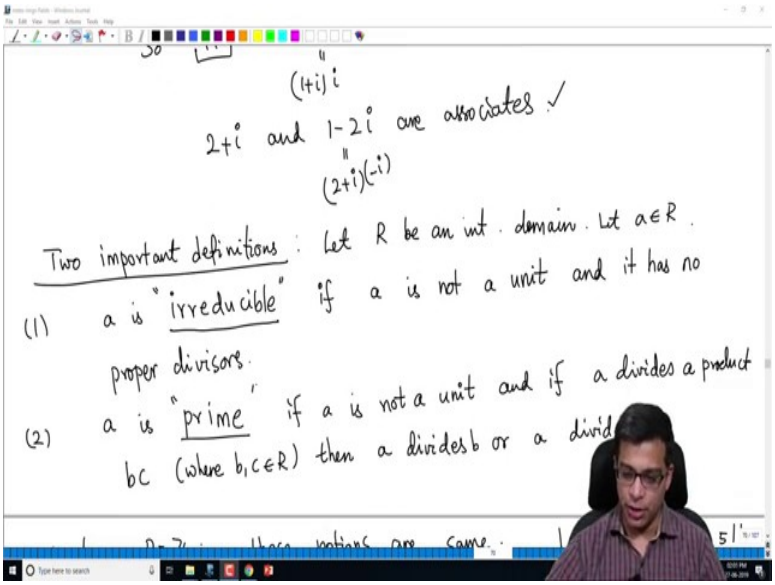
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture – 24
Irreducible, prime elements, GCD

In the last video, I defined the notion of irreducible elements and prime elements in an arbitrary integral domain, and we are looking at various examples. Let us recall what is a, what is an irreducible element, so and what is a prime element.

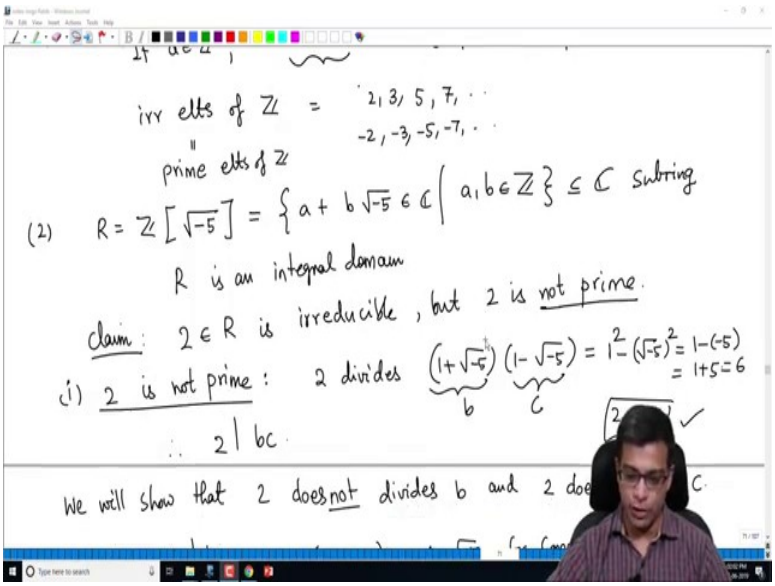
(Refer Slide Time: 00:33)



So, before I start the new material, this is the definition, right. So, an irreducible element is a element which is not a unit and it has no proper divisors. So, we talked about the notion of divisors, just like we have the notion of divisors in integers we have divisors. And, a proper divisor is analogous to proper divisor is a, proper divisors in the integers, where for example, number 10 has divisors 1 and 10 certainly, but they are not considered proper divisors. So, proper divisors of 10 are 2 and 5.

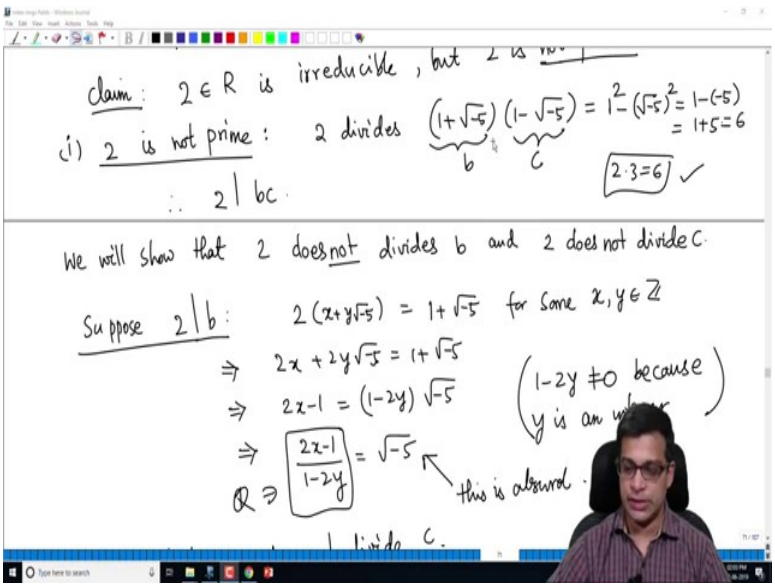
So, an irreducible element in an arbitrary integral domain is an element which has no proper divisors. On the other hand, a prime element is an element which when it divides a product of two elements, it must divide one of them. In the case of integers, they both agree, which is not difficult to check using high school arithmetic and elsewhere it will follow from our general results that we will prove later.

(Refer Slide Time: 01:25)



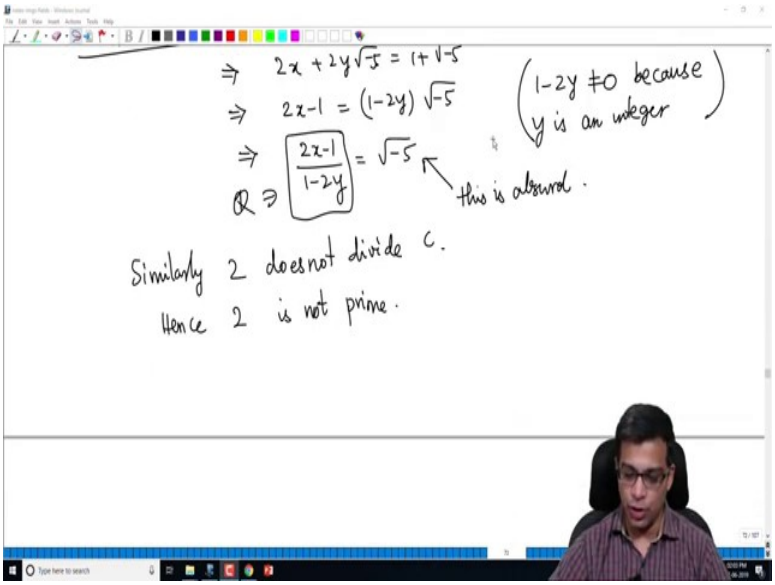
And I ended the last video, half way between, half way in the example that we are doing. We are trying to give an example of an element in a ring which is irreducible, but not prime. So, we considered the ring R which is Z adjoint square root minus 5. So, it consists of elements like this a plus b times square root minus 5, where a and b are integers. And in this we are trying to look for an irreducible element which is not prime. And I claimed that 2 will do the job for us and I think in the end, by the end of the last video I proved that 2 is not prime.

(Refer Slide Time: 01:56)

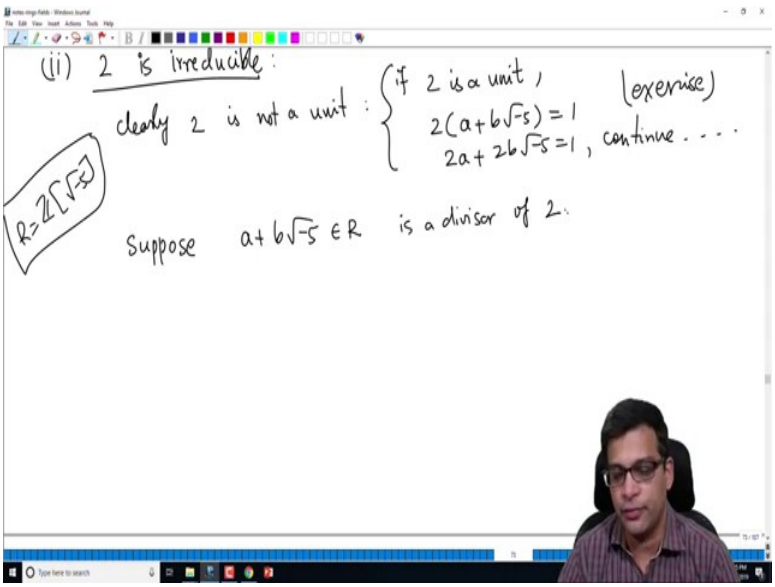


Because 2 divides the product of 1 plus root minus 5 and 1 minus root minus 5 which is actually 6, or 2 divides the product, but we argued that 2 does not divide either of them.

(Refer Slide Time: 02:06)



(Refer Slide Time: 02:18)



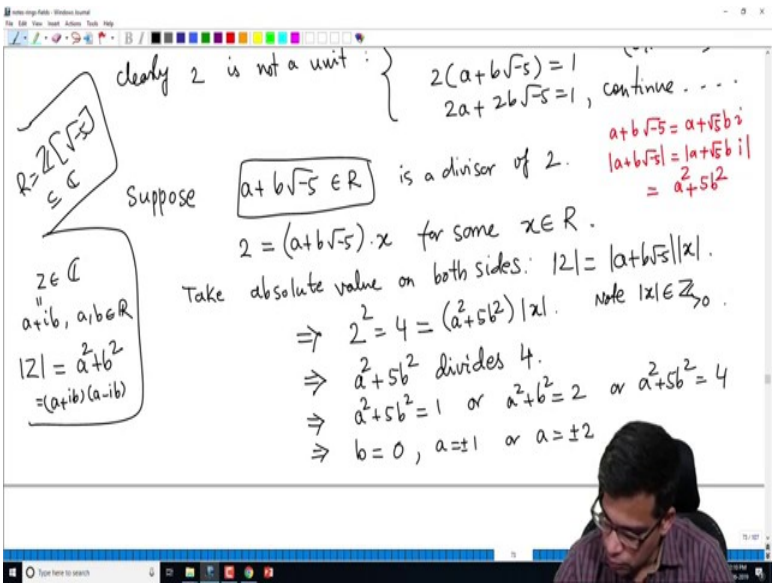
So, the second part that I will do now is that. So, let us continue now, 2 is actually irreducible. Once I show this, it will follow that in this ring we have an element which is not prime, but it is irreducible. So, if you recall the definition of an irreducible element, it should not be a unit and it should not have proper divisors. So, I will simply write clearly

2 has, 2 is not a unit, ok. This is actually very easy and I should leave this as an exercise for you to check the details.

But suppose, if 2 is a unit, what does this mean? Unit remember means, it has a multiplicative inverse. 2 times a plus b times root minus 5 will be equal to 1 by definition, because 1 is the multiplicative identity element, 2 is a unit means 2 times this is 1. But, if this happens you have 2 a plus 2 b and continue, ok, so you continue like this to get a contradiction. So, this is an exercise for you. It is a very simple exercise, but I will leave this for you to do.

So, now we need to show that it has no proper divisors. So, suppose there is a divisor because remember our ring is a R is Z adjoint square root minus 5. So, this is the ring that means, elements are of this form, where a and b are integers, is a divisor of, suppose this is a divisor of 2, if this is a divisor of 2 we would like to conclude after some work that it, it is in fact, a proper divisor. So, why is that?

(Refer Slide Time: 04:15)



So, now I am going to recall for you the notion of an absolute value. Remember if z is a complex number. Let us say z is a plus i b, where a and b are real numbers, right. So, any complex number can be written as a plus i b, where a and b are real numbers and i of course is a square root of minus 1. Then, I am going to use this notion of absolute value which is a squared plus b squared. In fact, it is the square root of this maybe, but I am going to use this, absolute value of z is a squared plus b squared.

So, now if a plus b times minus square root minus 5 is a divisor of 2 that means, by definition of a divisor in an arbitrary ring, 2 can be written as a plus b times root minus 5 times some other element in the ring. So, I do not need to, spell it out. So, let me just write this as x, by definition of a divisor I have this. And, remember all the numbers that we are considering in this ring are complex numbers. Of course, R is contained in complex numbers, right. So, we can take absolute value both sides, on both sides we get absolute value of 2 is a plus b times minus square root minus 5 times absolute value of x, right. This is my definition of absolute value.

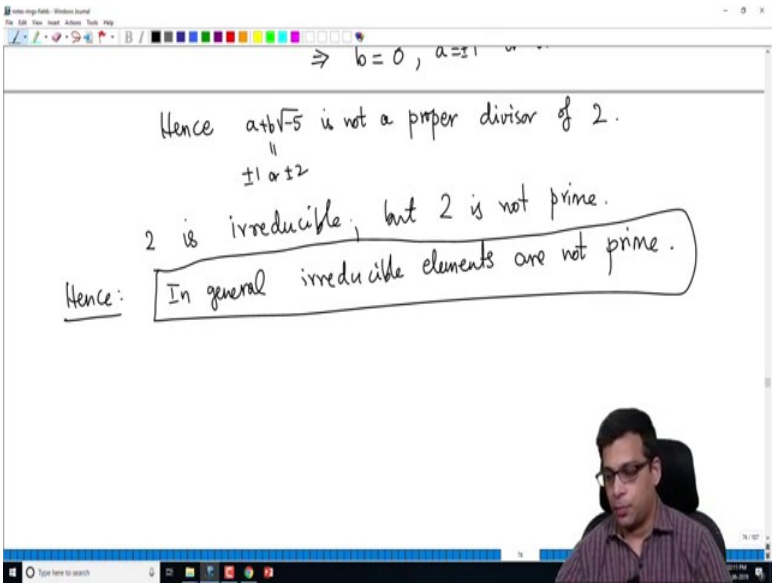
What this means. What is the absolute value of 2? This is actually 2 squared which is 4. And what is the absolute value of a plus b times square root minus 5? Remember I will write it here a plus b times square root minus 5. Let us convert it into a form like a plus i b, so this can be written as a plus square root b times i, right. It is a complex number where the real part is a imaginary part is square root b. So, absolute value will be, is the absolute value of a plus square root b i which is a squared plus 5 b squared, right, with the square the real parts to are the imaginary part and add them a square plus 5 b square. It is actually just a plus i b times a minus i b, that is what we have.

So, 2 squared is 4, these are 2 equal complex numbers that means, absolute values are equal. So, we have a square plus 5 b square times absolute value of x. I do not know what absolute value of x is, but remember absolute value of x will be also an integer in fact, a non-negative integer; because; positive integer even. Because x is of the form a, it will be of the form c plus square root 5s b i. So, if you take the absolute value it will be a c squared plus 5 b squared. So, it will be a positive real number as long as x is a positive integer as long as x is a nonzero element.

This means a squared plus 5 b squared divides 4. This means a squared plus 5 b squared divides 4. Now, we are in the realm of integers, right. You have an integer a squared plus y b squared which divides 4 that means, a squared plus 5 b squared must either be 1 or a squared plus b squared must be 2 or a squared plus 5 b squared must be 4. Remember a squared plus 5 b squared is a positive number, because a plus i, a and b are positive integers a and b are integers nonzero integers. So, a squared and b squared are actually positive integers; a squared plus 5 b squared must be a positive integer that divides 4.

Now, certainly this implies that there is only b has only one possibility because b must be 0, because as soon b is positive or b is negative, but nonzero b squared will be positive and 5 b squared will be at least 5. But a squared plus 5 b squared is 1, 2 or 4, so b has to be 0. And a immediately you see that a squared has to be 4, a squared has to be either 1 or 2 or 4, it cannot be 2. So, it has to be either 1 or 2. So, a is 1 or a is 2, ok. So that means, that or of course, it can be plus minus 1 minus 2. But I should write, but immediately you see that the divisor we started with, the arbitrary divisor that we started with a plus b times square root minus 5 is either plus 1 plus minus 1 or plus minus 2.

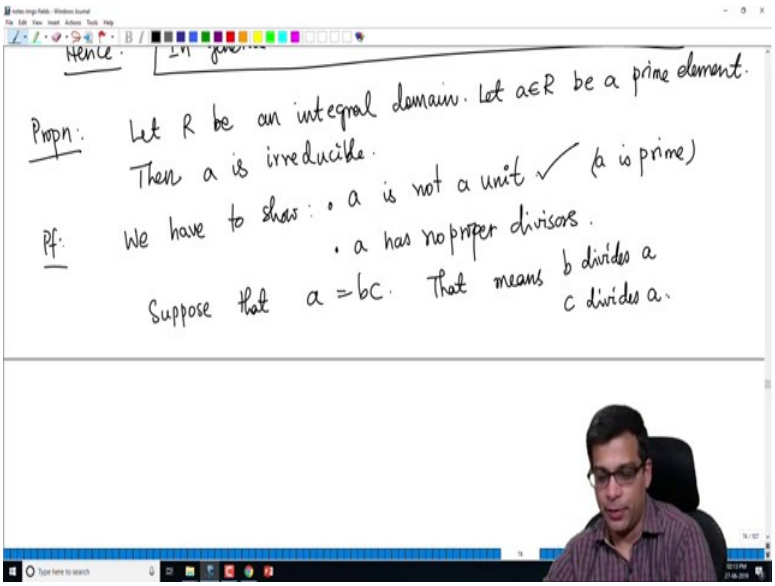
(Refer Slide Time: 09:27)



Hence, hence we conclude that a plus square root b times square root minus 5 is not a proper divisor. So, this is either 1 plus minus 1 or plus minus 2. So, it is not a proper divisor, right of 2, because a proper divisor is supposed to be something which is not a unit and which is not an associate. 1 and minus 1 are units, and 2 and plus minus plus minus 2 are associates of 2, hence 2 has no proper divisors and 2 is not a unit, so 2 is irreducible. But 2 is not prime.

So, this example I did only to illustrate the fact that in general irreducible elements are not prime. So, that is my goal. In general irreducible elements are not prime. So, this is an important fact to remember. In an integral domain irreducible elements can be there that are not prime.

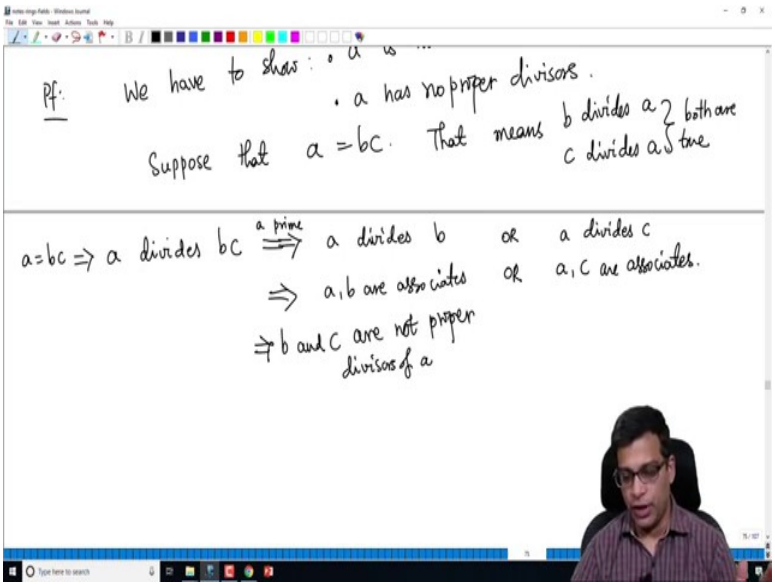
(Refer Slide Time: 10:39)



However, the converse is true. So, this is a proposition. Let me prove this. Let R be an integral domain, ok. Let R be an integral domain and let a in R be a prime element; then a is irreducible, ok. So, a prime element if you recall the definition I gave in the last video, a prime element is not a unit and if it divides a product bc, it divides one of them. So, it is not a unit. So, now, I want to show that it is irreducible. So, to show, we have to show two things, a is not a unit and a has no proper divisors, right.

So, to show these two facts, because these two parts give the definition of irreducibility; a is not a unit is because a is prime. Remember a prime element is automatically not a unit, so that is already given. So, we have to show that a has no proper divisors. So, suppose we have a is equal to bc. Suppose, we have such a thing; that means, in particular remember that means, b divides a and c divides a, because b times is a, b divides a, again b times is a, so c also divides a.

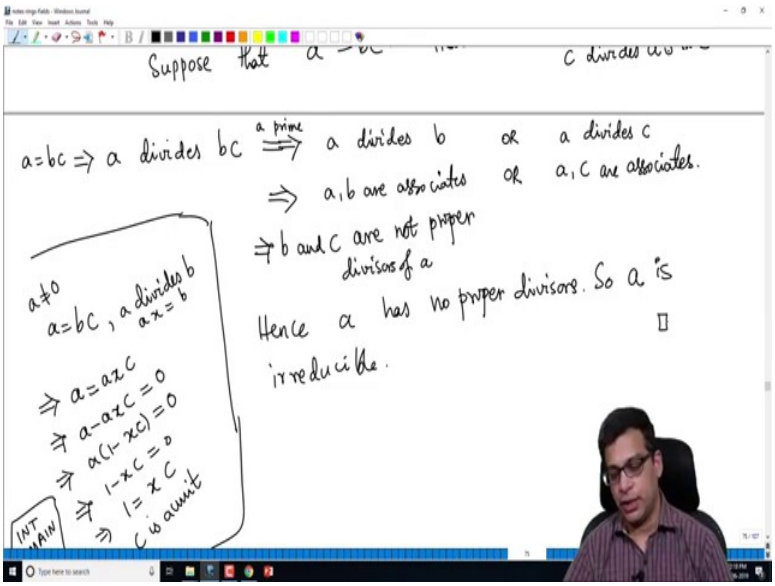
(Refer Slide Time: 12:36)



So, now let us use primality of a. We know that a divides bc, of course, a is equal to bc. So, a equal to bc implies a divides bc, an element divides itself. So, a divides bc, because a is prime; so, I will write it here, because of the primality of a, a divides b or a divides c, right. A prime element has the property that if it divides a product, it divides b, if it divides a product bc, it divides either b or c, but b remember divides a or c divides a. So, we have a divides b and b divides a. So, a and b are associates or if a divides c, c also divides a. Remember these both happen.

So, no matter here whether a divides b or a divides c, we can apply both these statements because b divides a and c divides a both are true. So, a and c are associates. So, a and b are associates and a and c are associates. Sorry a and b are associates or a and c are associates. But this means b is not a proper divisor of a, b and c are not proper divisors. Actually, I should say they are both not proper divisors because a proper divisor is one where both terms are not units and not associates, right.

(Refer Slide Time: 14:35)



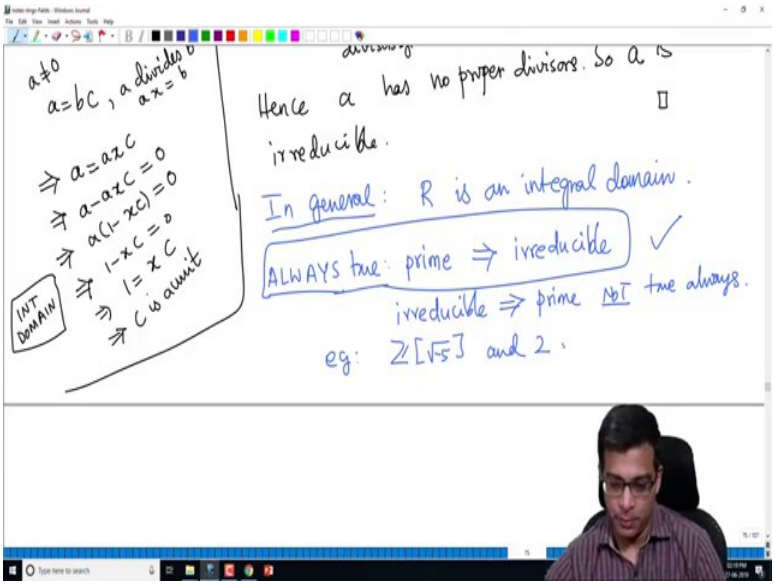
So, we cannot have, of course, if just to give you illustrate this; suppose a is equal to bc and b is an b and c are associates, b and a are associates; this means that we have a is equal to bc. On the other hand, b divides a also, a divides b also; so, this is b sorry. So, you have a is equal to bc is given, b also divides a. So, I am assuming a divides b, so, so I should write a divides b. So, I am just working out what happens if a divides b that means, ax is equal to b, right. a divides b means, there exists some x such that ax equal to b. So, if ax equal to b, I can replace this as ax c, b is equal to ax.

So, ax c, that means, a times 1 minus x is equal to c. I can just subtract both sides sorry, a this is not correct. What I should write is a minus axc is 0 that means, a times 1 minus xc is 0. And I am assuming a is nonzero, that goes without saying, right. If it is a 0 element then it is certainly prime and irreducible whatever you call it, it is just a convention, but a is not 0. Now, here is where integral domain is important. In all this subject of when we talk about irreducible and prime elements we are assuming that we are in an integral domain. So, if a times one minus x is 0, a is nonzero, so 1 minus x is 0 that means, c is a unit, right because 1 equals xc that means, c has a multiplicative inverse.

So, as long as you have a factorisation where one of them is actually an associate then the other must be a unit. So, this is not a proper factorization, and a has no proper divisors, hence a has no proper divisors, so a is irreducible. It is already not a unit because its

prime and we now concluded that it has no proper divisors. So, it is an irreducible element.

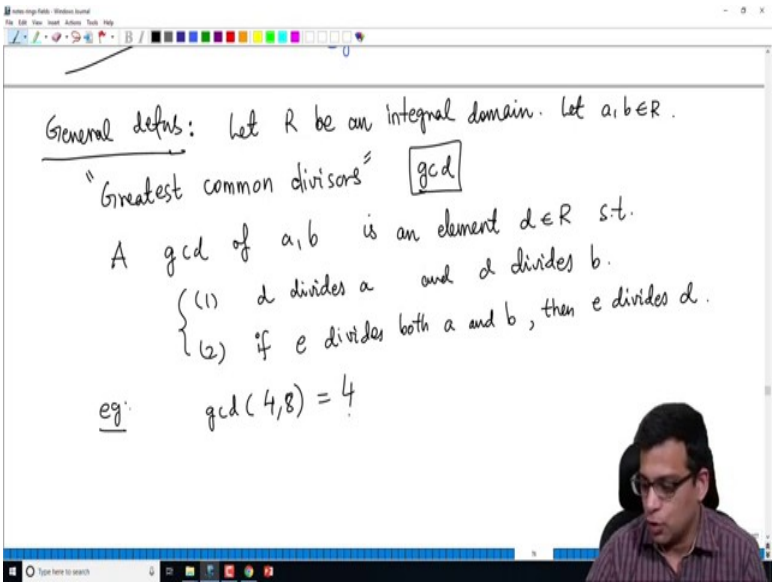
(Refer Slide Time: 17:15)



So, just to recap the general picture for you, I will write in general regarding prime and irreducible elements, R is an integral domain, R is an integral domain. Always, the following is true: prime implies irreducible. This is always true as we showed just now in this proof. The converse, so this is always true. Irreducible implies prime, not always true. As remember the example of Z adjoint square root minus 5 and 2. So, in this ring 2 is irreducible, but 2 is not prime. So, this is the general description of irreducible and prime elements in a arbitrary integral domain.

So, in the remaining video and in the next video or so, we are going to study rings where actually the converse is true. So, the topic that we are currently discussing is the notion of principal ideal domains, and unique factorisation domain. So, before I continue and define principal ideal domains, let me quickly give you some general definitions.

(Refer Slide Time: 18:46)



General definitions are the following. So, let R be an integral domain. Let R be an integral domain, and let us choose two elements a and b in R. Let us choose two elements. I talk about I want to talk about greatest common divisor. So, this is short form is gcd that you all are familiar from high school, right we know about gcd, LCM and so on. So, I want to carry over the notion that we have in integers namely gcd to an arbitrary integral domain.

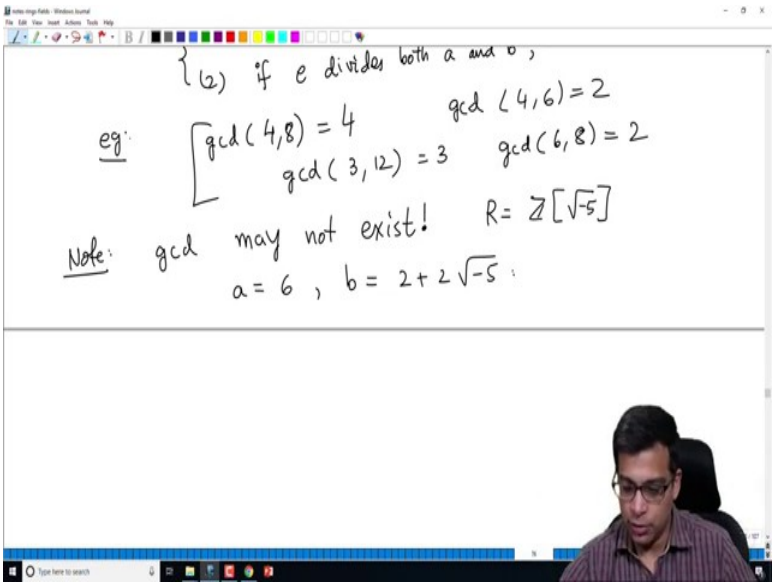
So, what is gcd? So, let us formally define that. I want to now talk about a gcd of a, b. So, because there could be many more, there could be more than one I mean. So, always we will say a gcd because even in integers if you follow the definition of that I will give now. gcd, if 3 is gcd of 2 numbers minus 3 is also gcd. So, I want to define a gcd of a and b is an element d in R such that it has two properties. So, first of all just like in the integer case, I want d to divide a and d to divide b, ok. So, I want d to divide a and d to divide b. It is a common divisor. So, this is a common divisor part, it divides a and it divides b. But it is greatest common divisor. So, it is not enough to be a common divisor.

And how do you phrase the greatest common divisor, the greatest part? In integers we have the notion of being big or small, in an arbitrary integral domain there is no order we cannot say one element is bigger than another element, but we are now going to use this following notion which also holds in the case of integers. If e divides both a and b, so if there is some other common divisor. So, d is the common divisor and if there is some

other common divisor then that common divisor divides d. So, this is the greatest part, first is the common divisor part second is the greatest part. So, e divides a and b implies e is a common divisor then e divides d. So, a greatest common divisor is a common divisor which is divisible by every common divisor.

So, the standard examples remember are for example, we check gcd of 4 and 8 then of course, it is 4.

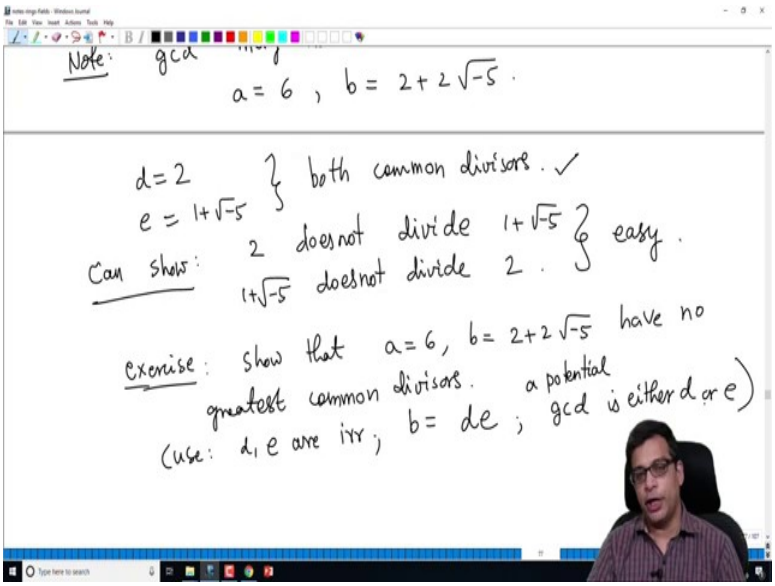
(Refer Slide Time: 21:42)



Gcd of 4 and 6 will be 2, gcd of 3 and let us say 12 is 3, gcd of 6 and 8 will be 2 and so on, ok. So, this is all something that you are familiar with. We look at all numbers that divide both of them and we take the largest one in the case of integers, but because there is no largest or smallest elements in arbitrary rings, we are going to stick to this definition where we want the common divisor to be divisible by every other common divisor.

So, I want to stress that gcd may not exist, gcd may not exist and that is because, again the ring that we used earlier which gave us an example of an irreducible element that is not prime, in this same ring we can take the following. So, let us take a to be 6, and b to be 2 plus 2 times square root minus 5. So, these are the two elements I will take, so a is this, b is this.

(Refer Slide Time: 22:58)



So, now let us take d to be 2 and e to be 1 plus square root minus 5, these are both common divisors, ok. So, one can show that both are common divisor that is because 2 certainly divides 6, 2 times 3, 6, 2 also divides this 2 times 1 plus square root minus 5 is 6. So, this is easy. Similarly, e divides 6 because 1 plus square root minus 5 and 1 times 1 minus square root minus 5 is 6. So, 1 plus square root minus 5 divides 6 it certainly divides b, so because 2 times this is there b.

On the other hand, we know that, this requires a little bit work can show 2 does not divide 1 plus. In fact, this is not to show because if divides you write 2 times 2 as, 2 times something equals 1 plus square root minus 5 and you use your standard arguments that we have used earlier in this video to get a contradiction. 2 does not divide this similarly this also does not divide 2. So, you have these two things. So, this is easy actually, this is not that difficult. This is a standard calculation.

So, you have two common divisors, one does not divide the other, ok. So, now, in fact, you can show that there is no gcd because 2 is irreducible. So, you now; I will leave this as an exercise show that a which is 6 and b which is 2 plus have no greatest common divisor, that is because you can show that d and e are irreducible. So, they will not; so, and b is actually d times e, right, because b which is 2 plus 2 times square root minus 5 is d times e. So, any common divisor must be, so gcd is either d or e. gcd, if a potential gcd I should write, a potential gcd is either d or e because b has only 2 divisors really. So, it is

either d or e, and we just showed that d does not divide e, e does not divide d. So, there cannot be a common device. There are common divisors, but there cannot be a greatest common divisor in this sense. We do not have a common divisor which is divisible by every other divisor, ok.

So, I am going to stop this video here. In this video, we looked at more examples of, more properties of irreducible and prime elements. We have given an example to show that irreducible does not mean prime, but prime always implies irreducible and we have defined the notion of gcd in an arbitrary integral domain. In the next video, we will start studying principal ideal domains and unique factorization domains.

Thank you.