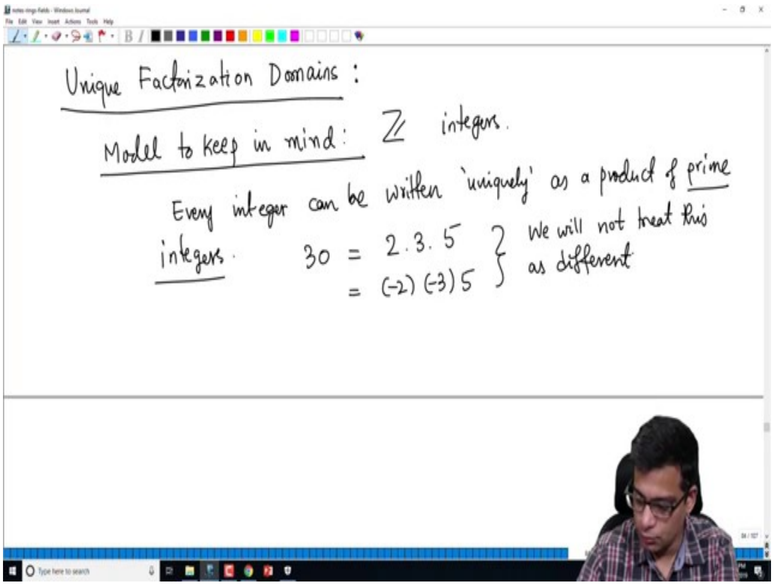
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 26
Unique Factorization Domains 1

In the last video I defined and studied principal ideal domains, we are special classes of rings where very nice property holds that every ideal is principal. So, in this video we are going to study a more important class in some sense of rings and more general class certainly it includes PIDs, is this notion of Unique Factorization Domains.

(Refer Slide Time: 00:38).



So, these are nice rings which cover most of the interesting examples that we have studied in this course and which this property that we want to define is very important. Principal ideal domains are also very nice, but the property is too special many nice rings do not have that property. For example, the ring Z x is perfectly good ring, but it is not a principal ideal domain.

But it is a unique factorization domain as we will prove in this course, so unique factorization domains are an important class of rings. So, as the name suggests we are going to ask for the following property, we want every element to have a factorization into irreducible elements and that factorization should have should be unique essentially unique, I will define what unique means.

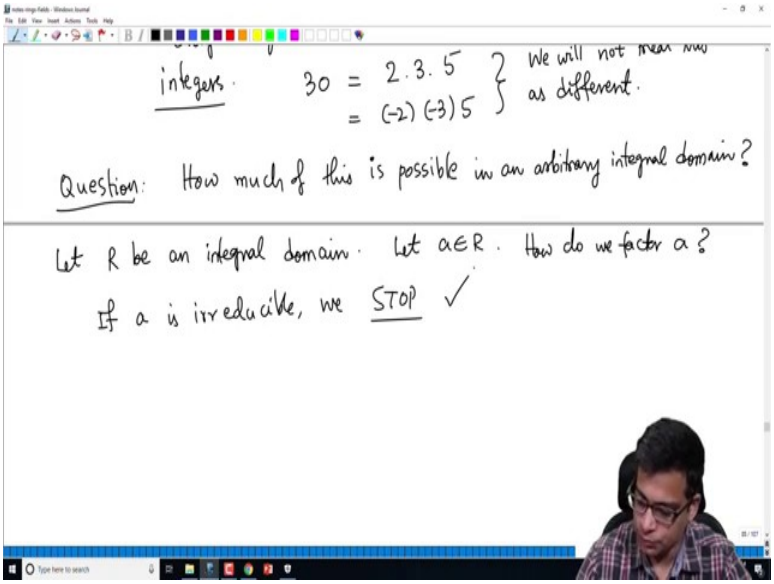
But the model to keep in mind is the following is the model that you are familiar with is the ring of integers and in school you all learned that every integer can be factored into a product of prime numbers. Prime numbers are irreducible elements in the integers, because in the set of in the ring of integers irreducible and prime are really the same notions.

So, model to keep in mind, in the ring of integers, we can say that every integer can be written essentially uniquely I will say why I will put this in quotes and say essentially can be written uniquely as a product of prime integers. So, I am going to call them prime integers now, because in an arbitrary ring also we are going to talk about prime elements. So, prime integer is actually a prime integer the way we have learned it in school right. For example, 30 can be written as 2 times 3 times 5, but it is not quite unique because I can also write it as minus 3 minus 2 times minus 3 times 5.

And, now I am going from the notion of prime integers that we have learned in school which in under which notion a prime number is has to be a positive number. But in the more general notion of prime elements in an arbitrary integral domain Z is an integral domain, so there is no reason to exclude negative numbers. So, minus 2 is also a prime element so and hence it is an irreducible element so we can write it like this.

So, I am not going to we will not read this as different right, because the way that we will not read this as different is we will consider 2 and minus 2. Appearance of 2 and minus 2 is the same, that means whether 2 comes or minus 2 comes we are not going to make a difference, because they are associates that is the crucial statement there. So now, this is the model as I said to keep in mind; we want to see whether this can be carried over to arbitrary integral domains. Can we now say that any element in that ring can be factored like this and if possible uniquely ok?

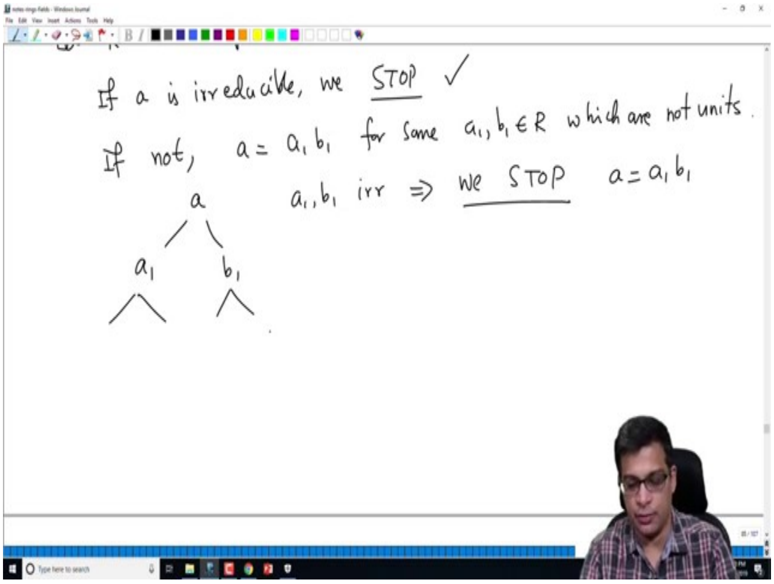
(Refer Slide Time: 04:16)



So, the question is what we have learned in school is that in integers you can do this, question is: how much of this is possible in an arbitrary integral domain? So, if you go to an arbitrary integral domain how much of this is possible? So, first of all we want to factor. So, how do we go about factoring? So, let R be an arbitrary integral domain. So, we will put some conditions later and define unique factorization domains, but let us start with an arbitrary integral domain and let us take an element R (Refer Time: 04:16) element a.

So, how do we factor a how do we factor a? So, this is what we do. So, we if how do we factor a into a product of irreducibles? If a is irreducible, we stop. So, it is sort of an algorithm, so if a is irreducible we stop there is nothing to do a is its own irreducible factorization. For example, the number of five in the ring of integers is irreducible, so you do not do any more work you stop.

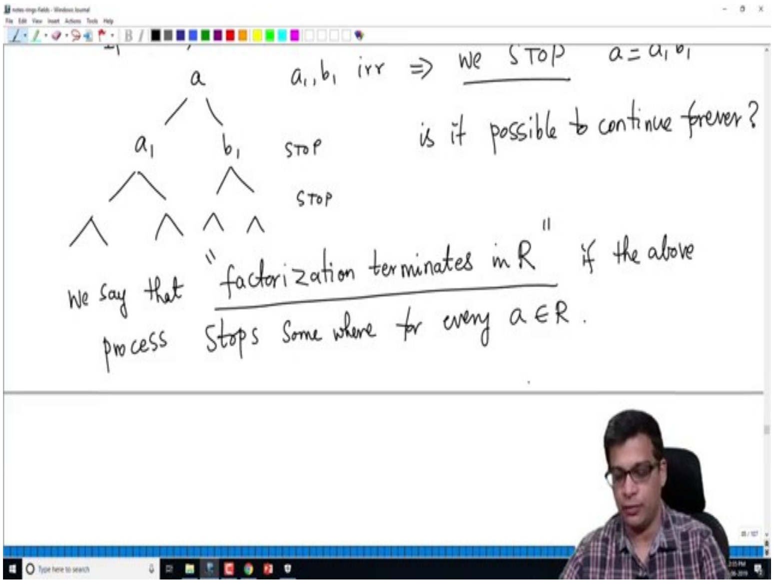
(Refer Slide Time: 05:46)



So, if a is irreducible we stop if a is not irreducible by definition a can be written as a 1 b 1 for some a1, b1 in R which are not units right which are both not units. Because, if a is not irreducible we know that there is a proper divisor, if a1 is a proper divisor we can find another proper divisor b1 such that a is a times a1 b 1.

So, we have gone from a1 a 2 a1 b1 if a is irreducible we stop otherwise we find two other elements a 1 b 1. If a 1 is irreducible we stop here and if b1 is also irreducible we stop and that is the irreducible factorization. If both are irreducible we stop with the factorization given by a1 b1. If either of them is not irreducible we continue right, a 1 factors properly as a product of two non-units b 1 factors properly as a product of non-units and we look at those four elements. If they are all irreducible we stop here or so we may stop at any stage.

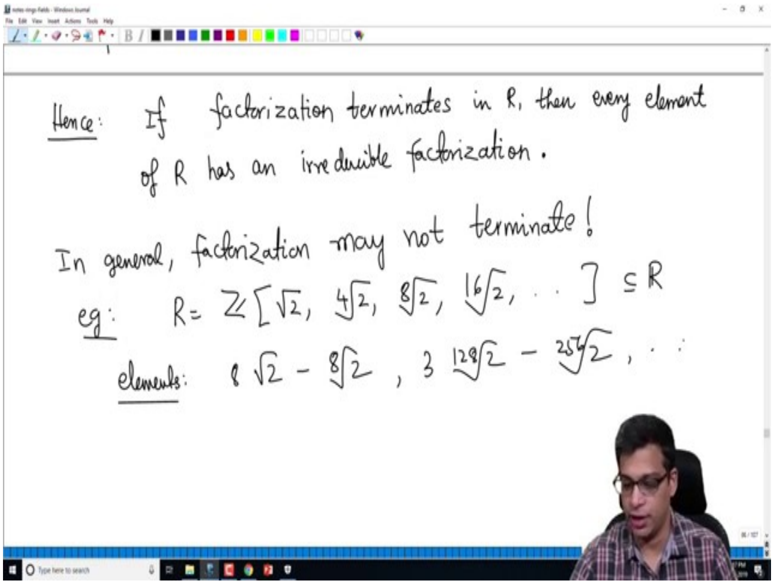
(Refer Slide Time: 07:09)



If at any stage we have all irreducible elements we stop and thereby we achieve our irreducible factorization, otherwise we will continue right and potentially we may have to continue forever. So, we say that factorization, so the question is can we continue? Is it possible to continue forever. So, that will not be good right, if you have to continue forever, that means there is no factorization for a because you cannot only if you stop somewhere we achieve a factorization of a.

So, we say that factorization terminates in R we say that factorization terminates in R, if the above process stops or terminates somewhere for every a in R. So, if it stops for every a we start with some if it is irreducible we stop, if not we factor it. If the two factors are irreducible we stop if not we continue we factor those two and then keep continuing suppose it stops somewhere for every element in the ring then we say that factorization terminates in R, so that is a phrase. So, it is a property of a ring.

(Refer Slide Time: 08:50)



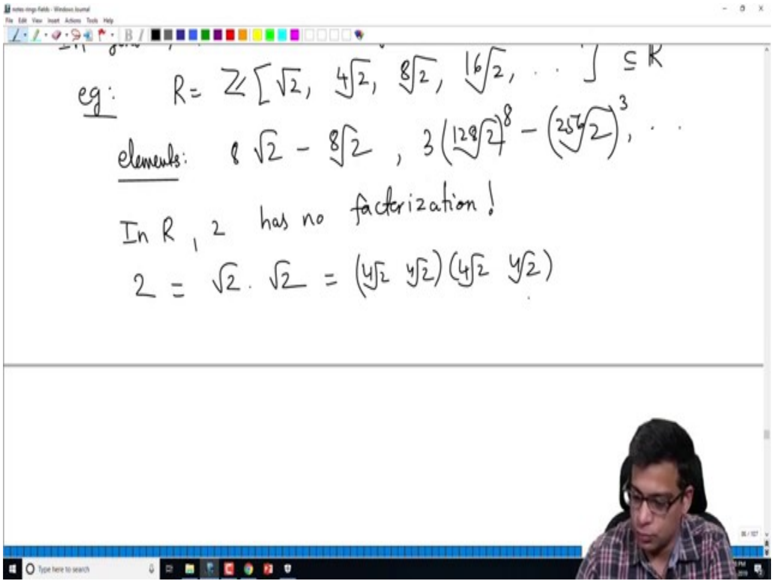
So, the statement is hence the conclusion is if factorization terminates in R, then every element of R has an irreducible factorization ok. So, this is clear right, if factorization terminates in R and you are given an arbitrary element of a arbitrary element a of R we continue the process we described in the previous page. If it is irreducible we stop if not we factor it, if the two factors are irreducible we stop if not we continue factoring them and eventually it stops.

Because I am assuming that factorization terminates in R that is a phrase, that that phrase represent says that for every element this process stops. Obviously, then every element has a irreducible factorization. We are not yet coming to uniqueness I am currently only interested in establishing when factorization actually exists. So, it exists when factorization terminates, I should right away warn you that in general factorization may not terminate as the following example shows.

In general, factorization may not terminate. So, the above process I described may never stop as an example let us look at the following ring. Let us look at the ring given by Z adjoined square root 2, 4th root of 2, 8th root of 2, 16th root of 2 and so on ok. So, this is actually a subring of the real numbers, where I am adding square root of 2 4th root of 2 8th root of 2 and so on. So, any element of this ring is a finite sum of some integer times an element some 2 power n th root of 2 plus another element times 2 power n 1th root and 2th root of 2 and so on. So, elements are like this.

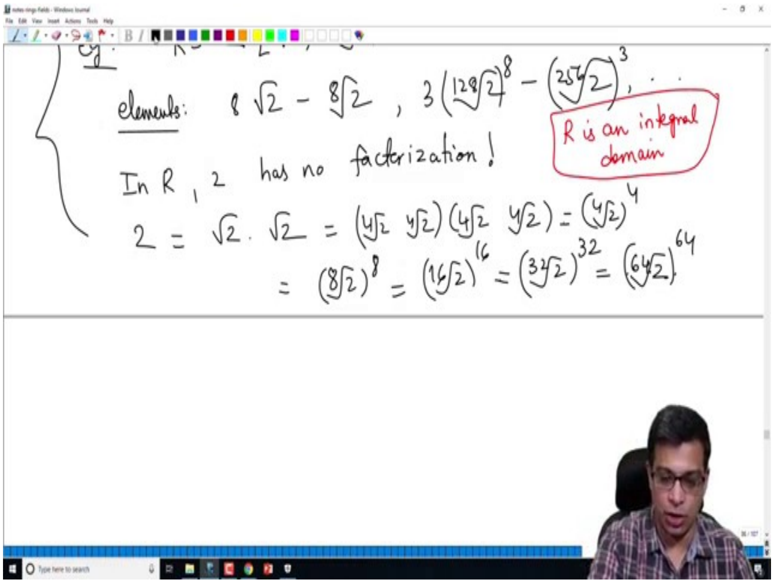
For example this is an element ok. So, it can also be some 124 128 rather root of 2 some 3 times this minus 256 root of 2 and so on right. So, this is a ring.

(Refer Slide Time: 11:27)



Any such combination you take in fact I can take squares any powers and it will be an element of this. So, these are elements, I claim that in this ring in R, 2 has no factorization, because let us follow the algorithm that I described earlier. So, 2 is not irreducible because it is a product of square root 2 and square root 2 right neither of them is a unit. But, square root 2 is also not an irreducible element because, it is fourth root of 2 times 4th root of 2 and then also 4th root of 2 4th root of 2. So, basically what I am saying is that you can continue this right.

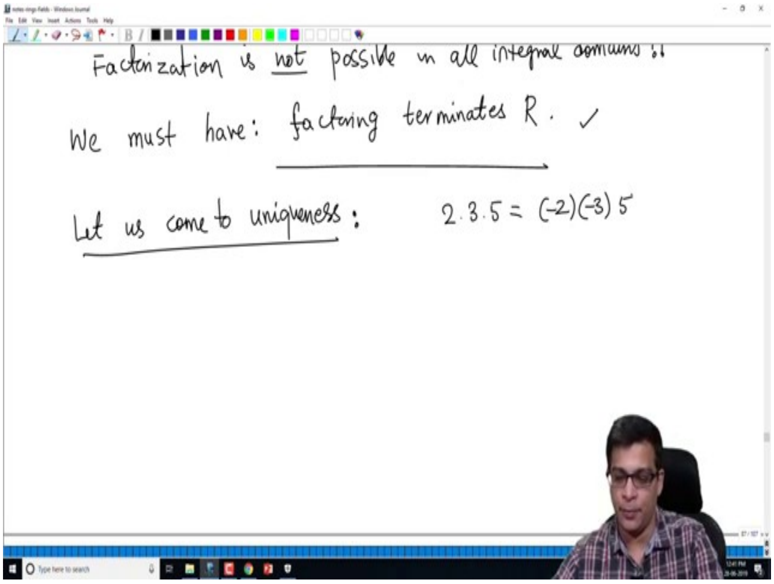
(Refer Slide Time: 12:16)



This is 4th root of 2 power 4, but I can also do 8th root of 2 power 8 16th root of 2 power 16 32 th root of 2 power 32, where do you stop there is nowhere you can stop 2 has no finite factorization. You cannot say this is a factorization because 32nd root of 2 is not an irreducible element, it actually further becomes 64th root of 2 squared that is 32 square root 32 30 second square root of 2 is 64th square root of 2 square.

So, you can keep doing this at any stage, you do not have a factorization, so you have to keep going. So, this is a strange ring of course, it will not happen in most common rings and I will tell you for example, it does not happen in Noetherian rings as we will see later. So, immediately we conclude that there is no hope of doing factorization in any integral domain. So, this is certainly an integral domain right, R is an integral domain because it is a subring of the real numbers. So, certainly in factorization is not possible.

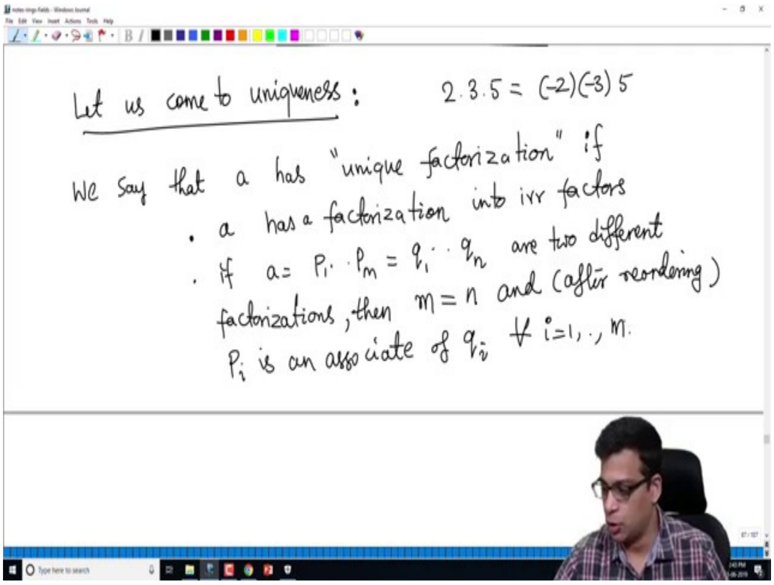
(Refer Slide Time: 13:31)



Leave alone unique factorization, factorization itself is not possible in all integral domains; it is too bad right. We are hoping that maybe the what happens for the integers can be carried forward for every integral domain, but that s not the case, as this example shows. So, we have to ask for so we must have the property that factorization factoring or factorization terminates in R right. So, this we have to ask it may not be true for every integral domain as this example shows.

So, we have to ask for as a special property of R, so this must happen. So, this is a special condition, but now let us come to uniqueness. Let us come to uniqueness ok. So now, remember uniqueness on the nose is not true even for integers because, the factorization 2 3 5 and factorization minus 2 minus 3 5 should be considered really same, though the exact elements that appear there are not same. So, what is the notion of uniqueness that I want to define?

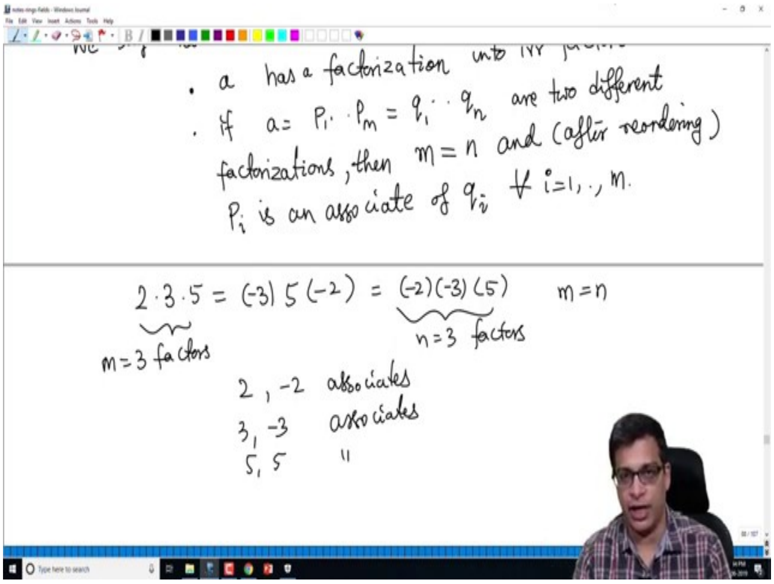
(Refer Slide Time: 15:00)



So, we say that a has unique factorization, if a small element a. So, I want a small element I say element small a has unique factorization if the following happens, given any two. So, first of all if a has first of all a has factorization into irreducible that must be happening into irreducible factors, otherwise the if there is no factorization there is no point talking about uniqueness of factorization.

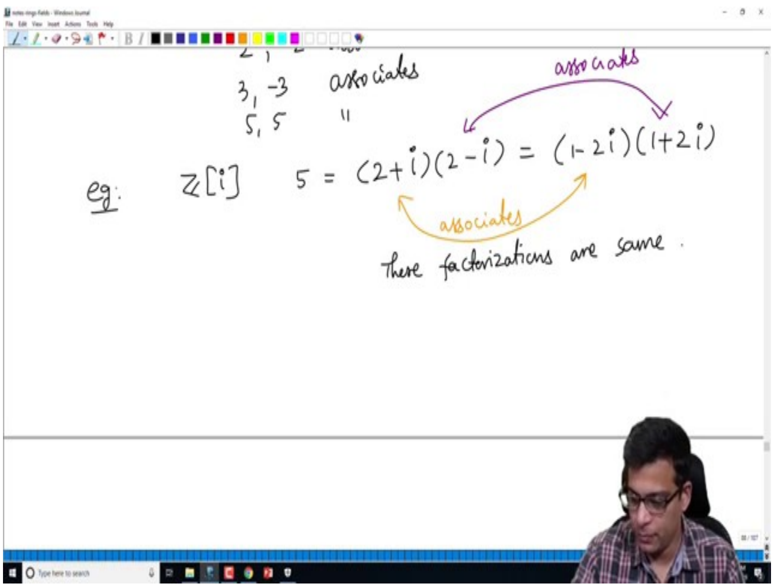
So, first of all it has a factorization and if we have two different factorizations p 1 through p m is equal to q 1 through q n are two different factorizations. Whenever I say factorization I mean factorization to irreducible factors, that means p 1 through p m q 1 through q n are both are all irreducible elements. Then we must have m equal to n and after reordering if needed p i is an associate of q i for all i from 1 to m. So, one m and n are same to begin with and after reordering because we have to reorder possibly.

(Refer Slide Time: 16:47)



See 2 3 5 is same as minus 3 5 minus 2 right. So, unless you reorder you cannot say 2 and minus 3 are associates. So, we reorder one of them then there are three factors here that is m and there are also three factors here. So, m and n are equal and after having re-arranged 2 minus 2 are associates, of course in the ring of integers they are associates 3 minus 3 are associates. And of course 5 and 5 are associates because they are actually equal elements. So, this is exactly what we mean by unique factorization, not quite that elements are equal but elements are associates.

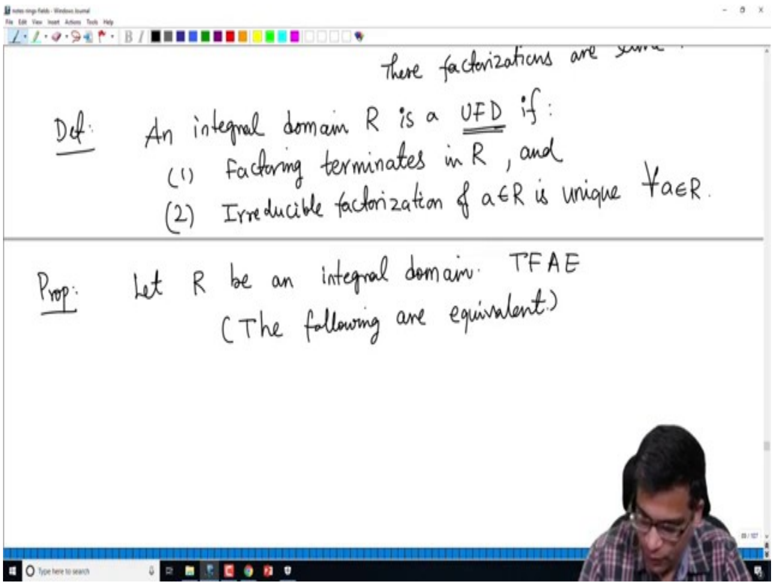
(Refer Slide Time: 17:40)



Another example I will write Z i which I told you as a fact last time that it is a PID. In fact, it will turn out to be UFD also after we prove that every PID is a UFD, but in this ring we have 2 plus i times 2 minus i is 5 because 4 plus 1, but this is also equal to 1 plus 2 i or rather I will write maybe 1 minus 2 i and 1 plus 2i ok.

So, these two are associates, because you multiply this by i or minus i you get this and these two are associates. You multiply this by i you get i squared minus i squared is 1 2 i. So, this is also unique, these factorizations are unique or rather or for all practical purposes they are considered same, so these factorizations are same.

(Refer Slide Time: 18:51)



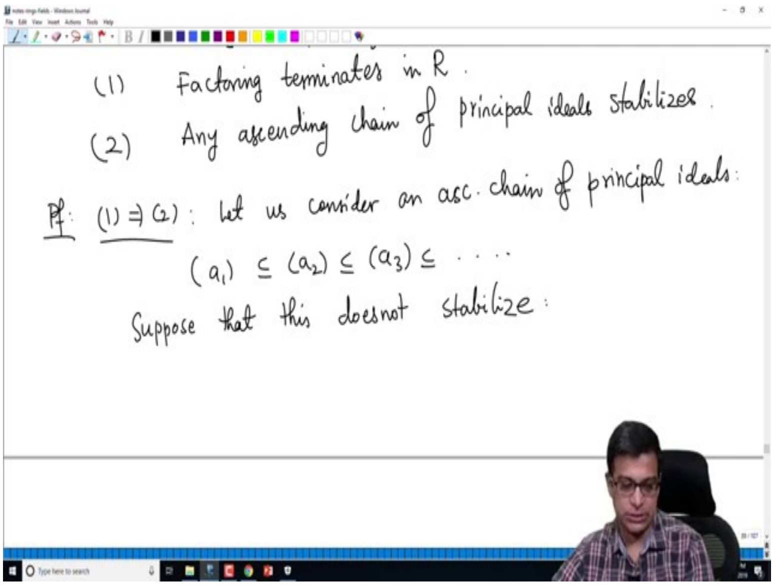
So, now I am ready to define the main definition of this video an integral domain R is a UFD, I will use the short abbreviation UFD for unique factorization domain. So, it has two properties, of course it has two properties it is a two words right it is an three words really unique factorization domain. So, it has to be an integral domain that is why the factorization must exist. So, factoring terminates in R this must happen.

So, that every element has a factorization into irreducible factorizations of any element is unique for all a in R. So, unique in the sense of this, so I say that they are unique if the number of irreducible must be equal and after reordering if needed. The first one is an associate of the first one second one is an associate of the second one and so on. So, this second property is a uniqueness first property is a factoring in the hypotheses that it is a domain takes care of D.

So, unique factorization domain is one which is an integral domain where factoring terminates and because of the first property every element has a unique irreducible factorization. But irreducible factorization must be unique ok. So now, in this rest of this video and in the future videos we are going to study properties of unique factorization domains.

So, let me prove a proposition to get control of the first property, see factoring seems factoring terminating seems a difficult condition to check. So, I want to do a proposition to simplify that process, let R be an integral domain then the following are equivalent. So, this is a standard notation for TFAE, it means the following are equivalent, TFAE the following are equivalent.

(Refer Slide Time: 21:17)

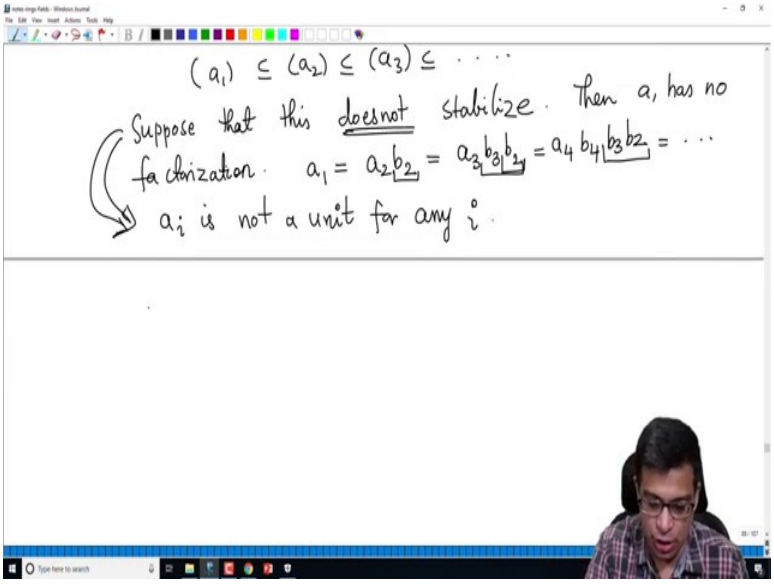


So, what are the two statements that I want to make here factoring terminates in R, factoring terminates in R which is what we are interested in finding out and the second condition is that any ascending chain of ideals not just any ideals. In fact, I want any ascending chain of principal ideals stabilizes. So, this notation should remind you of the video when we were talking about Noetherian rings, recall that a Noetherian ring is a ring where every ascending chain of ideals stabilizes, we did not put the word principal there. So, this is a weaker condition any ascending chain of principal ideal stabilizes.

So, in particular a Noetherian ring will have the second property hence it will have the first property. So, in any Noetherian ring factorization terminates. So let us prove this. So, I will prove this is very simple, so let us prove 1 implies 2. Suppose factoring terminates in R and let us take an ascending chain of primes, principal ideals rather. Let us consider a1 contained in a 2 contained in a 3 and so on. So, I am trying to show that assuming one I want to show that any ascending chain of principal ideals stabilizes.

Suppose not suppose you have an ascending chain of principal ideals which does not stabilize.

(Refer Slide Time: 23:20)

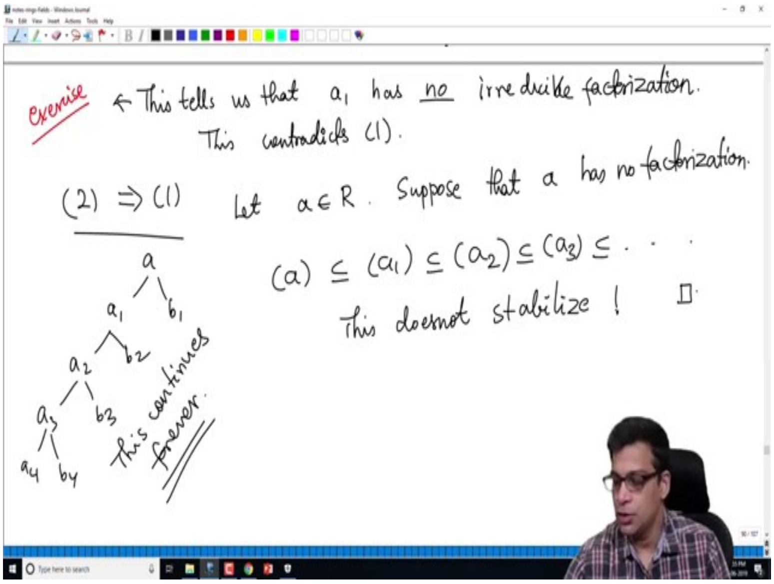


So, then we will show that then a1 has no factorization, that is because which violates then that factor terminates, because if this continues like this what we have is a1 can be written as a 2 times b 2 right. The fact that a1 is contained in this means a1 is in the ideal generated by a 2; that means, a 2 times b 2 for some b 2. So, a1 can be written as a 2 b 2, but a 2 is in the ideal generated by a 3 which means we have a 3 b 3 b 2.

So, I am retaining b 2 as it is, but a 2 can be written as a 3 times b 3 and remember if this chain does not stabilize this statement here implies a i is not a unit for any i right. If a i is unit for some i, that means the ideal generated by a i would be the unit ideal. But unit ideal will be equal to R. So, beyond that everything is unit ideal that means the chain has stabilized, stabilizing means after some finite stage they are all equal.

So, if a hundred is a unit the ideal generated by a hundred is R, that means a1 hundred and one is also R a1 hundred and two is also R. So, beyond hundredth stage everything is R, but then the chain has stabilized which we are assuming as not happened it does not stabilize. So, it is not a unit that means, these are all proper factorizations. So, you can continue now a 4 b 4 b 3 b 2. So, I have carried over b 3 b 2 and written a 3 as a product of a 4 b 4 and then it keeps going.

(Refer Slide Time: 25:26)



So, it is a simple exercise now to show that this tells us that. See a i's and b i's may not be irreducible, but if a 1 has an irreducible factorization you cannot keep forever factoring like this, a 1 has no proper factorization sorry a1 has no irreducible factorization. If there is a chain of principal ideals which does not stabilize the first one or any one of those cannot have a factorization this contradicts 1. So, it must be the case that 1 implies 2 if factoring terminates is given an ascending chain of principal ideals must stabilize. So, let us prove 2 implies 1.

So, this little thing I will leave as an exercise for you, to convince yourself that if a1 has an irreducible factorization you cannot possibly keep forever factoring a1. Now let us prove 2 implies 1, so now I am assuming 2 I am assuming that there is a given any chain of principal ideals it stabilizes. So, let small a be any arbitrary element, I want to show that the algorithm that I defined at the beginning of this video terminates. How, recall what was the algorithm if a is irreducible a has a factorization.

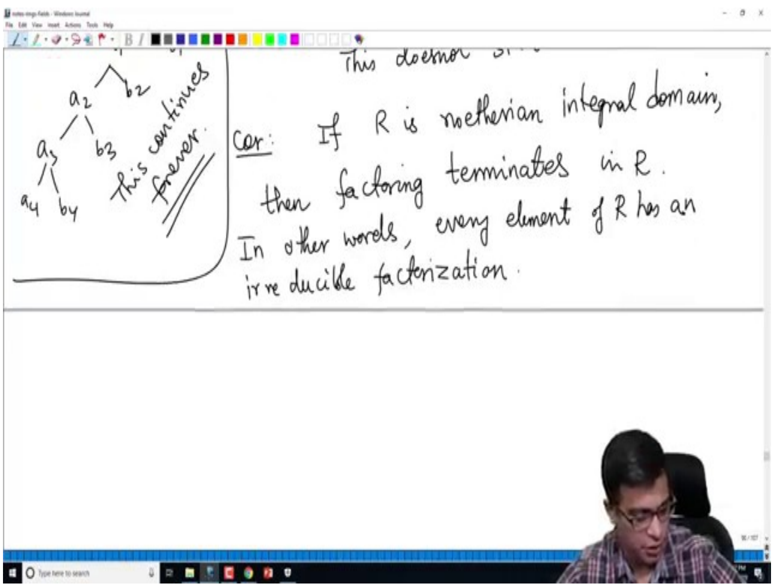
So, suppose so actually I am going to assume that 1 is false and get a contradiction. Suppose that a has no factorization, I am trying to show one right I am assuming two and I am trying to show one which is that factoring terminates in R, which is another way of saying that every element of R has a factorization. Suppose that there is an element of a R called a which has no factorization. That means, we could have factored a as a1 b1 and we would then factor a1 as a 2 b 2 a 2 as a 3 b 3 if a 3 as a 4 b 4 and so on right, this must continue forever.

This algorithm continues forever, that is the meaning of a having no factorization. But that means, the ideal generated by a is in the ideal generated by a1 right because a is a1 b1 ideal generated by a1 is in the ideal generated by a 2, because a1 is a 2 b 2, similarly the ideal generated by a 2 is in the ideal generated by a 3 and this continues forever, this does not stabilize. That is the meaning of our algorithm does not stopping anywhere that means this does not stabilize, because at each stage we have a proper factorization.

So, for example, the ideal generated by a four is strictly bigger than ideal generated by a 3. If it was not a 3 and a 4 would be associates, so b 4 would be a unit and you would have stopped. So, somewhere actually I should be more careful somewhere in this tree we have an infinite chain, maybe it stops here but b 3 we factor it is does not stop there. So, wherever it does not stop if you trace through that path we get an infinite chain of principal ideals which does not stabilize.

So, this is not quite correct because it maybe that this stops, but somewhere else it does not stop. But does not matter I can assume without (Refer Time: 29:09) of generality that this does not stop. So, this does not stabilize so 2 implies 1.

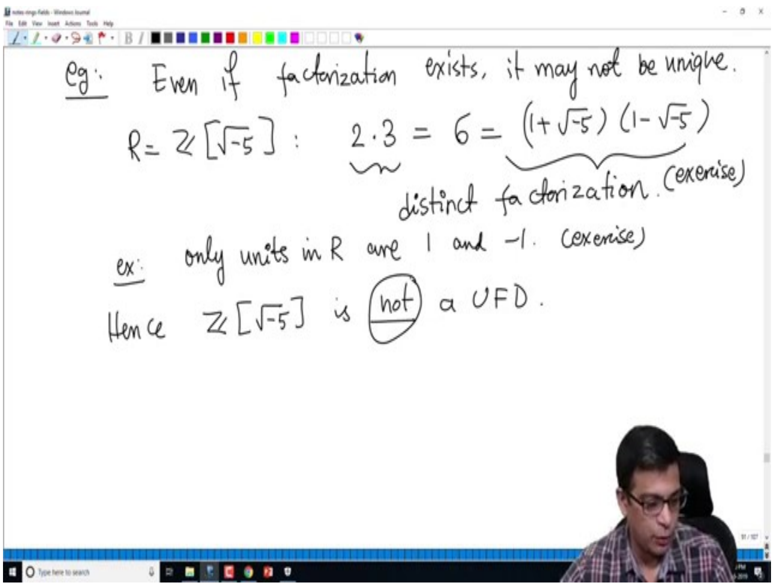
(Refer Slide Time: 29:17)



So, the advantage of this proposition is that we have we are able to conclude: if R is a Noetherian integral domain, then in a Noetherian integral domain then factoring terminates in R right. So, in other words every element of R has an irreducible, ok. So, Noetherianness is too strong a property, because in Noetherian rings every ascending chain of ideals stabilizes.

Whereas, for factoring to terminate we only need that every ascending chain of principal ideals to stabilize. But still if you have a Noetherian ring we can be sure that factorization terminates and hence every element has a irreducible factorization. It is not going to imply that irreducible factorization is unique, but at least you are guaranteed that factorization terminates. So, that every element has a factorization.

(Refer Slide Time: 30:48)



So, now I will end this video by giving an example even if factorization exists it may not be unique ok. It may not be unique because as the example our favourite example this is something that we have considered before R I will take Z adjoined square root minus 5. This is providing us all the examples that we are interested in right. It gave us an example of an irreducible element which is not prime, it gave us an example of it was going to give us an example of something which where unique, factorization is not unique. So, and this is something we have seen before.

So what I will leave for you is to show that these are distinct, they are actually not same as I defined earlier. When do we call two factorizations same, the number of irreducible factors that appear are same is equal and up to reordering they are associates of each other. So, what you have to do is 2 and 3 are irreducible, 1 plus square root minus 5 and 1 minus square root minus 5 are irreducible. So, these are both irreducible factorizations, but 2 is not an associate of either of them this is something that came up earlier and this can be proved by proving this fact only units in R are 1 and minus 1.

So, there are no other units, so if two and either of these elements are associates. For example, 2 and 1 plus root minus 5 is associates 1 plus root minus 5 will be 2 times a unit. But this says that only units are 1 and minus 1, but 2 times 1 is 1 2 times minus 1 is minus 2, neither of them is equal to 1 plus root minus 5. So, this is the exercise that I want you to do and I want to also prove that 2 and 2 is irreducible. We have proved using the same argument prove that 3 is irreducible and similar argument tells you that 1 plus root minus 5 and 1 minus root minus 5 are irreducible, so these are distinct irreducible factorizations.

So, this is not unique and hence this ring is not a UFD right, though actually turns out that this is a Noetherian ring. So, it is in this ring factorization terminates. So, every element has a factorization into irreducible elements. However, as this example shows this is not a UFD. So, this is an important example which provides various counter examples to things. So, what I want to do next in this video we have learned what UFD s are these are rings, where factorization exist and is unique and we have proved that in a Noetherian ring factorization exists.

But it may not be unique, but factorization exists and in even more bad rings like Z adjoined roots of 2, 2 power nth roots of 2, even factorization does not exist. And in a nicer ring like Z adjoined square root of minus 5, factorization exists but it is not unique. In the remaining, next few videos we are going to look at more examples of UFDs, in particular we will prove that a PID is a UFD. So, that gives us a collection of nice examples of UFDs and we will prove that there are some rings which are not PIDs, but which are UFDs, so that is for the next video.

Thank you.