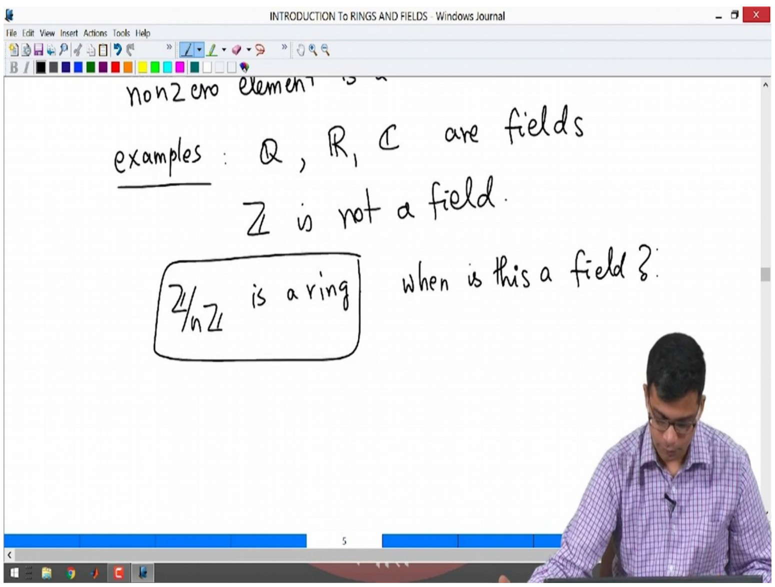
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 03
More examples

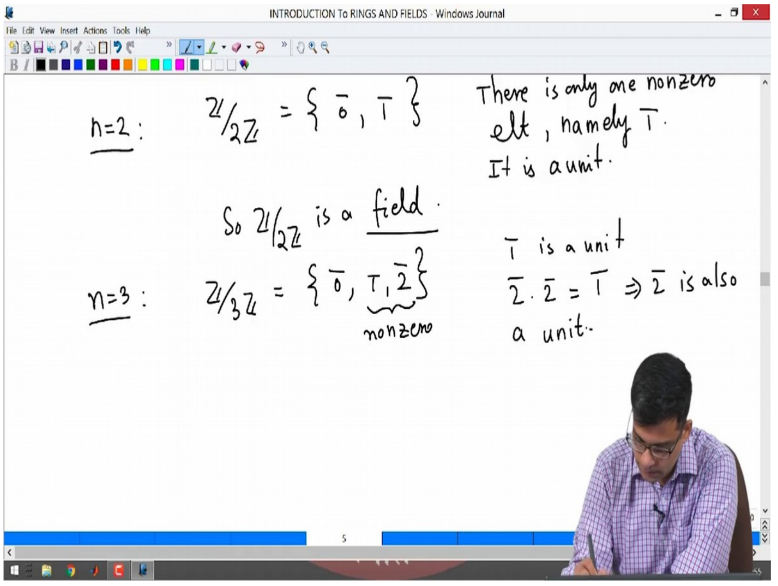
(Refer Slide Time: 00:17)



So, in the last video we looked at units in a ring, we talked about fields and I said Q, R, C are fields and Z is not a field. So, I want to give couple of examples of more examples of fields. So, remember in the last example last video, we looked at the ring Z mod n Z right. So, the construction of the set is exactly that we had in the case of groups. So, you had the group of integers under addition the subgroup n Z.

So, you take the quotient group. So, that is your underlying group on which we have multiply defined multiplication and we noticed that, it becomes a ring under that multiplication and addition. So, the question is when is this field? So, when is this a field?

(Refer Slide Time: 01:17)



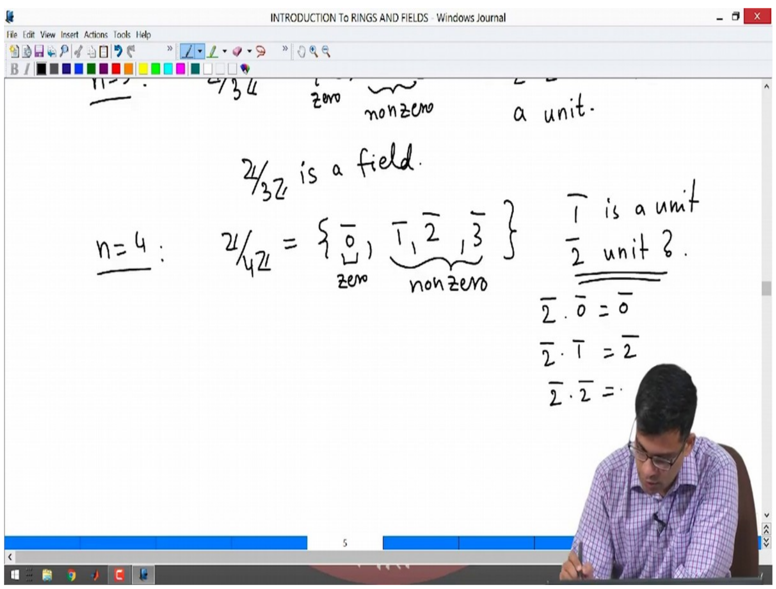
So, for example, let us take let us so, I will start with n equal to 2, because n equal to 1 is not interesting, because you get the 0 ring; 0 ring is not a field by convention you have you in a because you need multiplicative group. So, non-units every non-zero element is a unit, but you want then at least 1 non-zero unit.

So, take n is n is at least 2. So, we assume n is at least 2. So, let us first start with n equal to 2. So, what is Z mod 2 Z? So, we have 2 elements 0 bar and 1 bar and in order to be a field non-zero elements must be units. So, there is only 1 non-zero element right, only 1 non-zero element namely 1 bar.

So, and is it a unit? Of course, it is because 1 bar is anyway unit. 1 is a unit in any non-zero ring and it is a unit right, 1 bar times 1 bar is 1 bar, so, it is a unit. So, Z mod 2 Z is a field right, because every non-zero element is a unit. What about n equal to 3? Z mod 3 Z, let us take this.

So, and this has 3 elements, 0 bar 1 bar and 2 bar, there are two non-zero elements these are non-zero, 1 bar and 2 bar and we know 1 bar is a unit, because 1 bar is always a unit being the multiplicative identity. 2 bar times 2 bar if you remember the multiplication table that I wrote last time 2 bar times 2 bar is 1. Directly you can say 2 bar times 2 bar is first multiply 2 and 2 and take the residue. So, it is 4 bar which is 1 bar. So, this implies 2 bar is also a unit right.

(Refer Slide Time: 03:32)

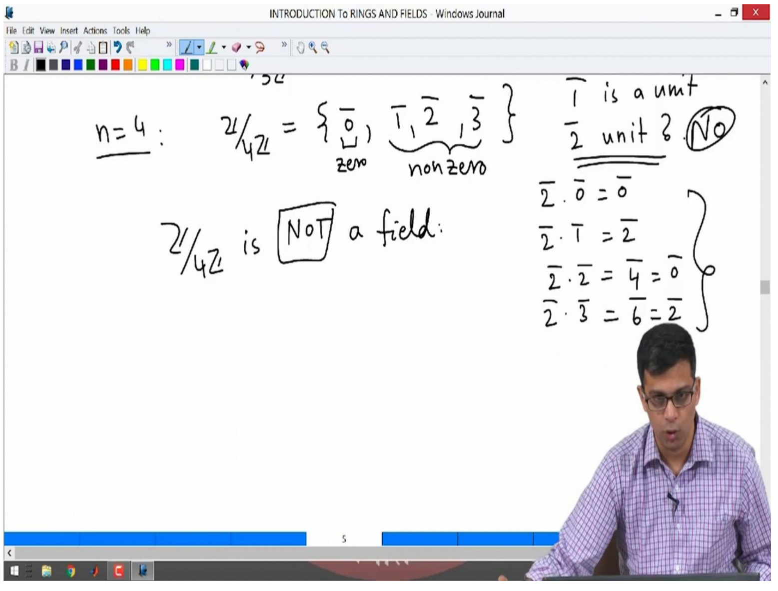


So, Z mod 3 Z is also a field, because it has 2 non-zero elements and both are units. So, when I say non-zero elements in a ring, if you remember in the previous video I said a field is a ring where every non-zero element is a unit. Non-zero element by definition is any element that is not equal to the additive identity.

It is our convention to remember, it is our convention to call the multiplicative identity is 0, sorry additive identity is 0 and multiplicative identity 1. So, non-zero means not equal to additive identity so, in Z mod 3 Z additive identity is 0 and multiplicative additive identity is 0. So, non-zero elements are 1 bar and 2 bar ok. So, and both are units, so, it is a field.

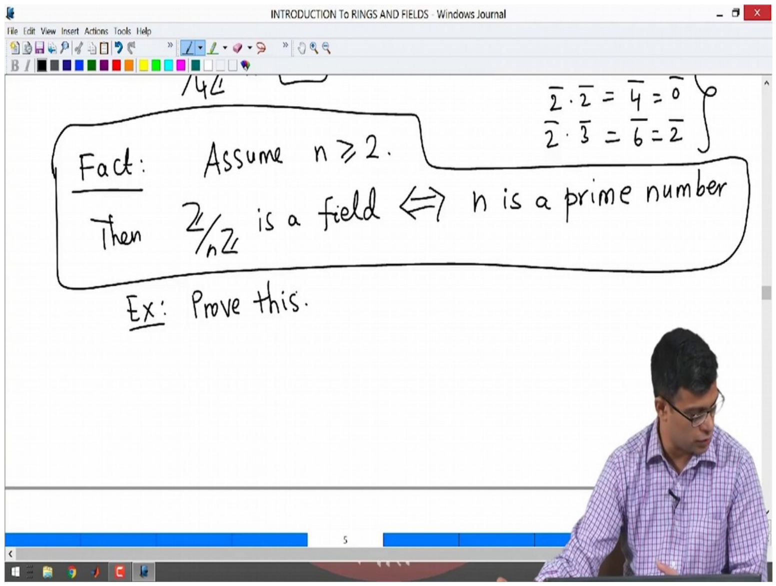
Let us look at n equal to 4. So, what is Z mod 4 Z. So, Z mod 4 Z has 4 elements, 0 bar, 1 bar, 2 bar, 3 bar. So, this is the zero element these are the non-zero elements. You have to check one by one whether all of them are units or not 1 bar all of them are units or not. 1 bar is a unit that is because it is the multiplicative identity. Is 2 bar a unit? Let us check. So, let us they have only 4 elements. So, let us check 1 by 1 if you have multiply them with any of them do you get 1 bar.

(Refer Slide Time: 05:20)



So, 2 bar times 0 bar is 0 bar, 2 bar times 1 bar is 2 bar, 2 bar times 2 bar is 4 bar, which in this case is 0 bar 2 bar times 3 bar is so, remember this is 4 bar which is 0 bar, this is 6 bar this is 0 bar. So, none of them is 1 bar. So, this is not a unit. So, 2 bar is not a unit; that means, Z mod 4 Z is not a field right. So, there is a non-zero element which does not which is not a unit. So, 2 bar is a non-zero element in Z mod 4 Z and it is not a unit. So, in this ring there do exist elements which are non-zero yet do not have multiplicative inverses.

(Refer Slide Time: 06:05)

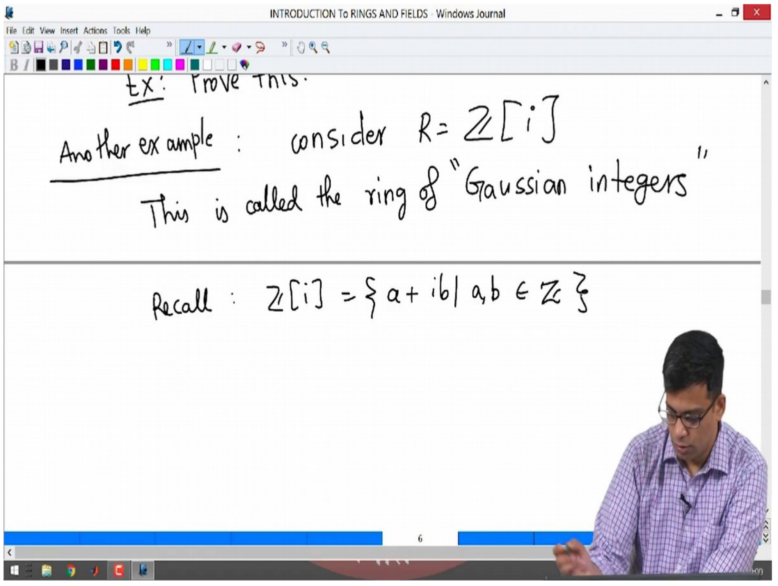


So, they are not, it is not a field ok. So, now you might see a pattern here. I will write a fact here and you can I will tell you how to check this and ask you to complete the proof. So, Z mod n Z so, assume n is at least 2, then Z mod n Z is a field if and only if n is a prime number ok. So, this is the fact. In fact, this is an exercise, prove this.

So, I will leave the proof completely to you for now, in a later video I will maybe quickly tell you how to prove this. So, it is a good exercise for you to get used to working with rings. So, I have done three examples 2 3 4 2 5 and 6 7 are few more examples and try to identify I told you what the fact is.

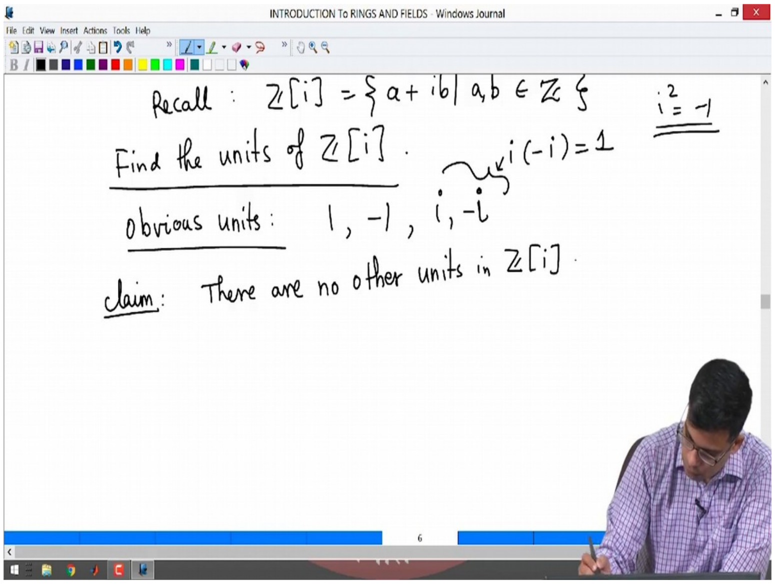
So, you should now be looking for places where prime number plays a role 2, 3 are prime numbers, 4 is not a prime number. And in fact, if 4 is not a prime number, 2 is a divisor and 2 bar happened to be not a unit ok. So, that gives you some idea of where to look. So, I want you to do this on your own and this will give you some comfort level with working with rings. I want to do one more quick example again to tell you how to work with rings and that also allows me to check if that ring is a field or not.

(Refer Slide Time: 07:53)



So, another example so, consider the ring Z i. So, this ring is called ring of Gaussian integers. So, this is an important ring in ring theory, it is called the ring of Gaussian integers. Remember this is, I told what this is earlier, Z i is the set of elements. So, it is a subring of complex numbers, where you look at elements of the form a plus i b where a and b are integers.

(Refer Slide Time: 08:47)

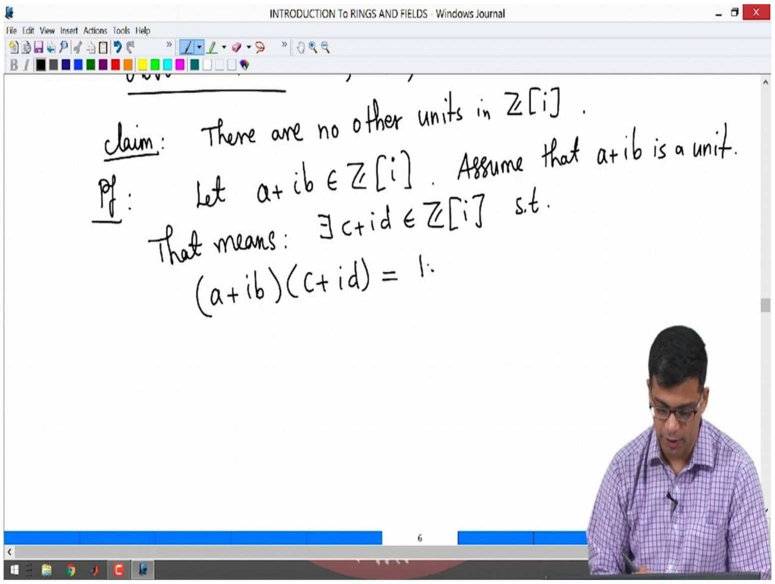


So, what are the units of? So, here find the units of, that is the problem that I want to do now. So, you get used to working with rings find the units of Z i. So, there are some obvious units so, obvious units. So, let me write them first. So, you may want to pause this and pause the video now and think for few minutes about what are the obvious units?

So, if you want you can think about it and come back to the video. What are the obvious units? There is 1 definitely 1 is a unit, in any non-zero ring 1 is a unit we agreed. As soon as 1 is a unit minus 1 is also unit, because minus 1 exist because there is an additive inverse of 1 we call that minus 1, minus 1 is it is own inverse multiplicative inverse. So, it is unit, there is another obvious unit. There are two other obvious units in fact.

I claim i is a unit. Why is i a unit? Because, if you do i times minus i, remember i squared is minus 1 right. So, i times minus i is 1. Similarly, minus i is a unit, i times minus i is 1; that means, i has a multiplicative inverse it also means minus i has a multiplicative inverse. So, i and minus i are definitely units. So, my claim now is I want to prove this claim now, there are no other units the ring Z i.

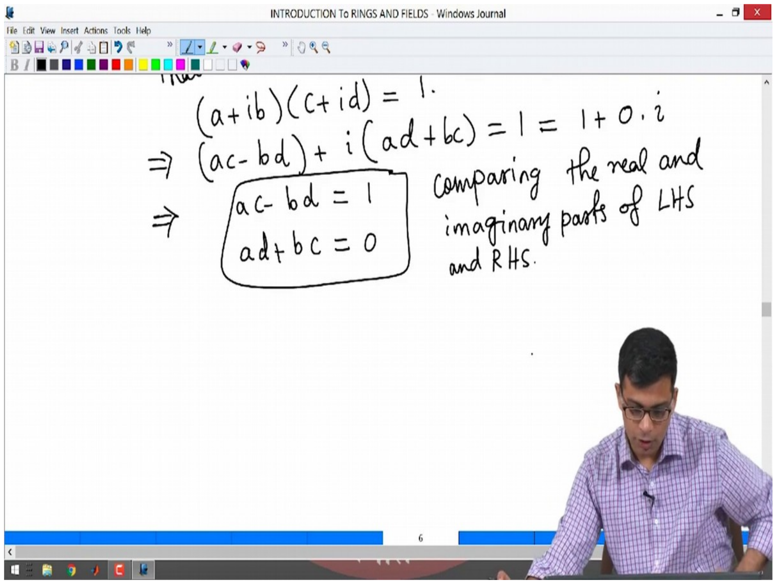
(Refer Slide Time: 10:43)



The ring of Gaussian integers has exactly 4 units there are no other units. So, what is the proof of claim? So, in any such proof you have to start with an arbitrary element of Z i assume that it is a unit and try to derive a contradiction. So, let a plus ib be an element of Z i. So, in other words let it be a Gaussian integer, assume that a plus ib is a unit ok.

So, suppose that it is a unit; that means, there exists c plus id, also in Z i such that a plus ib times c plus id is 1 right, this is exactly the definition of being a unit. So, unit is an element in a ring which admits a multiplicative identity.

(Refer Slide Time: 11:43)

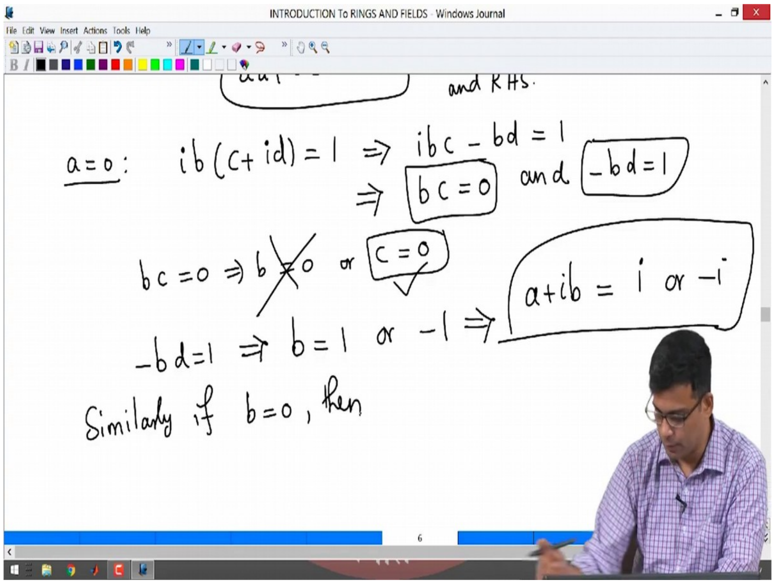


Suppose a plus ib is a unit that means, it has an identity multiplicative inverse call it c plus d plus id. So, a plus ib times c plus id is a plus ib times c plus id is 1. Now, expanding this out we get ac minus bd time plus i times a d plus bc equals 1, right. Because, i squared is minus 1 I get this.

Now, you have a complex equality of two complex numbers; that means, their real parts and their imaginary parts agree. What is the real part and imaginary part of the right hand side? 1 is a real number. So, real part is 1 imaginary part is 0. Real part on the left hand side is ac minus bd. So, we get ac minus bd is 1, the imaginary part on the left hand side is ad plus bc.

But, the imaginary part on the right hand side is 0, so, we get this. So, this is by comparing the real and imaginary parts of LHS the left hand side and RHS, we get this ok. So, now, let me first quickly get rid of the cases trivial cases. So, suppose a is 0.

(Refer Slide Time: 13:07)



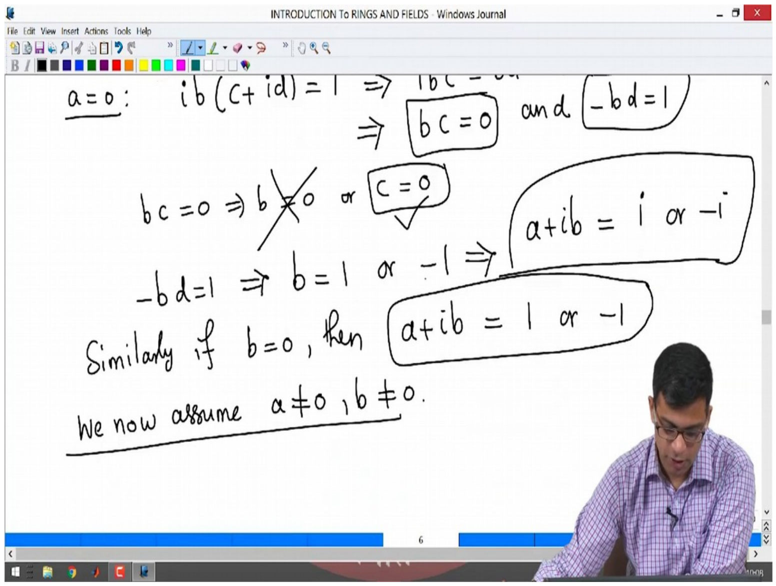
So, a plus ib is the number I am starting with suppose a is 0; that means, ib is a unit right. So, i b times c plus id is 1. So, ib times c plus id is 1; that means, we have ibc minus bd is 1, ok. I am just simplifying these equations in the box right. So, this implies bc is 0, correct and this is the second equation a is 0. So, bc is 0 and minus bd is 1. So, we get two equations. This is exactly these equations in the special case that a is 0, but bc is 0 implies b 0 or c 0.

But, can b be 0? a is already 0 under assumption. If b is 0; that means, a plus ib is also 0, but; that means, a plus ib is the 0 element, but the 0 element cannot be a unit. So, b cannot be 0; that means c is 0. So, what we have is and bd is also. So, actually this must happen and also bd is minus 1; that means, actually we do not need c is 0, but anyway I wrote that.

Let us use this: minus bd is 1 this implies see b and d are integers right bd is 1 means b is 1 or minus 1. If, you have two integers multiplied to 1 those integers must be either 1 or minus 1; that means, a plus ib which was our original remember unit is either i or minus i which we already considered.

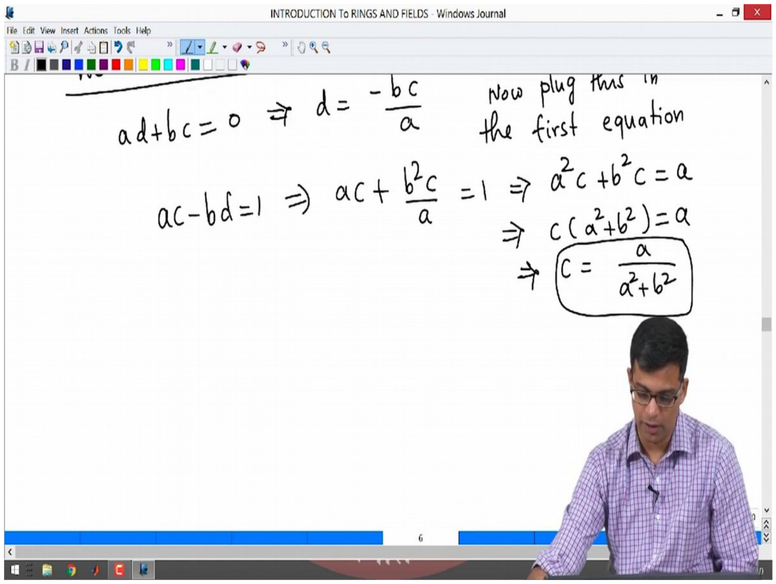
So, remember i and minus i we already know are units. So, if a is 0; that means, you have just unit of the form ib b is either i or 1 or minus 1. So, a plus ib is 1 or minus i. Similarly, if b is 0 then; that means, in the original unit that we started with a i b a plus ib, if b is 0; that means, we are looking at a unit ia; that means, it is an integer by itself.

(Refer Slide Time: 15:51)



Then a plus ib is 1 or minus 1 right, because b is 0 a is a unit that makes it must be 1 or minus 1. So, we now assume a is non-zero, b is non-zero. And we basically we will say that there is a contradiction, there cannot be any there cannot be any unit with a and b both non-zero and how do you do this? Let us look at our two equations ad plus bc equal to 0 let us use the second equation.

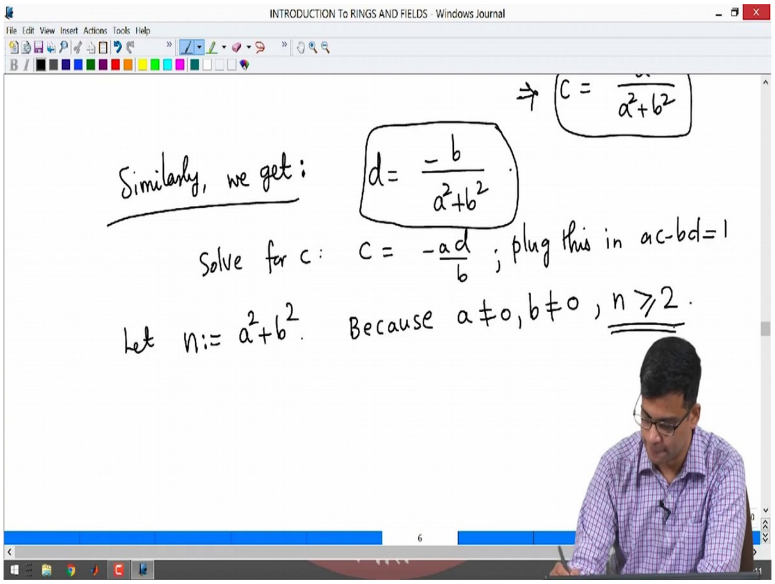
(Refer Slide Time: 16:27)



So, we have ad plus bc equal to 0; that means, d is equal to minus b c by a. So, note that a is non-zero. So, I can divide by a, so, d is minus bc by a. Now, substitute this or plug this in the first equation. So, first equation was; first equation was ac minus bd is 1. So, that is the first equation. So, let us plug that in. So, we have ac minus bd is 1 plug that value of d here. So, you will get ac minus minus bc by a times b, so, ac plus b squared c by a equals 1 right.

So, this means a squared c plus b squared c is equal to a; that means, c times a squared plus b squared is a; that means, c is a by a squared plus b squared. So, this is a simple calculation. If you have any questions you should just pause and check this on your own, it is a very simple direct calculation right.

(Refer Slide Time: 17:55)

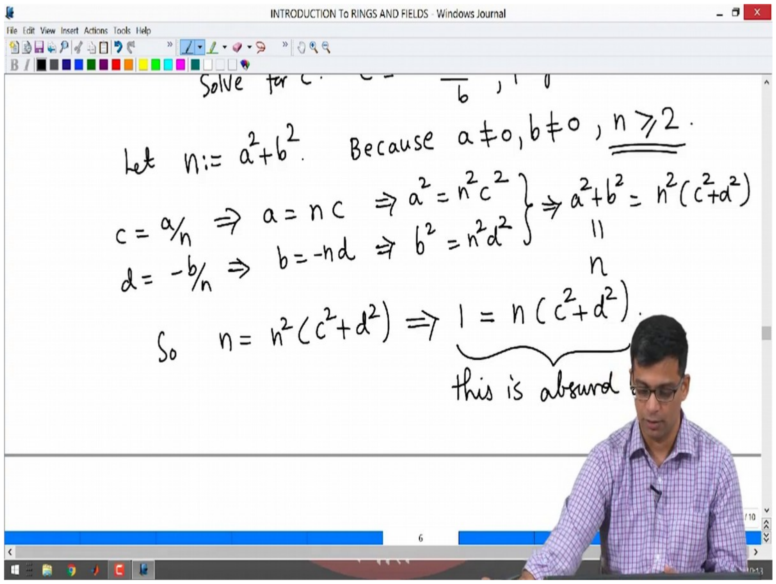


So, c is equal to a by a squared plus b squared. So, we get similarly so, this I will leave for you, we get I have that here d equals minus b by a squared plus b squared. See this is because we start with ad plus bc is equal to 0, but instead of solving for d like we did here, we solve for c; we solve for c and so, I will just start the process and you will finish it.

So, c equals minus ad by b plug this in ac minus bd equal to 1, plug this in ac minus bd equal to 1 and do a similar calculation that I have done here to get this equation d equals minus b by a square plus b squared. So now, I am going to simplify instead of writing a square plus b square I will call it n. So, let us define n to be a squared plus b squared.

Because, remember a and b are non-zero numbers and they are both integers right. So, and their squares are positive numbers I claim that n is at least 2, because a is not 0; that means, a squared is a at least 1. So, a is at least 1 or a is less than or equal to minus 1. In either case a squared is at least 1 similarly b squared is at least 1. So, their sum is at least 2 so, n is at least 2.

(Refer Slide Time: 19:35)

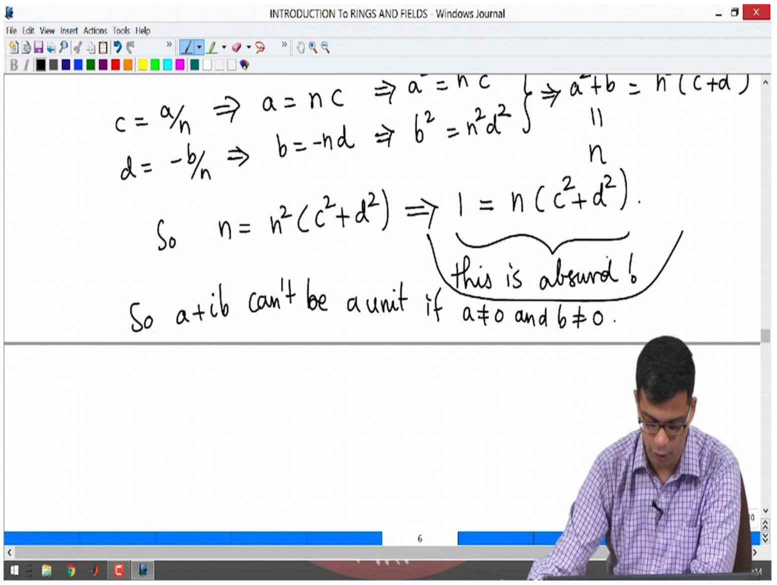


Now, we also have the earlier equations have this form c equals a by n, this implies a equals nc. Similarly, d equals minus b by n this implies minus b is or let us say b is minus nd, right. So, I have in this box c equals a by n, n is a squared a by plus b squared. So, a is nc b is minus nd.

So, this tells me that a squared is n squared c squared this tells me that b squared is n squared d squared, these two together tell me that a squared plus b squared is n squared times c squared plus d squared, right. I am adding these two, but a squared plus b squared is by definition n. So, what we have is n equals n squared time c squared plus d squared, but n is a positive integer in fact, n is at least 2.

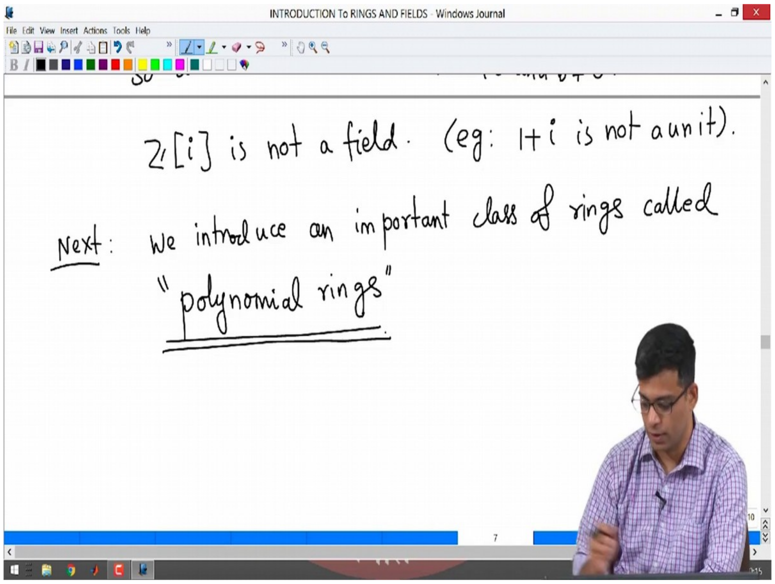
So, I can cancel n 1 n in both sides I get 1 equals n times c squared plus d squared, but this is not a this is absurd, why? Why is this absurd, because n is at least 2 right and c squared plus d squared is an integer, whatever it is, it is an integer. So, we have 2 at least 2 here times an integer equals 1 that is absurd because 2 does not have a multiplicative inverse.

(Refer Slide Time: 21:17)



So, what is a contradiction? So, a plus ib can not be a unit right, if a is non-zero and b is non-zero. So, this proves our earlier claim, that the only units so, I will go back to that. So, the claim was the only units in Z i are 1 minus 1, i minus i ok. So, this is just a computation I wanted to do this because in this course, the idea is also to do various computations and with the hope that you get comfortable with doing computations in ring theory.

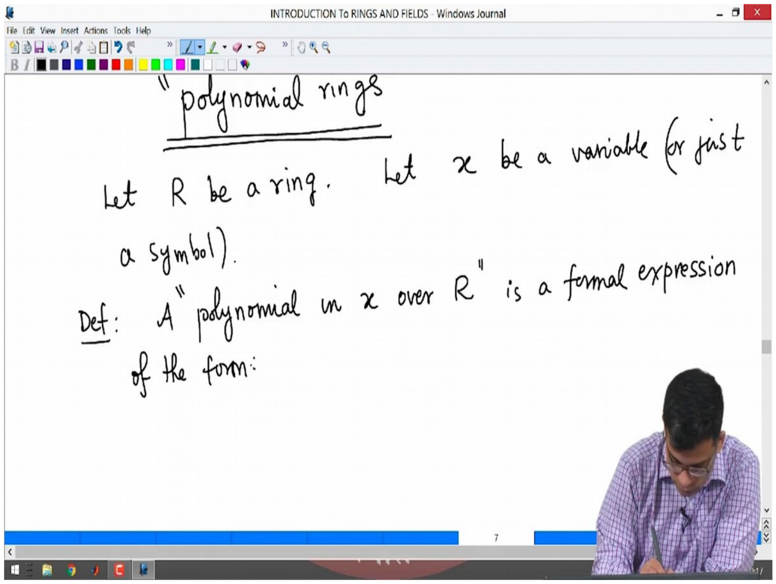
(Refer Slide Time: 22:05)



So, in particular we conclude that Z i is not a field, because it has lots of elements that are not units. For example, 1 plus i is not a unit, it is not a 0 element and it is not a unit ok. So, it has very few units, it has infinitely many elements, but only 4 units. So, units are important objects in rings, but they may be very few. For example, Z has only 2 units and Z i has only 4 units. In the other extreme when you have every non-zero element is a unit, you have what is called a field, ok.

So, in the next order of business for us is to introduce a very important class of rings called polynomial rings. So, we introduce ok. So, I am going to introduce this is something that maybe you are familiar with, but still I will, just to get the notation fixed for the course, I will introduce this and lot of this course will be study of polynomial rings. So, these are important for you to understand carefully.

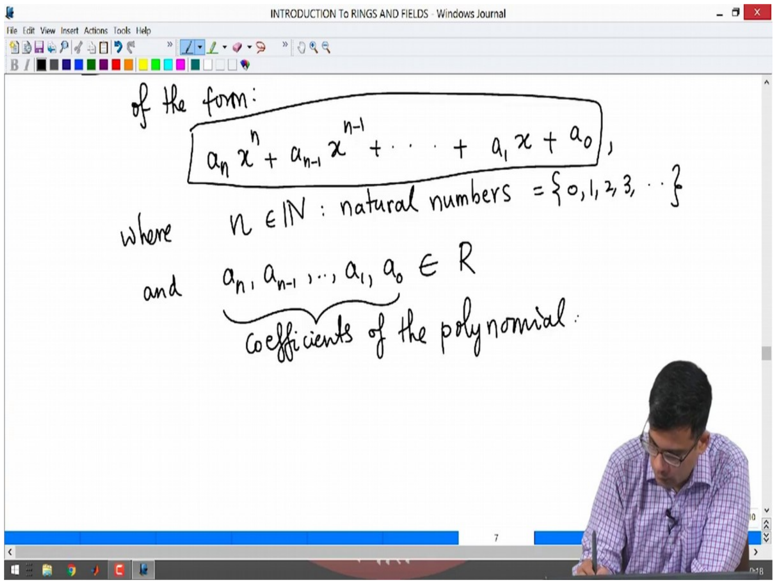
(Refer Slide Time: 23:37)



So, I will spend, I will gradually introduce these. Today, I want to discuss the definition and basic examples. Polynomial rings can be defined over any base ring so, any starting point. So, we will start with a ring R, so, let R be a ring.

And we use a symbol called x ok, this is just a symbol. So, let x be a variable or just a symbol so, it has no other meaning that is what I mean, think of this just as a symbol ok. So, x is just a symbol it is not a number, it is not an element of any set that you are used to it is just symbol, it has only those properties that we give it ok. So, I am going to define a polynomial. So, this is the terminology a polynomial in x over R is a formal expression of the form. So, what is the formal expression that we want to call a polynomial, it is something like this.

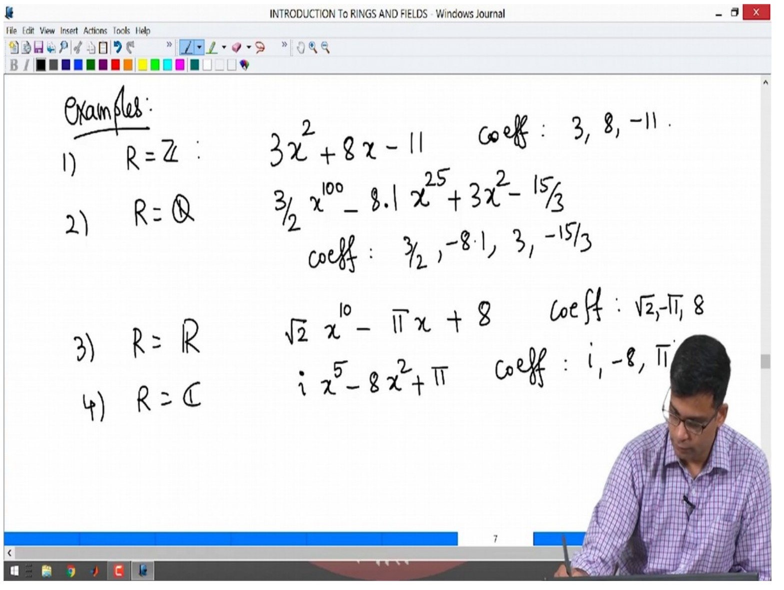
(Refer Slide Time: 25:01)



So, a n x n so, I will describe these in examples. So, it becomes clear, x n minus 1 dot dot dot a 1 x plus a 0, what are these things? Where n is a natural number. So, I am going to use this notation for natural numbers and for me natural numbers include 0. So, this is the set 0 1 2 3 and so on. So, n is a natural number n could be 0 also. And, these elements an, an minus 1 this was this n minus 1 are subscripts a1, a0 are elements of the underlying ring ok.

So, a polynomial is something like this. So, polynomial is just a expression like this, where these are called coefficients. So, these are called ok. So, just to get used to this let us take some examples.

(Refer Slide Time: 26:22)

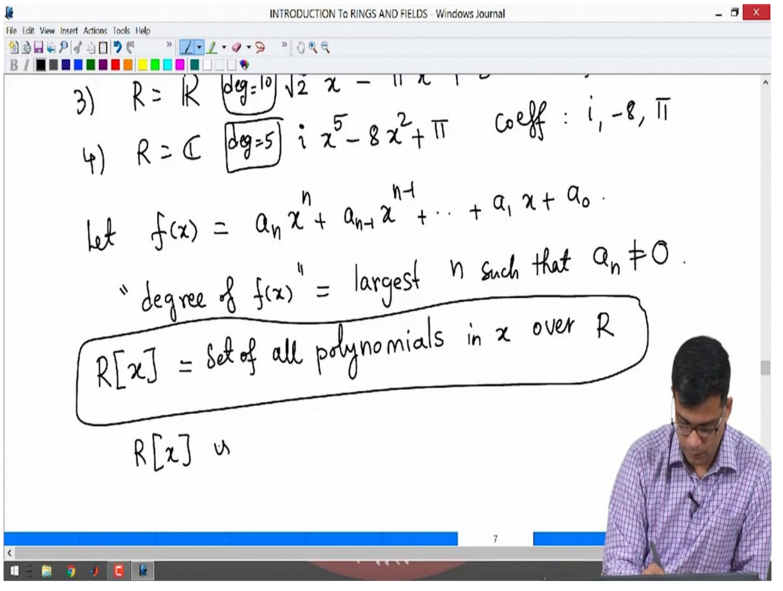


So, 1 so, R equals Z. So, one polynomial would be 3 x squared plus 8 x minus 11 right. So, 11 so, it is exactly like in that box right. So, have x squared. So, I am taking n to be 2 here x squared x power 1 and then x power 0; 3, 8 and minus 11 are the coefficients. So, here the coefficients are 3, 8 and minus 11 and they are integers. So, that is why Z is playing a role here. Similarly, you can take R to be Q, R to be Q. So, here you get root 3 by 2 x power 100 minus 8.1 x power 25 plus 3 x squared minus 15 by 3.

So, this is an element, is a polynomial right. So, here the coefficients are 3 by 2 minus 8.1, 3 and minus 15 by 3 right. So, the underlying ring plays a role in providing coefficients. So, this is not a polynomial over remember polynomial over R is important. The first example is a polymer over Z. So, it is also a polynomial of Q if the coefficients are also rational numbers.

But, the second one is not a polynomial over Z, it is only a polynomial over Q. Similarly, you can take I mean the you can keep doing this, you can take real numbers, you can take root 2 x 10 minus pi x plus 8. So, here the coefficients are root 2 pi and minus pi and 8 right and you can take. So, this is a polynomial over real numbers, but not over rational numbers. So, you can take i times x power 5 minus 8 x squared plus pi for example. So, this is a polynomial over complex numbers, but not over real numbers because i is not a real number.

(Refer Slide Time: 28:49)



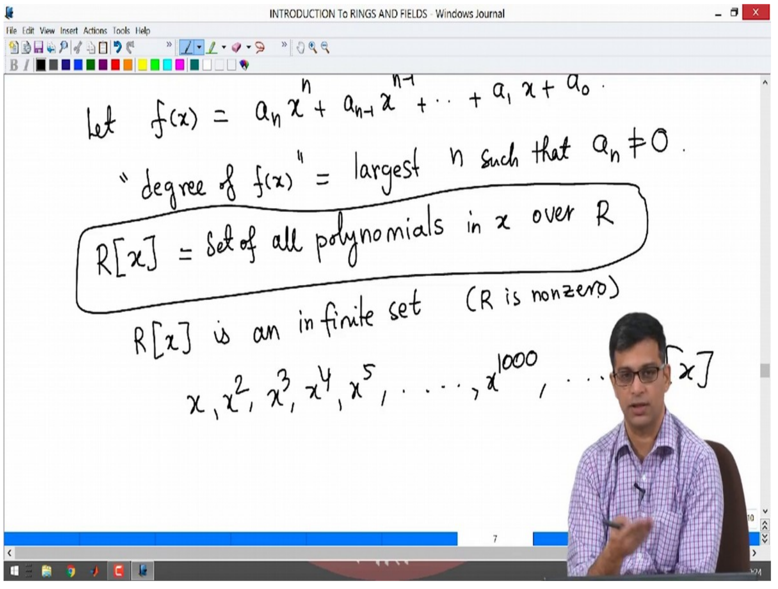
You can also do, so we will discuss this later, we can also take coefficients as polynomials so, that we will discuss later. So, I hope this is clear: a polynomial is just a formal expression like this ok. So, and the coefficients are coming from the underlying ring x is just a new variable that we have introduced.

And some terminology: we call degree. So, let us say f is a we usually used the symbol f to denote polynomial f, g, h to denote polynomials. Let us say f is a polynomial. So, that is, let us say this is a polynomial, degree of f is the largest n such that a_n is non-zero. Remember by definition a polynomial is a finite sum like this you cannot keep forever adding things.

So, there must be a largest n beyond which they are all 0. So, the largest n such that a_n is non-zero is called the degree. So, if we go back to the examples here degree here is 2 right, degree here is 100, because the largest coefficient largest term that has non-zero coefficient is 100, here degree is 10, here degree is 5, ok. So, degree is that and finally, I want to introduce this notation R square bracket x stands for the set of polynomials in x over R.

So, this is the important set for us. So, it is the set of all polynomials in the variable x over R. So, it is set of all polynomials. So, let me emphasize that set of all. So, you take all degrees ,all coefficients. So, it is really a huge polynomial, it is a huge set even if R has only finitely many elements. For example, Z mod n Z mod 3 Z Z mod 2 Z have only few elements right small 2 or 3 elements. So, the set of coefficients you can get is finite, but because the degree can be arbitrarily large, R[x] would be an infinite set right.

(Refer Slide Time: 31:45)



Because, you can take it contains x, x squared, x 3, x to the 4th, x to the 5th, it contains all these elements right x power 1000 and so on. So, these are all in R x ok. So, as long as R is non-zero I guess assume that R is non-zero. So, there is 1 in it that is not 0 then you have all these elements.

So, it is an infinite set. So, the goal for us next in the next video is to give a ring structure to this. So, that it is currently just a set of all polynomials. Once we talk about adding polynomials, multiplying polynomials and we verify that these addition multiplication have the required properties, it becomes a ring so, then we will call it a polynomial ring.

So, this is an important class of rings for us and that we will focus a lot on this course. So, I will stop the video today here with this.

Thank you.