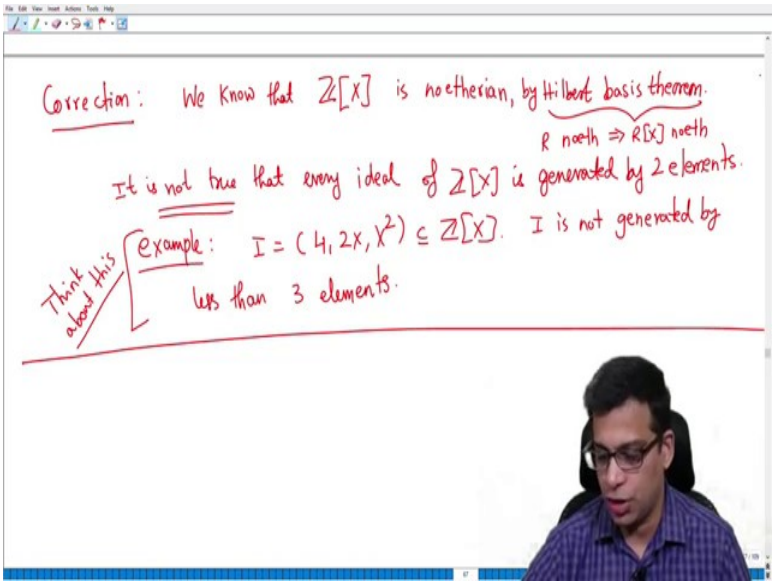
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 23
Irreducible, prime elements

Let us continue now. Before I talk about unique factorization domains and principle ideal domains which is going to be our goal for the next few videos, let me correct something I said in a previous video which was incorrect, ok.

(Refer Slide Time: 00:35)



So, let me make this is the correction. So, this is the correction that I want to make and the correction is something where I made remark that I made in passing. So, recall that, we know that the polynomial ring in one variable over Z is noetherian. We definitely know that because we can use Hilbert basis theorem right, Hilbert basis theorem, recall which we proved last time says that if you have a noetherian ring this says that R noetherian implies R X noetherian.

So, the polynomial ring in one variable or a noetherian ring is also noetherian, we certainly know that the ring of integers is noetherian because every ideal in Z is actually principal, finitely generated so, Z X is noetherian. The mistake I made was, when I said that every ideal in Z X is generated by 2 elements. So, the statement now I want to it is not true that every element of Z X is generated by 2 elements ok. So, this is something

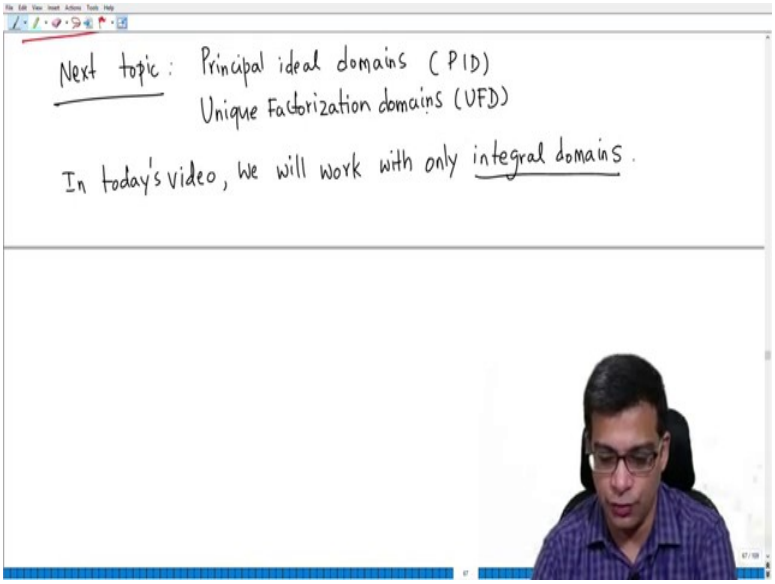
that I said in a previous video and I actually asked you to do as an exercise, that statement so that you know that Z X is noetherian without using Hilbert basis theorem, but this is not true ok.

So in fact, there are elements there are ideals sorry I should not say element, every it is not true that every ideal of Z X is generated by 2 elements that is false. In fact, there are ideals in Z X that are generated by three elements and that cannot be generated by 2 elements in more generally and we have in fact, for any n there are ideals of Z X that are generated by n elements, but not by n minus 1 elements ok. So, as an example this is something that I cannot prove, it requires some more techniques in ring theory to prove this.

So, I will only assert this you can think about this some other time. So, if you take the ideal generated by 4, 2 X and X squared ok. So, certainly I is generated by three elements by definition by 4, 2 X and X squared; I is not generated by less than three elements. So, I is not principal which is not difficult to show and, but I is also not generated by any 2 elements. So, that you take there are no 2 elements in I that generate I that is what I mean you need at least three elements to generate I.

So, as I said this requires some techniques that we are not going to cover in this course, but it is something for you to keep in your mind. Remember that, the fact that Z X is noetherian is still true, we do not need this stronger statement that every ideal of Z X is generated by 2 elements, we only need this statement that every ideal of Z X is finitely generated. I is in this example certainly finitely generated because it is generated by three elements. I am saying that it is not generated by less than three elements so that is just correction I wanted to make about noetherian rings in this example that we discussed in a previous video ok.

(Refer Slide Time: 04:49)

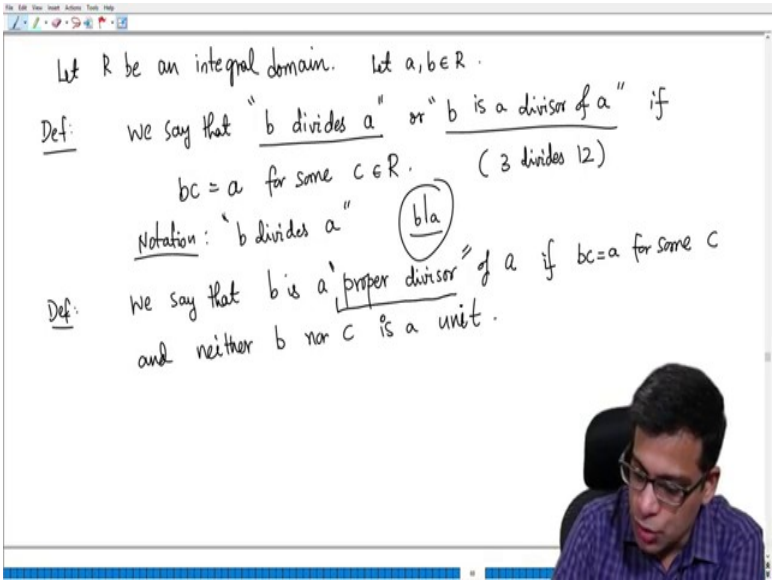


So, the next goal for us is to introduce next goal next topic in the course is what are called Principal Ideal Domains and which I will denote which is very standard notation is called PID, Principal Ideal Domains and Unique Factorization Domains; so, these are called UFD; so these are the abbreviations so, these are special kinds of rings.

So, the rings which have certain nice properties and we will discuss these in this video and next 2 or 3 videos ok. So, before I start talking about these exact properties of these rings, let me introduce some generalities so, some general stuff. So, in today's video and in next few videos, we will work with only integral domains ok.

So, many of the concepts that we will introduce are valid only for integral domains and the reason we do this is principal ideal domains, unique factorization domains as the word domain suggests, they are actually integral domains and with additional properties. So, we are going to stick to integral domains.

(Refer Slide Time: 06:27)



So, let us start with this, let R be an integral domain; as I am going to do this concepts that I will introduce in today's video, keep in mind the example of the integers, all these concepts are actually developed with integers as the model.

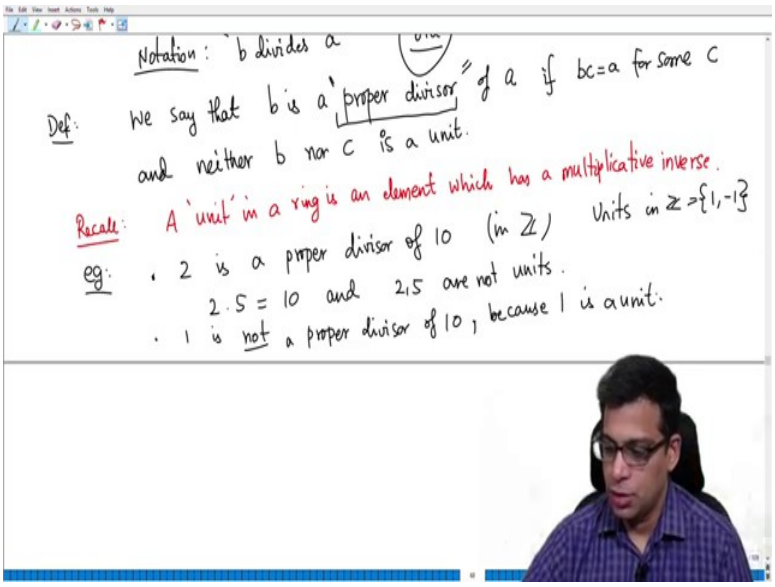
So, we look at the nice properties that integers have and try to generalize them to more rings ok. So, in this process, let me define give some definitions so, these are just definitions or notations. So, we say that so, let a and b be two elements of R ok. So, let us say a and b are two elements of R, we say that so, this is very common language, but I want to formally define this. So, that in future it will be clear to you, we say that b divides a or b is a divisor of a. So, you are familiar with the notion of division for integers so, I am trying to generalize this to an arbitrary integral domain.

We say b divides a or b is a divisor of a if the most natural thing right bc is equal to a for some c in R. So, if a is a multiple of b, we say b divides a; this is of course, what we mean when we say 3 divides 12 right 3 divides 12; that means, 3 that is because 3 times 4 is 12. So, that is now generalized to an arbitrary ring situation and we use a notation this is convenient instead of writing in words b divides a, we write b divides a to indicate that we write b vertical bar a this implies this is a shorthand for the statement b divides a that I will use often or that b is a proper b is a divisor of a.

On the other hand, we want to introduce the notion of a proper divisor we say that b is a proper divisor of a if, of course, first of all b divides if b c is equal to a for some c and

neither b nor c is a unit so, this is an important notion here. So, let me explain this, first of all in order for a proper divisor in order to be a proper divisor, it must be a divisor, but I want to rule out certain obvious divisors, I do not want to consider those trivial divisors. So, I am introducing the notion of a proper divisor, what do I mean by a proper divisor, I first of all want b to divide it so, b c is equal to a, but I do not want c or b to be unit, recall.

(Refer Slide Time: 10:04)

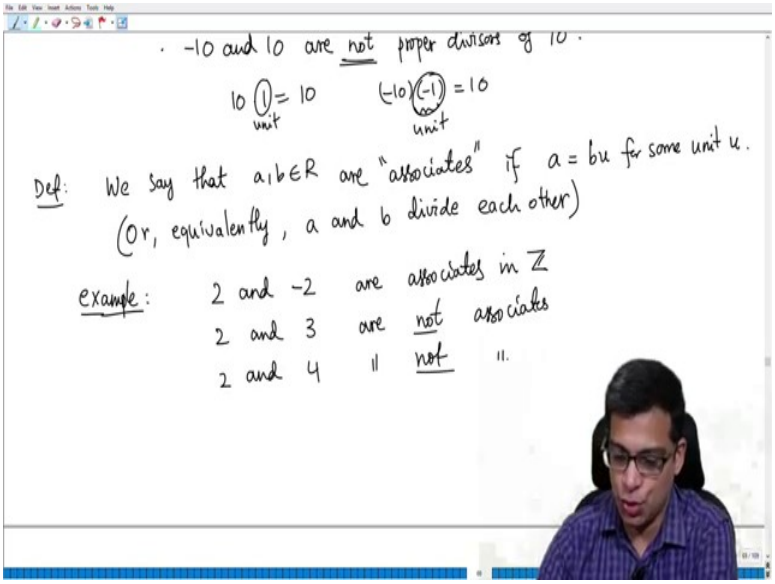


So, recall that a unit in a ring is an element with which has a, remember what is a unit, it is an element which has the multiplicative inverse. Remember in a ring not every element is required to have a multiplicative inverse. If it does have a multiplicative inverse, we call it a unit ok.

So, this is in so, in order to be a proper divisor first of all it cannot be a unit and it that what it multiplies to cannot also be a unit. So, as an example, we can say 2 is a proper divisor of 10 right in Z of course, this is the example is in Z. 2 is a proper divisor of 10 because 2 times 5 is 10 and 2 and 5 are not units. What are units in Z? It is clear that the only units in Z are the integer 1 and the integer minus 1.

So, 2 is a proper divisor of 10. On the other hand, 1 is not a proper divisor of, it is a divisor all right, but it is not a proper divisor of 10 right. This is because 1 is a unit, a proper divisor cannot be a unit.

(Refer Slide Time: 11:58)

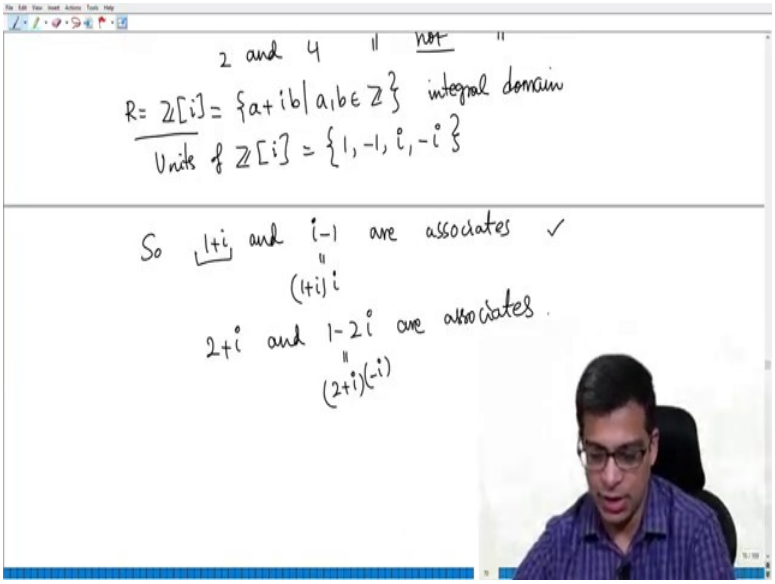


So, on the other hand minus 10 is also not a minus 10 and 10 are not proper divisors of 10 also right because 10 times 1 is 10, but this is a unit. Similarly, minus 10 times minus 1 is 10 and this is a unit. So, 10 and minus 10 are actually divisors of 10, but the what you multiply them with to get 10 is a unit. So, 10 and minus 10 are not proper divisors, 1 is not a proper divisor.

So, 10 has several divisors, but only some of them are not proper, some of them are proper. So, this is a general notion in general in any ring, we have the notion of a proper divisor. One more definition, we say that two elements a, b in R. So, now, I am back in arbitrary integral domain remember that I am not working with an arbitrary ring in this video, I am working with an arbitrary integral domain. We say that two elements a, b in an integral domain are associates if a is equal to bu for some unit u or equivalently a and b divide each other ok.

So, associates means a divides b, b divides a of course, every element is an associate of itself, but there could be more two different elements which are associates of each other. For example, 2 and minus 2 are associates in Z right 2 is minus 2 times minus 1, minus 1 is a unit. So, they are associates 2 and 3 are not associates, 2 and 4 are not associates right. The only associate of 2 is actually 2 or minus 2. So, in Z, this what is this what happens.

(Refer Slide Time: 14:44)



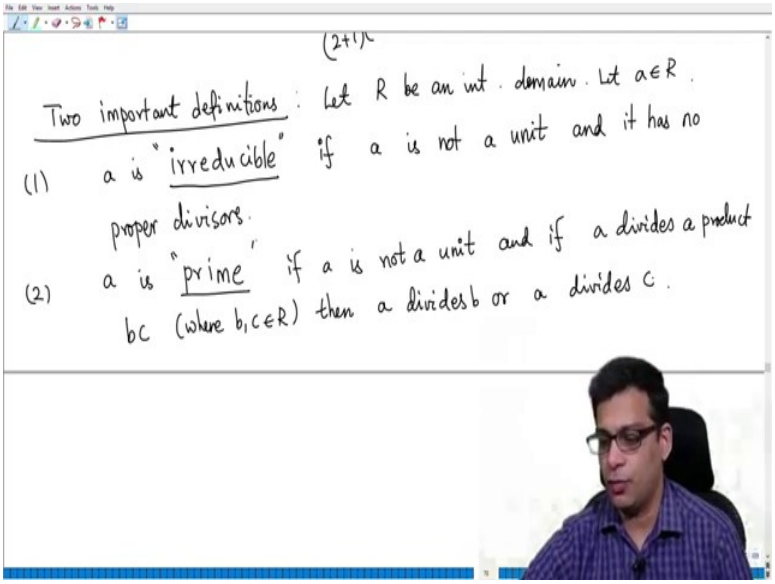
In let us look at another example now R equal to Z i remember Z i is the set is the ring of all complex numbers which are of the form a plus i b, where a and b are integers and this is an integral domain being a sub ring of field, it is an integral domain. So, we can also talk about associates in this ring and what are units of R, I do not recall if I explicitly did this, but I mentioned this I think sometime in the beginning of this course.

Units of Z i are actually there are 4 of them 1, minus 1, i, minus, i. So, these are the units of this rings Z i. So, now, in using these units, we conclude we see that. So, 1 plus i and i minus 1 are units are associates, why is this, because i minus 1 is 1 plus i times i right, i is a unit, this times i unit is 1 minus i minus 1 so, they are associates. Similarly, 2 plus i and 1 minus 2 i are associates because 2 plus i times so, let us see 2 plus i times i or minus i, minus i is also unit when you multiply 2 plus i and minus i, you get minus 2 i plus 1 which is equal to this. So, these are also associates.

So, this examples shows that associates may look different in the familiar example if integers of course, an associate of a number is either that number or the negative of a that of that number, but if a ring has more units you have more interesting associates. So, these are examples of associates ok.

So, now, we have defined what it means for an element to be a divisor of another element, what it means for an element to be a proper divisor of another element and we also defined the notion of associates.

(Refer Slide Time: 17:06)



So, now I am going to give you two very important definitions which are valid in any integral domains ok. So, what are these two important definitions? 1 so, let R be an integral domain, I will shorten it like this let R be an integral domain. So, I want to define the following two things. So, first I will say that and let a be an element of R ok. So, we say that a is irreducible so, we have talked about irreducible polynomials earlier and this is actually same as that, but now I am doing this not just in any polynomial ring, but in fact, for any integral domain, a is irreducible if the following happens.

What you think it should happen? Remember, irreducible polynomials are those that do not factor in a non trivial way. So, same notion I will use, a is irreducible if I want first of all that a should not be a unit; I do not want to call units irreducible for simplicity because I do not want to every time I am working in a proof or something I and I am working with irreducible elements, I do not want to assume that it is not the unit.

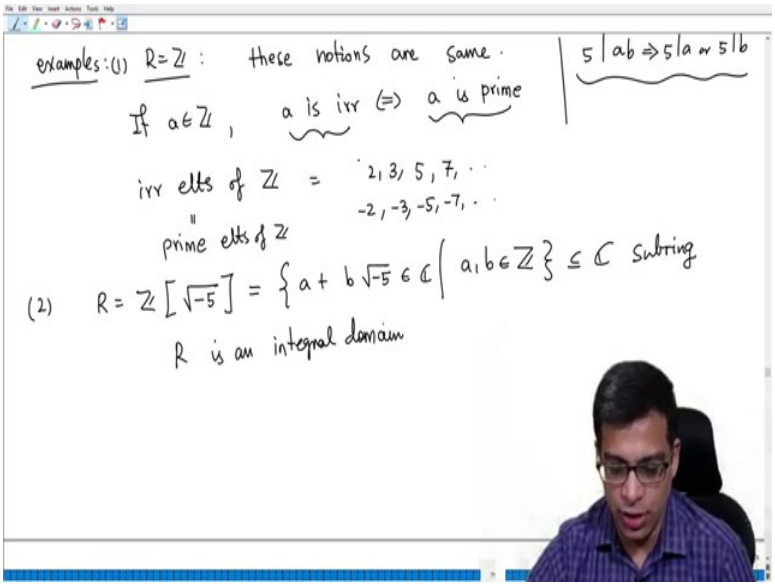
So, I will declare that a irreducible element is by definition not a unit and it has no proper divisors right. So, if you think about this, this is exactly what we have in the case of polynomial rings, a polynomial is a reducible if it really has no proper divisor.

Remember, everything has a divisor because a is a divisor of itself, any unit is a divisor of a, but I do not want to consider those as actual divisors. So, I will only as that it has no proper divisors then it is irreducible, I will give you examples and discuss more about this after giving both definitions. So, the other important definition is a is prime.

So, the other important definition is a is prime again if a is not a unit. So, I again do not want to consider units as primes and if a divides a product bc where of course, b and c are elements of R this should recall for you the definition of prime numbers in integers.

So, if a is not a unit and if a divides a product bc then a divides b or a divides c, right. So, this is what we call a prime element, a prime element is one which is not a unit and it has a property that if it divides a product of two elements two other ring elements, it must divide one of them.

(Refer Slide Time: 20:33)



So, now let me quickly give you some obvious examples before we discuss more interesting examples. When R is Z these two notions are same, what I mean is, an integer if a belongs to Z, a is irreducible if and only if a is prime. This is something that you may have studied in you may remember from some high school arithmetic that you may have done.

See prime numbers of course, we know it is a one definition of prime number is that what we are now calling irreducible is often what people think of as prime integer because a number an integer is prime if it has no factors other than one and that integer, but one and that integer in our notation are not proper divisors. So, you take a positive integer, we call it a prime if it has no other positive proper divisors, it has no divisors other than 1 and p; then p is prime.

That notion is actually what we are calling irreducible in the case of an arbitrary integral domain, but you also do after defining prime numbers, the theorem that a prime integer has a property that if that integer p is prime if and only if p divides a product of two integers a and b then it must divide one of them.

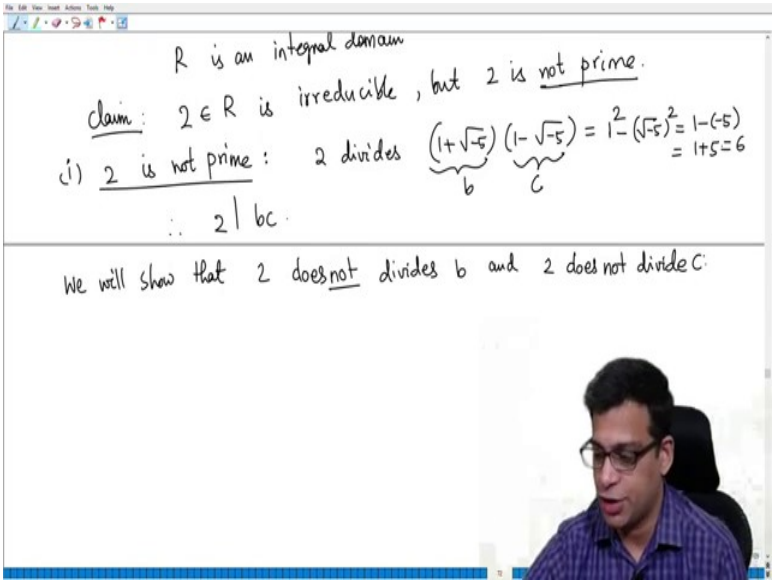
For example, 5 divides a b this is something you would have seen before then 5 divides a or 5 divides b, this kind of statement you see in, this kind of statement is familiar to you. 5 is prime because it has this property, that is what we are calling a prime element in an integral domain. In the case of the integral domain Z, these are actually same irreducibility is equivalent to primality. So, what are irreducible elements Z; I mean you can write 1 should not be considered irreducible because 1 is a unit.

So, there are 2, 5, 2, 3, 5, 7 so on and of course, we can also consider nothing in the definition, disallows these allows negatives of these are also prime elements or irreducible elements ok. So, in the case of Z, it is very clear that they are both the same concept; an element is irreducible if and only if it is prime.

So, now on the other hand so, this as I said, a familiar example. Now, let us look at the ring R equal to Z adjoined square root of minus 5. Now, this ring is very similar to Z adjoined i, in the sense that it is all complex numbers which are of the form a plus b times square root minus 5, where a and b are integers.

So, this is a sub ring of C so, R is an integral domain so, R is an integral domain. So, in this I want to introduce, I want to actually show that there is an irreducible element that is not prime which that phenomenon does not happen in Z because every irreducible element is prime every prime element is irreducible, but that is not in general true.

(Refer Slide Time: 24:27)



So, in this I make two claims, 2 as an element of R is irreducible, but 2 is not prime ok. So, this I am I am going to prove these two statements. So, I am claiming that the element 2 in the ring R which is Z adjoined square root minus 5 is irreducible, but not prime so, in general in other words irreducible elements need not be prime.

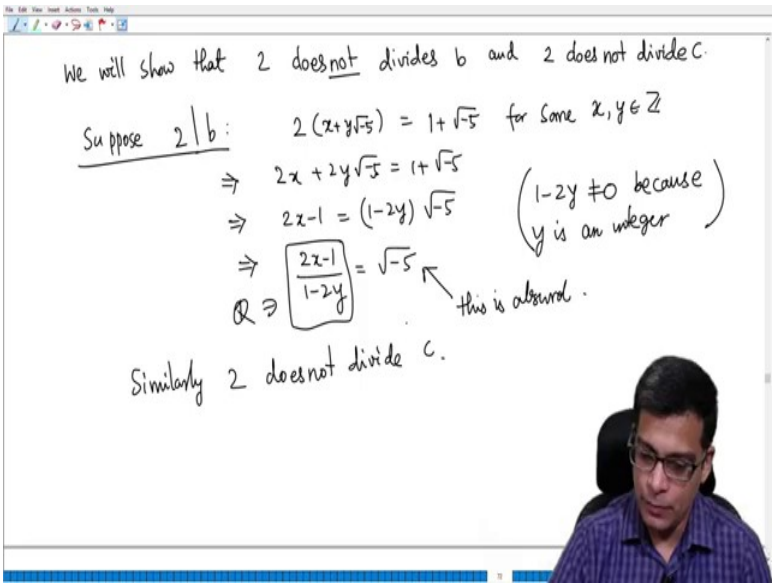
So, first of all, why is 2 prime or not prime. So, let us prove that first, 2 is not prime ok. The remaining part of this video will be proving this claim which is which is not difficult, but it is a tedious calculation. So, please make sure that you carefully follow this, this is an interesting example that we will encounter again in the course. So, 2 is not prime, what do I need to show that 2 is not prime, I need to show that there are two elements in the ring whose product 2 divides but 2 does not divide it.

So, and the product that I will take is 6. So, 2 divides I claim 1 plus root minus 5 times 5 minus root minus 5, what is one plus. So, this is my b if you want and this is my c, what is 1 plus root minus 5 times 1 minus root minus 5, this is the usual form right a minus b times a plus b is s squared minus b squared so, this is 1 squared minus square root minus 5 squared. So, this is 1 minus minus 5, this is 1 plus 5 which is 6.

So, certainly 2 divides b c so, 2 divides b c, we will show now that 2 does not divide b and 2 does not divide c right.

If 2 divides the product of b and c, but 2 does not divide b or 2 does not divide c then by definition 2 cannot be a prime. So, why does not 2 does not divide why does, why does not 2 divide b, the reason is so, suppose 2 divides b.

(Refer Slide Time: 26:56)



So, we proceed by contradiction, suppose 2 divides b, what is the meaning of that. At the beginning of this video, I told you in general in any ring when an element divides another element I mean that 2 times some ring element is b right, 2 times a ring element is b. In this case, 2 divides 6 because 2 is of course, 2 times 3 is 6 so, 2 divides 6.

So, 2 divides b remember b is 1 plus root minus 5 if 2 times some x plus y square root minus 5 is equal to 1 plus root minus 5, where x and y are in Z, if there exists x and y integers such that 2 times x plus y minus y square root minus 5 is equal to 1 plus square root minus 5 then we say 2 divides 1 plus square root minus 5.

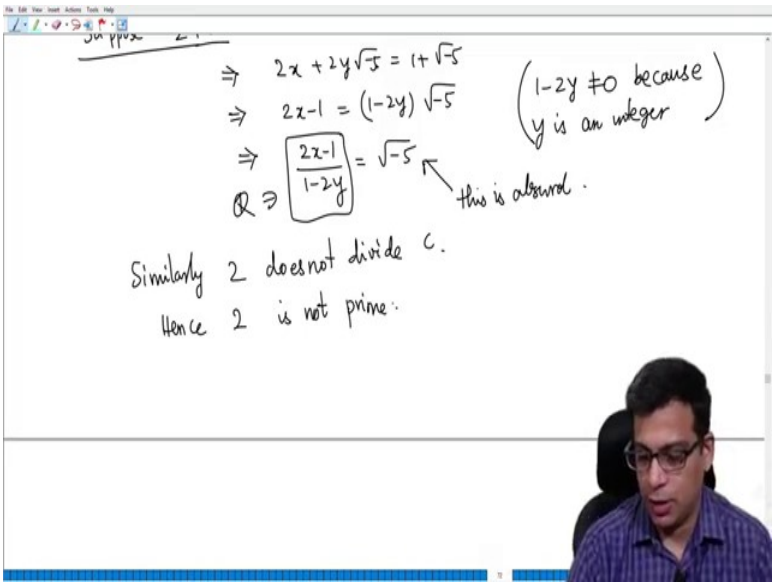
So, I am going to show that this is not possible. So, lets see some consequence of this equality you have 2 x plus 2 y square root minus 5 is 1 plus square root minus 5. So, I am going to rearrange terms here, I will subtract 1 and write 1 minus 2 y times square root minus 5 right. So, I am pooling together the like terms 2 x minus 1 so, 1 comes here 2 y square root minus 5 goes there. So, I have 1 minus 2 y times square root 5, but now I can work inside the complex numbers, these are all complex numbers in other words, I can divide by 1 minus 2 y to do this.

First of all, 1 minus 2 y cannot be 0 because y is an integer. Remember, y is an integer; that means, 1 cannot equal to y, 1 is an odd integer in other words so, 1 minus 2 y cannot be 0. So, I can divide by 1 minus 2 y, but this is absurd, why is this absurd, for several reasons; one reason is that this is a rational number right because it is a ratio of two integers, it is rational number certainly square root minus 5 is not a rational number also this real number, but this cannot be a real number so that is another reason.

So, 2 does not divide b so, do you agree that I have proved that 2 does not divide b similarly, 2 does not divide right so, I hope this is clear to you.

So, the same proof more or less, you assume that 2 times x plus 5 times x plus 5 square root minus y is equal to 1 minus square root minus 5 which was c and do similar calculation to get a contradiction. So, 2 does not divide c, 2 does not divide b, but 2 divides bc.

(Refer Slide Time: 30:15)



Hence, 2 is not prime; so this is the first part.