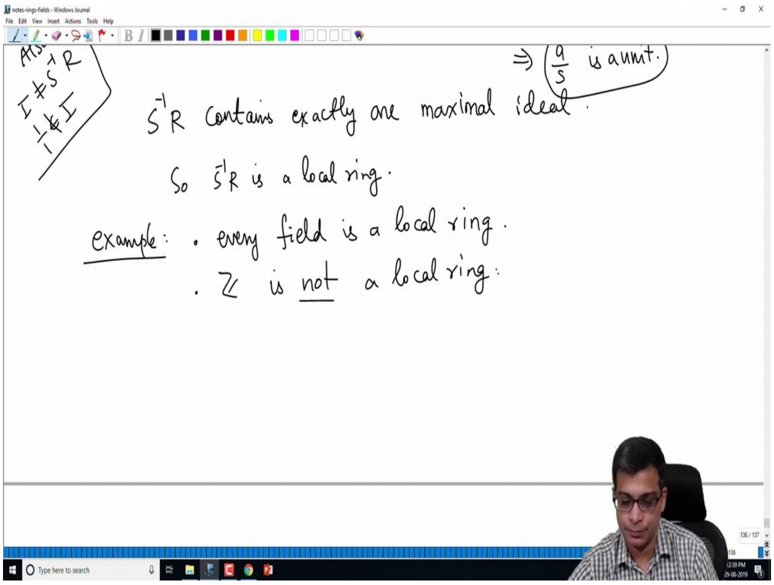
So, first of all consider the following set I in S inverse R a by s in R such that a is even. So, one can check that I is an ideal of S inverse R. So, it is a sub set of S inverse R it is. In fact, an ideal why is that? 0 is there, if you add two things a t plus b s by s t, if a is even and b is even, a t plus b is also even. So, this is an I similarly, if a by s times any element. So, in this case both are in I now, suppose this is in R S inverse R and this is in I this is a b by s t, but if b by t is in I means b is even. So, a b by s t is also an I, because if b is even, a b is even.

So, this is an ideal and now, take an element that is not in I. So, let a by s a by s be in S inverse R and not in I then by definition of I a is odd right. So, the here I suppressing somethings, there could be several represent representations of a by s, never the less for all of them the numerator will be even or for all of them numerator will be odd, because for example, in this example what is an example of things in I.

So, 2 by 7 is in I right, because a numerator is odd, but 2 by 7 may be also written as 6 by 21 by multiplying by three both sides, but even if you use the representation 6 by 21, the numerator is even. You can never write this with an odd number on top divided by another odd number, because 2 by 7 cannot be equal to another odd number by odd number, because when you cross multiply one will be even other will be odd. So, which cannot be, which cannot happen.

So, this is well defined I am suppressing that here. So, you can ask in the discussion forum any questions about this or work it out by yourself, but this is a well defined ideal well defined set. So, now, if somethings is not in I; that means, a is odd, because if a is even then it will be an I so; that means, s by a is in S inverse R right, because if a is odd we can consider s by a so; that means, a by s times s by a is 1, this means a by s is a unit and by the exercise that we just did.

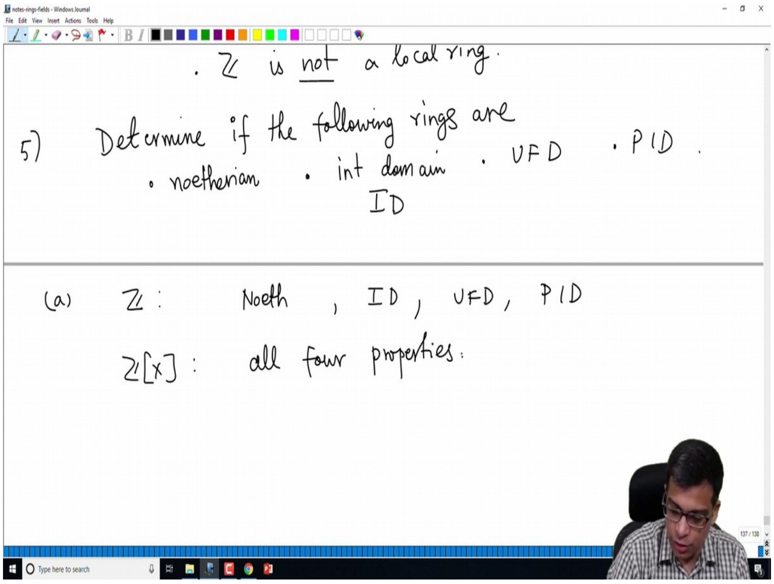
(Refer Slide Time: 26:01)



S inverse R contains exactly one maximal ideal right, because we have found an ideal I and also it is not equal to R, I should say also I is not S inverse R, because for example, 1 by 1 is not in I not in I yes, it is a proper ideal with the property that everything outside it. If you take a by a that is not in it is a unit and by the problem that we just did if you have a ring and an ideal proper ideal in that ring such that everything outside it is an unit that proper ideal is the only maximal ideal of that ring.

So, S inverse R is a local ring. So, this an example of a local ring. Also another example is every field is a local ring, because field has exactly one maximal ideal namely the 0 ideal and just to finish this Z is not a local ring, ring of integers is not a local ring this is, because it has several maximal ideal 2 Z 3 Z 5 Z and so on. So, I am going to now just do one final exercise to list some of the example of rings that we have studied. So, the final example that I want to do may be this the fifth example problem final problem, determine if the following rings are Noetherian.

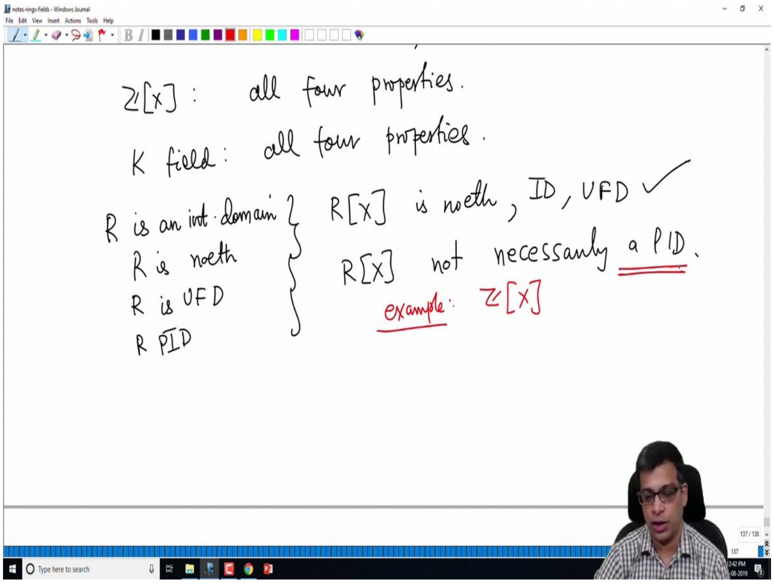
(Refer Slide Time: 27:31)



Remember, Noetherian means ascending chain condition on ideal holds or every ideal is finitely generated, integral domain which I denote by I D, UFD or PID, determine if the following rings have this property. So, let me just this is mainly to list the summarize the rings that we have studied. So, I may forget some of them, but I will try to do as many as I can remember Z so, Noetherian.

So, I will Noetherian yes, integral domain also yes right, because this is our first example of integral domain we have show that it is a PID. So, hence it is a UFD. So, it has all the properties. If you take Z X, this also all four properties; it is a Noetherian ring, it is integral domain, it is UFD, it is PID, any field all four properties.

(Refer Slide Time: 28:50)

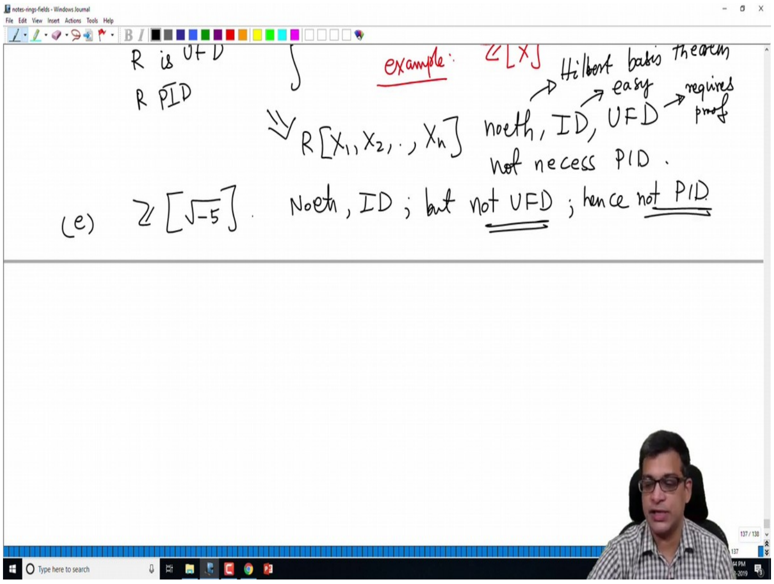


So, these are all simple examples right. A field is Noetherian, it is integral domain; obviously, it is PID UFD, it has only two ideals. So, there is no problem there what about if K, if R is an integral domain and R is Noetherian, what about R X? This is an arbitrary ring which is integral domain and Noetherian, then this is Noetherian right this is also integral domain, you can check if, because multiplication of two non-zero polynomials will give you a non-zero polynomial, this is ok.

But what about UFD or PID that is not clear unless you assume similar conditions for R. So, R is UFD suppose I assume then this is also UFD. R is integral domain Noetherian UFD, then it is a UFD, but if R is PID, R X is not necessarily a PID right, because so, take it, R which has all the four properties that we are interested in Noetherian ID integral domain UFD PID, polynomial ring in one variable inherits three of those properties it is Noetherian integral domain UFD, but not necessarily PID.

What is a example? The simplest example is Zx Z is Noetherian integral domain UFD PID, but it is not a PID. So, this is the property of being a PID is not inherited when you are attach a variable.

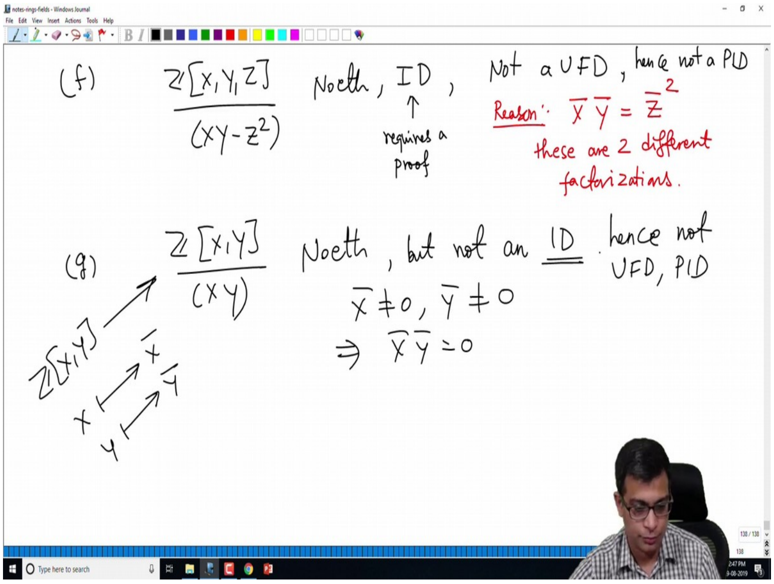
(Refer Slide Time: 31:00)



So, a again this properties will carry over to polynomial rings in any number of variables finitely many. These are Noetherian ID UFD of course, not necessarily PID, as we showed in the one variable case itself and these are important theorems right this is Noetherian part is Hilbert basis theorem, ID part is easy, this is just a simple calculation and UFD is also required proof.

What we have done is for R equal to Z and in those videos I said, proof more or less carries over to any arbitrary UFD ok. So, this is let us say b c d. Let us do one more example some more examples what about Z adjoined square root minus 5? This is Noetherian I D, but not U F D. If you recall in the videos when we discussed UFDs, we showed that this has factorization, but it terminates, but it is not unique, 6 can be written in two different ways as product of irreducible elements. Once it is not be UFD, it cannot be PID, because a PID is a UFD.

(Refer Slide Time: 32:33)



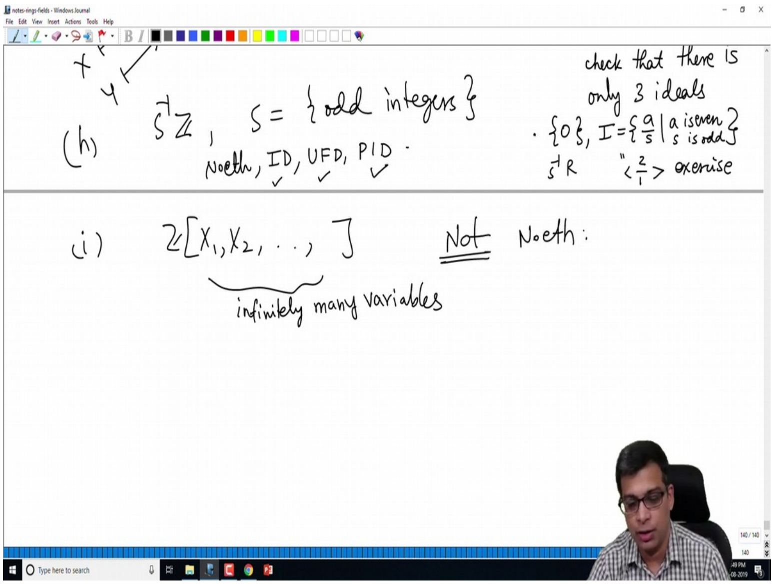
Next example ok, some of these are not immediate one has to check. So, what I will let you do is this is Noetherian, because this is a polynomial ring in one variable three variables modulo an ideal. So, image of a Noetherian ring is Noetherian and the ring Z X Y Z is Noetherian. So, when you quotient by this the image of Z Z Y Z; so, it also Noetherian ID requires a proof and let me not do that for now. And, we can discuss it in may be discussion forum this is an irreducible polynomial that one I has to show you cannot write this is the product of two polynomial.

So, it is irreducible. So, it is a integral domain it is not a UFD and the reason is X bar y bar is equal to z bar squared. So, this is these are two different factorizations. So, these are two different factorizations. So, this is not UFD and hence, not a PID. So, one has to check this, what really one has to check is X by X bar y bar z bar are three distinct irreducible elements. That is not that difficult to check that I will leave it for you g Zxy mod X Y.

So, this is Noetherian, because again Z X Y is Noetherian by Hilbert basis theorem, Z X Y mod XY is an homomorphic image of Z X Y, because there is the unique surjective map there is a natural surjective map from Z X Y to Z X mod XY and image of Noetherian ring is Noetherian. So, this is Noetherian, but this is not a integral domain and hence now, not UFD PID also, because UFD PIDs are D stands for domain.

So, something that is not a integral domain cannot be UFD or PID, why is it not in ID, because X bar and Y bar are not 0, but X bar Y bar is 0. So, when I write bar I mean simply the images under the natural map from Z X to Z X Y to this the residence of X and Y what about. So, the next example so, this is a example of something that not even integral domain.

(Refer Slide Time: 35:21)

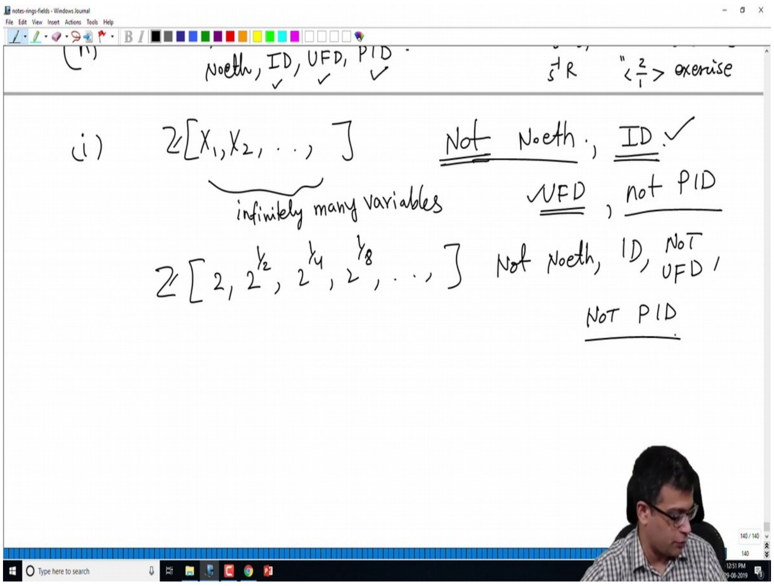


So, one more example: so, the ring that we consider X inverse R S inverse Z where S is odd integers, the previous problem that we considered. Here, S inverse R 1 can check. So, S inverse R is Noetherian see, there is only one ideal here, right one maximal ideal and actually that is I am not saying that there is only one ideal, there are many ideals, but only one maximal ideal and one can check that every ideal actually, I have proved that there is only one ideal only maximal ideal check that there is only three ideals 0, the ideal I from last problem, which is a by s, where a is even and s is of course, odd and S inverse R itself.

There are only three ideals, these are the three ideals. So, now, Noetherians can be checked, because one equivalent condition for Noetherian S is every ideal is finitely generated. Here of course, there are only three ideals they are all finitely generated I can be written as the ideal generated by 2 by 1, 2 by 1 generate set. So, one can check this is an exercise for you. So, it is Noetherian it is a integral domain and it is a PID actually, because every ideal is principal here, there only three ideals. 0 is certainly principle generate by 0, S inverse R is certainly principle generated by S inverse R and I is generated by 2 sorry, S inverse R is generated by 1, I is generated by 2 1. So, it is a PID.

So, it is also UFD and one can check that it is an ID of course, that is required to verify the deep part in UFD and PID. So, this is an example of another ring, which is Noetherian integral domain UFD and PID and let me just give you a final example, where something which is not even Noetherian. For example, if you take Z adjoined X 1 X 2 infinitely many variables, this is not Noetherian ok. The ideal generated by all variables is not a finitely generated ideal. Similarly, it is though integral domain ok.

(Refer Slide Time: 38:03)



It is integral domain, it is also UFD one can show, but not PID, just like you can show unit factorization for polynomial in finitely many variables, you can show it for infinitely many variables, because to determine unit factorization you only look at once specific element. You take a specific polynomial, it only inverse finitely many variable. So, you are really working in finitely polynomial ring which is UFD it is certainly not PID, because you attach two variables it is already not PID.

It is not Noetherian similarly, one more example that we looked at was 2, second power of 2 fourth power of 2 it is not Noetherian, it is integral domain UFD, it is actually not UFD, that was one our example right and of course, not PID. It is not a UFD, because we constructed this ring to show that factorization does not even terminate in this ring ok. So, in this case it is not even a UFD.

So, these are the examples of some of the rings that we discussed in this a ring theory part of this course and I wanted to list all of them, because and with respect to the four properties that we emphasized here; integral domain, Noetherian, UFD, PID. So, I hope these are clear, please go back and see this video again if you have anything that is not clear you can ask questions about this. So, this completes the discussion on ring theory; in the next video we are going to start talking about fields.

Thank you.