

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

Lecture - 02
Examples of rings

So, let us continue. In the last video we looked at various examples of rings and we defined what rings are and what sub rings are. So, we will just continue with this discussion. So, before I start, some comments I want to make and these are important comments to make in the beginning.

(Refer Slide Time: 00:35)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}[i]$ are subrings of \mathbb{C} .

Remark:

1. It is possible to define rings without asking for multiplication to be commutative. They are called "non commutative rings".

Important example: matrix rings.

eg: 3×3 square matrices with real entries.

So, let us say a remark. So, remember one of the properties of in the definition of a ring was that ring is the multiplication of the ring is commutative. So, remark the

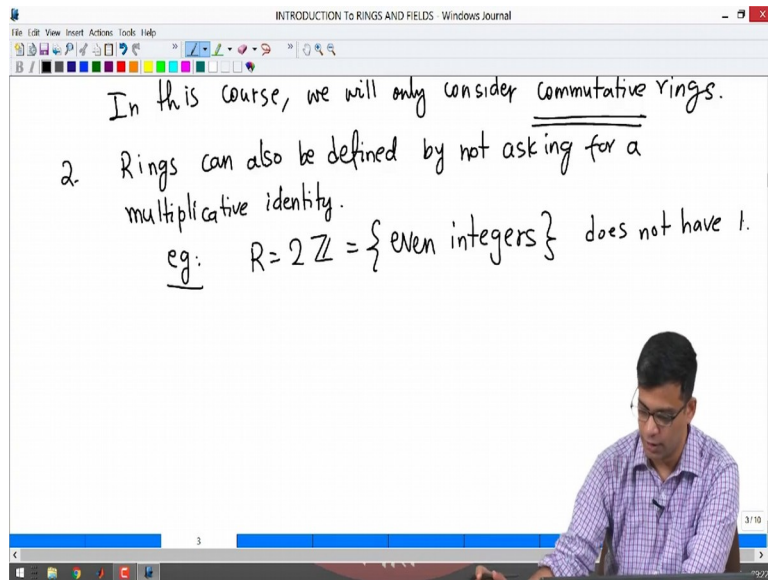
first remark is it is possible or it is done like this, it is possible to define rings without asking for multiplication to be commutative. So, in other words if you just remove that word from the definition, that multiplication need not be commutative. It has to have a other properties, it is associative it has one it has it is closed and what are the other properties?

So, it is associative it contains identity element, if you just ask that it is possible to study rings like that, they are called “non-commutative rings” ok, because you do not ask for commutativity. So, that is a definitely important example that people study and the most important example here is for non-commutative rings. So, matrix rings. So, I will not spend a lot of time on this I would not discuss this in detail. But matrix rings are so, example you look at for example, 3 by 3 square matrices with real entries. So, this is just an example.

You can multiply you can take any size square matrices with any entries in any ring in fact, is a integers, reals, complexes, rational numbers and so on. So, see here also we can add under addition it is a perfectly good abelian group, you can multiply matrices, it is associative it has identity element, but it is not commutative ok. So, that is why it is not a ring in the sense of my definition of the last video. However, it is what is called a non-commutative ring.

So, the study of non-commutative rings and their properties comes under the subject of non-commutative algebra. So, I am not studying doing that in this course. So, in this course we will only consider commutative rings.

(Refer Slide Time: 03:25)



So, in this course we will only consider commutative rings. So, the non-commutative ring theory is an important subject that is one studies people study, but it is not the focus for us in this course. So, for us we will only look at rings which were the multiplication is commutative in particular we will not study matrix rings in this course ok.

So, the other remark is that rings can also be defined, ok, by not asking for a multiplicative identity ok. So, in other words remember one is supposed to be there in any ring by our definition. So, you can ask you do not need to ask it. So, sometimes there other properties will be satisfied for example, if you take R to be $2\mathbb{Z}$. So, this is the set of all even integers. So, even integers; that means, integers of the form $2n$, where n is an arbitrary integer, they do have all the properties of a ring. So, there is an addition under addition, it is an abelian group, because 0 is there inverse of an even integer is even integer sum of 2 even integers is an even integer and so on.

It also has multiplication because if you multiply 2 even integers you get an even integer, you can it is associative multiplication of integers is a associative. It is even commutative right integer multiplication is commutative, but there is no 1. There is no element in the set which functions as 1. Of course, 1 is not even, but there is no integer here the functions as identity for multiplication, because you multiply any integer with anything in here, it is going to not give that integer back. So, this is a this does not have 1 ok.

So, one also studies sometimes, it is important to expand your definition of a ring to consider rings without unit without multiplicative identity, but we do not do that. So, in this course again let me emphasize this, I will make this remarks once and I will not say it again.

(Refer Slide Time: 06:09)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

In this course, we will always assume rings have 1.

More examples of rings:

• Zero ring $R = \{0\}$ In this ring $1 = 0$.

In this course, we will not consider this. So, we will always assume R has rings have multiplicative identity. So, basically what I am saying is that in my earlier video, first video, last video whatever the definition of ring is, is the ring that we

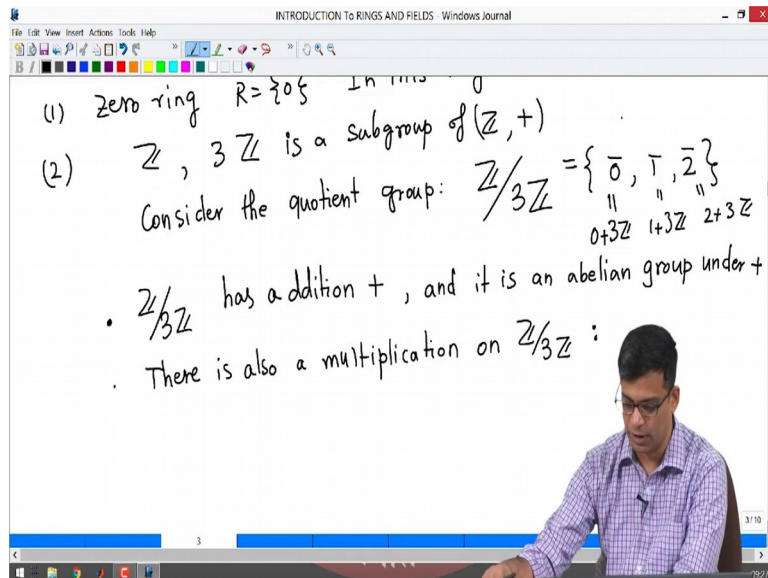
will consider. This remark is to indicate you that there are other kinds of things that people study.

But, in this course we will stick to the definition that I gave. So, before continuing with the properties of rings so, let me just give you more examples of rings. So, we look at various rings examples of rings in the last video, which are all subsets of complex numbers. So, they are in fact, sub rings of complex numbers. So, what I want to do now is give you examples of rings that cannot be that are not inside \mathbb{C} . So, that you see that there are lots of examples of rings.

So, one trivial example to just get rid of is we will quickly say this: the zero ring. So, the zero ring is just the ring consisting of just the element 0. So, here this trivially satisfies all the properties of a ring that I wrote in the last video. It is closed under addition multiplication and so on it is an abelian group under addition and multiplication is associative and so on.

So, what is the identity element multiplicative identity in this ring. So, in this ring there is a 1, but it is equal to 0. So, 1 is equal to 0 in this ring. So, this is a trivial example. So, I have do not want to spend a lot of time on this. But, one example of a ring that I want to consider when you studied groups; so, this is 1, you studied group quotients right.

(Refer Slide Time: 08:09)



So, if you have a group then you can quotient by a sub group. So, let us take \mathbb{Z} and let us consider $n\mathbb{Z}$. So, let us first look at just as an example let us say $3\mathbb{Z}$; $3\mathbb{Z}$ is a subgroup of \mathbb{Z} . So, here I am considering the addition, which is the only operation which makes \mathbb{Z} a group. So, $3\mathbb{Z}$ is a sub group of \mathbb{Z} right, because you can add 2 elements of this you get another element of this.

What are the elements of $3\mathbb{Z}$? These are multiples of 3. So, if you have 2 multiples of 3 you add them you get an again a multiple of 3, 0 is there inverse of a multiple of 3 is also a multiple of 3 and so on. So, consider the quotient group; so, consider the quotient group $\mathbb{Z} \text{ mod } 3\mathbb{Z}$. Remember from your group theory course, this has 3 elements we usually denote them by the it is set of cosets right set of cosets of $3\mathbb{Z}$ in \mathbb{Z} .

There are 3 of them denoted by 0-bar 1-bar 2-bar , this is really $0 \text{ plus } 3\mathbb{Z}$ this is $1 \text{ plus } 3\mathbb{Z}$, this is $2 \text{ plus } 3\mathbb{Z}$; there is addition on this right. So, you add them by just taking any representative and adding them. For example, 1-bar plus 2-bar is 0-bar , 0

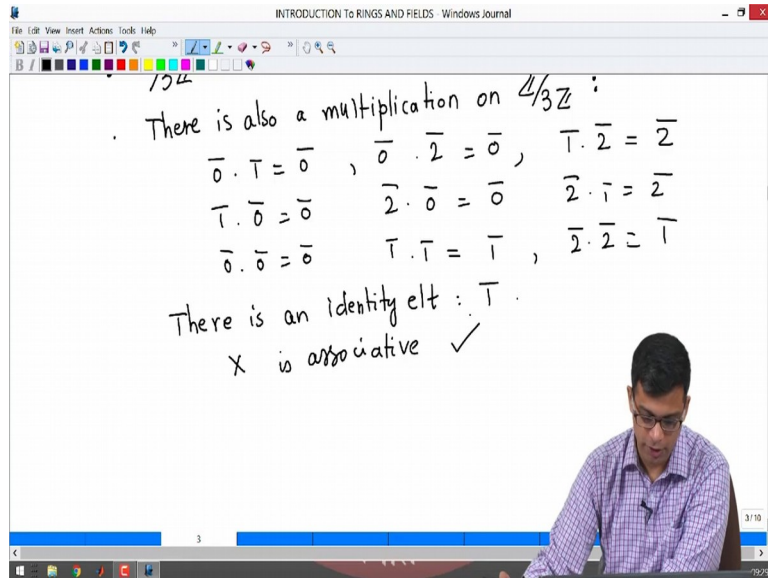
1 bar plus 1 bar is 2 bar 0 bar is identity element and so on. So, it is a group under addition.

So, let me record that here $\mathbb{Z}/3\mathbb{Z}$ has addition. So, let us denote again that by plus and it is a group under that. In fact, it is an abelian group. In fact, note that any group of order 3 is abelian. So, it is a group of order 3. So, it is under addition it is a group of order 3 so, it is abelian, but this is where you would have stopped in group theory.

Now, I want to introduce a multiplication on this set. So, I want to say that this also has multiplication. And then I want to ask is it a group, there is also a \cdot on $\mathbb{Z}/3\mathbb{Z}$. So, it has only 3 elements right. So, it is easy for me to define the multiplication. I will tell you how to multiply, you multiply just like you add. How did you add 1 bar and 2 bar? You picked any representatives of those cosets.

For example, 1 bar you can take representative 1, 2 bar you can represent take representative 2 and you add them, you get 3. So, you take the coset of 3 which is 0, you do exactly the same thing for multiplication, you take two representatives and multiply them.

(Refer Slide Time: 11:19)



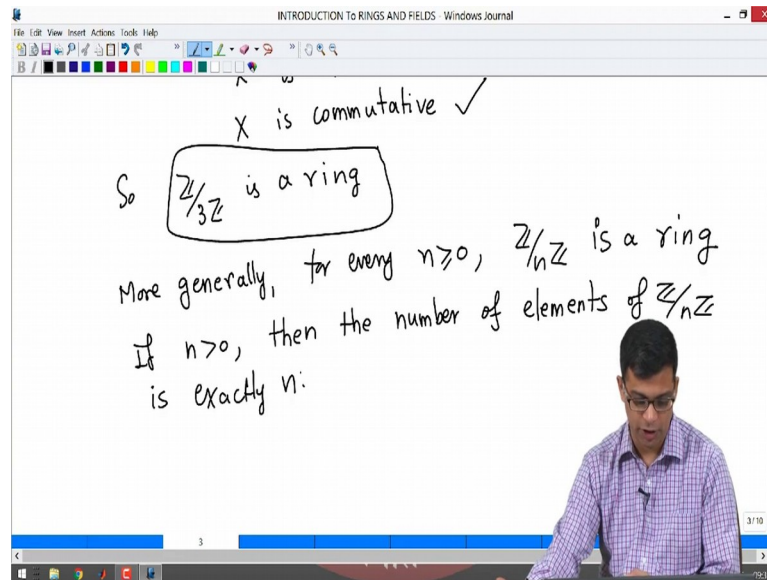
So, for example, 0 bar dot 1 bar is 0 bar 0 bar dot 2 bar is 0 bar and 1 bar dot 2 bar, what would this be? You take 1 and 2 multiply them you get 2 bar 2, so, you get 2 bar. So, and the other way because multiplication of integers is commutative you get the other if you interchange the role of the order of these elements, you get the same element.

And finally, I need to multiply an element with itself what is 0 bar dot 0 bar, that I claim is 0 bar right, that is clear because 0 time 0 is 0. What is 1 bar times 1 bar? It is 1 times 1 bar. So, it is 1 bar 2 bar times 2 bar is 4, but 4 bar is 1 bar because 4 is 1 modulo 3; so, this completely describes multiplication on $\mathbb{Z} \text{ mod } 3 \mathbb{Z}$.

So, now, if you just stare at this carefully, I claim that this multiplication has all the properties that we want. It has, there is an identity element, what is an identity element? Namely 1 bar right, 1 bar is an identity element, because whenever you mul-

multiply anything by 1 bar you get that element back ok, it is certainly associative, why is that? So, this is something I won't to spend a lot of time discussing, but this is basically because multiplication of integers is associative. So, and to multiply cosets you are really multiplying integers and then taking the corresponding cosets.

(Refer Slide Time: 13:11)



So, this is associative, this is also commutative for the same reason right, because multiplication of integers is commutative. And hence it has all the properties that we want. So, we are able to conclude now, $\mathbb{Z} \text{ mod } 3 \mathbb{Z}$ is a ring ok. So, $\mathbb{Z} \text{ mod } 3 \mathbb{Z}$ is a ring and it is a ring with exactly 3 elements.

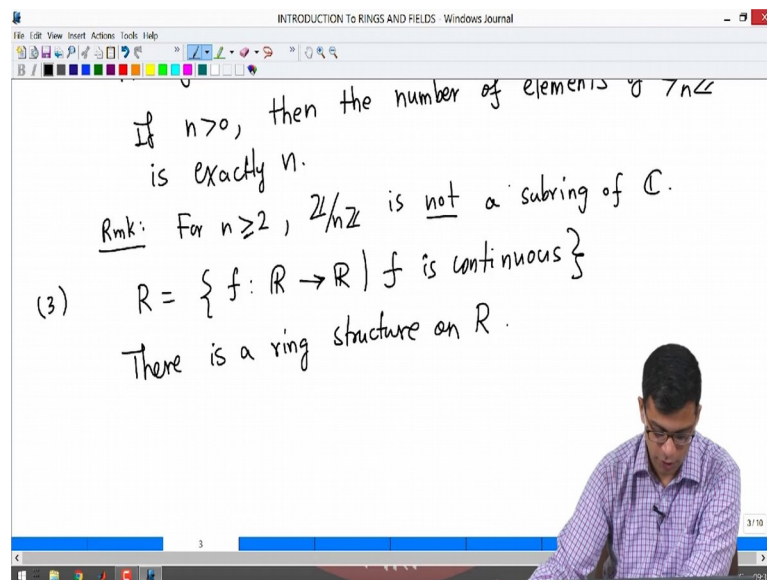
So, more generally for every positive integer, let us say for every non-negative integer $\mathbb{Z} \text{ mod } n \mathbb{Z}$, there is absolutely no difference it is exactly the same calculation and if you replace 3 by n you get that $\mathbb{Z} \text{ mod } n \mathbb{Z}$ is a ring.

So, if n is positive, then the number of elements is exactly n that is because we know this already because $\mathbb{Z} \bmod n \mathbb{Z}$ is a group of order n right. So, on that we are giving multiplication, so, it is a ring of order n .

So, what we have done in particular is given any positive integer n we have produced a ring of that order. For example, if n equal to 1 you get the 0 ring that I discussed earlier right. So, if you take n equal to 1, $1 \mathbb{Z}$ is just $1 \mathbb{Z}$. So, $\mathbb{Z} \bmod \mathbb{Z}$ has only 1 coset. So, we, namely the 0 coset. So, that is the ring 0 ring, but $\mathbb{Z} \bmod 2 \mathbb{Z}$ has 2 elements $\mathbb{Z} \bmod 3 \mathbb{Z}$ has 3 elements and so on.

And later on once we start talking about homomorphisms of rings and some other properties of rings, you will see that whenever n is positive $\mathbb{Z} \bmod n \mathbb{Z}$ cannot be realized as a sub ring of \mathbb{C} . So, these are examples of rings that are not sub rings of \mathbb{C} ok. So, I will remark that here and we will discuss this later.

(Refer Slide Time: 15:23)



INTRODUCTION TO RINGS AND FIELDS - Windows Journal

If $n > 0$, then the number of elements of $\mathbb{Z}/n\mathbb{Z}$ is exactly n .

Rmk: For $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is not a subring of \mathbb{C} .

(3) $R = \{ f: \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ is continuous} \}$

There is a ring structure on R .

For n positive $\mathbb{Z} \bmod n \mathbb{Z}$ let us say n at least 2, because n equal to 1 we get the 0 ring, that is a certainly a sub ring of \mathbb{C} . So, it is not a sub ring of \mathbb{C} , so, it is not a sub ring of \mathbb{C} .

So, next one more example I want to do, similarly that is not a sub ring of \mathbb{C} is I do not know the numbering. So, let us say this is next is 3. So, what is the next ring? So, let us look at let us get R to be the set of continuous functions from the real numbers to real numbers so, f is continuous. So, I am looking at all functions from the set of real numbers to set of real numbers that are continuous.

So, remember this is just something that you have learned in analysis right. So, continuous functions from \mathbb{R} to \mathbb{R} , you take all such things. I want to actually think of this as a ring. So, there is a ring structure on R . The usual \mathbb{R} is a set of continuous functions, what is this? Remember we have to start from scratch here. So, it is not like we can do in earlier examples there is already some there all coming from usual integers or rational numbers and so on.

(Refer Slide Time: 17:05)

$f+g \in R$ $f+g : \mathbb{R} \rightarrow \mathbb{R}$ $(f+g)(a) = f(a) + g(a)$ for any $a \in \mathbb{R}$

ex: $f+g$ is continuous. So $f+g \in R$.

Is R an abelian group under $+$?

✓ Zero element: $0 : \mathbb{R} \rightarrow \mathbb{R}$
 $a \mapsto 0 \quad \forall a \in \mathbb{R}$
 is the zero function

$(f+0)(a) = f(a) + 0(a)$

So, here we have to define addition multiplication carefully. So, how do we define addition? So, let us take two continuous functions. So, let us say f and g are both inside R ; that means, f is a function from R to R which is continuous, so, is g . So, I want to define f plus g right and I need it to be in R , I want to define a function which I want to call the sum of f plus and f and g .

So, there is an obvious thing to do. So, define because the target space as addition I can simply define f plus g of a real number let us say a to be f of a plus g of a right. So, for any so, take any real number the function f plus g on that real number simply is f of a plus g of a .

(Refer Slide Time: 18:13)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

ex: $f+g$ is continuous. So $f+g \in R$.

Is R an abelian group under $+$?

Zero element : $0 : \mathbb{R} \rightarrow \mathbb{R}$
 $a \mapsto 0 \quad \forall a \in \mathbb{R}$.

is the zero function

$(f+0)(a) = f(a) + 0(a)$

So, this is just definitely a function and it is an exercise in analysis to show that f plus g is actually continuous. So, it is continuous. So, f plus g is in R . So, this tells me that there is addition on R right, you give me two continuous functions I add them to get another continuous function.

Now, we have addition. So, we can ask is R an abelian group under addition. So, is R an abelian group under this particular addition that I defined? And you can quickly check that it is so. Because what is zero element? Zero element is simply the 0 function, what is a zero function? This function sends a to 0 for all a in R . So, the zero function so, zero element is the zero function zero function is a function which sends every real number to the real number 0.

Certainly it is a continuous function, it is a constant functions so, it is continuous function and if we add anything to 0. So, let us say f plus 0 of a is f of a by definition f of a plus 0 of a I am denoting the function also by 0, but f of a plus 0 of a is f of a because 0 of a is 0. So, this is the 0 element, so, that is good.

(Refer Slide Time: 19:57)

The whiteboard contains the following handwritten text:

- $a \mapsto 0$
- is the zero function
- $(f + 0)(a) = f(a) + 0(a) = f(a)$
- $f + (-f) = 0$
- $(-f)(a) = -f(a)$
- is a continuous function.
- + is associative ✓
- + is commutative ✓
- these both follow because + has these properties on \mathbb{R} .

The presenter is a man with glasses wearing a purple checkered shirt, looking down at the whiteboard.

So, there is a identity element certainly one can check that there is inverses right. So, because minus f a minus given a continuous function f you can define minus f of a to be minus f of a. So, this is a continuous function. For every continuous function it is negative is also a continuous function, we are just changing the sign.

So, every element has an inverse and one can check that plus is associative and plus is commutative. Remember we need an abelian group ok, these both follow, the basic reason that they both follow, these both follow is that addition and is associative and commutative in \mathbb{R} . Because, we are ultimately adding inside \mathbb{R} . Remember here we are adding inside \mathbb{R} , this addition is in \mathbb{R} , because f of a and g of a are in real numbers. So, you add them as real numbers. So, these both follow because plus has these properties on \mathbb{R} , ok.

So, the answer to this question is yes \mathbb{R} the set of continuous functions on real numbers, real valued continuous functions on real numbers is an abelian group under multiplication.

(Refer Slide Time: 21:41)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

Multiplication on R : $f, g \in R$

$fg : \mathbb{R} \rightarrow \mathbb{R}$

$(fg)(a) = f(a)g(a)$

ex: fg is continuous; so $fg \in R$.

So, now what is multiplication on R ? So, how do you multiply to real valued continuous functions on R real numbers, the exactly the same way; so, let us say that we defined addition. So, let us say f, g are in R how do you define fg from as a continuous function from R to R . You take fg of a to be f of a times g of a .

So, again we are using the fact that real numbers have multiplication earlier we use the fact that real numbers have addition here we are using the fact that real numbers say multiplication. It is an easy exercise to check that fg is continuous.

(Refer Slide Time: 22:45)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

$fg : \mathbb{R} \rightarrow \mathbb{R}$
 $(fg)(a) = f(a)g(a)$

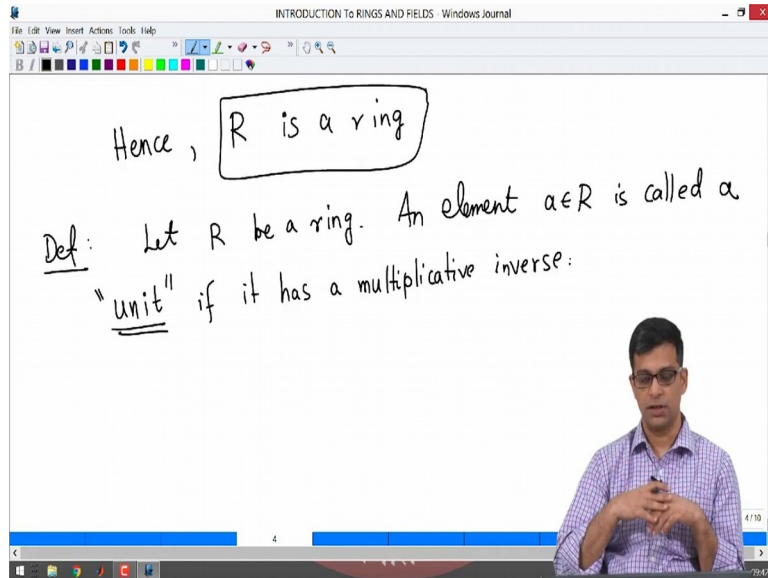
ex: • fg is continuous; So $fg \in R$.

- The constant function $1 : \mathbb{R} \rightarrow \mathbb{R}$
 $a \mapsto 1$
is the multiplicative identity.
- X is associative and commutative.

So, fg is in R . So, if f and g are continuous their product is continuous. So, there is a operation and one can check that the function the constant function 1, which sends every real number to 1 is the multiplicative identity ok.

Because, if f times the constant function is simply f so, it is the multiplicative identity and we can check quickly that is associative and commutative; again just like addition is commutative and associative on real numbers multiplication is associative and commutative on real numbers, that carries over to the set of functions. So, the multiplication on R also has the required properties.

(Refer Slide Time: 23:47)

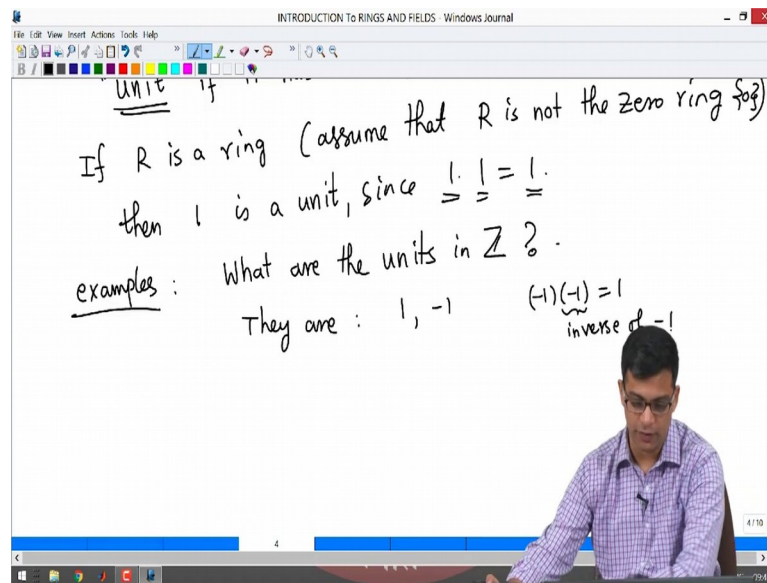


Hence, R is a ring ok. So, this is sometimes so, interesting ring to look at we will come back and consider this ring again in this course. So, this is a ring of this is a ring consisting of all continuous real valued functions on real numbers ok. So, these are some of the rings that I wanted to discuss, I want introduce one important definition and then we will look at more properties of rings.

So, this is the definition. So, note that in a ring multiplication is not a group operation. So, they it is not a group operation because it is allowed to not satisfy one group axiom. Namely, that not every element is required to have a multiplicative inverse so, but sometimes some elements do have multiplicative inverses. So, we want to give a special name to them. So, let R be a ring, an element a in R is called a unit if it has a multiplicative inverse ok, so, that is all.

So, unit is a element of a ring which has multiplicative inverse. Not every element in a ring is supposed to have, is required to have multiplicative inverses. So, it need not be a unit, but if it does we call it a unit.

(Refer Slide Time: 25:41)



So, one important remark is if R is a ring and assume that R is not the zero ring. So, R is not the zero ring consisting of just the element 0 , that is not an interesting ring. So, we usually do not study that. So, if R is a ring and we will all assume it for now that it is not the 0 ring that is in fact, an assumption that we make most of the time. Then 1 is a unit right, 1 is a unit because it has a multiplicative inverse. Since 1 times 1 is 1 , so, 1 has an inverse the inverse of 1 is itself. So, 1 is a unit, so, every non zero ring has a unit.

But, maybe some other units also exist. So, now, let us look at examples. So, what are the units in let us say the ring \mathbb{Z} ? So, the \mathbb{Z} the set of integers \mathbb{Z} is a ring, be-

cause we saw that it has addition and multiplication, what are the units? So, we agreed that 1 is a unit; 1 is a unit in any non zero ring, but minus 1 is also unit here right because minus 1 times minus 1 is 1. So, minus 1 has a multiplicative inverse. So, this is the inverse of so, minus 1 is the inverse of itself. What is multiplicative inverse I should have mentioned that earlier, multiplicative inverse is an element that you multiply to get 1. So, multiplicative inverse means just in the group sense. So, inverse is any element when you multiply you to get the multiplicative identity.

(Refer Slide Time: 27:57)

The screenshot shows a Windows Journal window with the following handwritten content:

- There are no other units in \mathbb{Z}
- let $n \in \mathbb{Z}$, $n \neq 1$, $n \neq -1$.
- ~~$n \square = 1$~~
- ~~$3 \square = 1$~~
- only units in \mathbb{Z} are 1 and -1.

So, minus 1 is a unit because minus 1 times minus 1 is 1, but there are no other units, right. Why is that? There are no other units of, no other units in \mathbb{Z} , that is because, you take any integer, let n be an integer, which is different from 1 and minus 1. Can you multiply n with something to get 1? So, for example, if n is 3 can you multiply with something to get 1? This is not possible right.

So, this is not possible, you multiply any integer n which is not 1 or minus 1 with any other integer you will never get 1, because the inverse really you need to go to

rational numbers to get the inverse you have to take 1 by n. But, 1 by n is not an integer. So, the only units; so, the only units in \mathbb{Z} are 1 and minus 1 ok. So, similarly now let me look at units in let us say \mathbb{Q} .

(Refer Slide Time: 29:03)

Units in \mathbb{Q} : Every nonzero rational number is a unit in \mathbb{Q} .

Proof: $\frac{a}{b} \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$

$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1$. So $\frac{a}{b}$ has a multiplicative inverse. So it is a unit.

The set of units in $\mathbb{Q} = \mathbb{Q} - \{0\}$.

0 is not a unit

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

I claim units in \mathbb{Q} are actually all non zero rational numbers. So, every non zero rational number is a unit, why is this? So, take any non zero rational number what is the proof of this? Let us take a/b in rational numbers.

So, a and b are in integer right, remember rational numbers are ratios of integers. And we assume that a is non zero and b is non zero, we take a non zero rational number. Does it have a multiplicative inverse? It does, because you take a times b time times a or b times b over a is 1.

(Refer Slide Time: 29:57)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

a UNIT

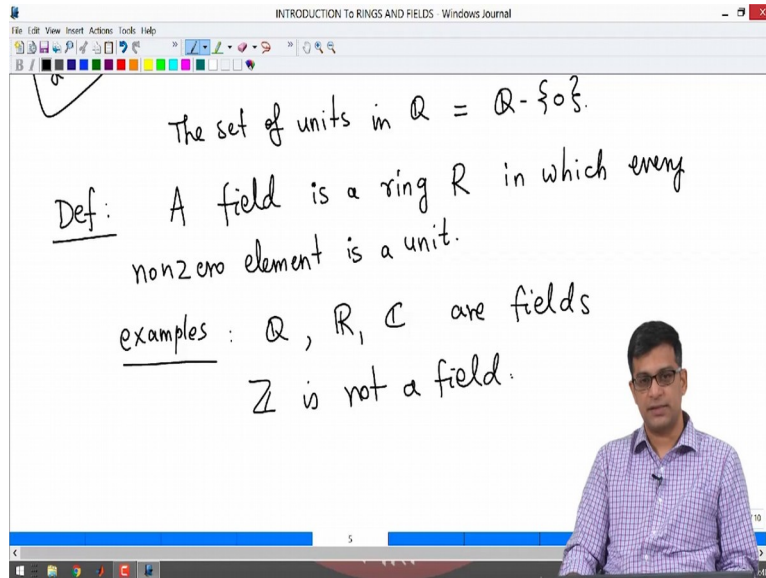
Proof: $\frac{a}{b} \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$

$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1$. So $\frac{a}{b}$ has a multiplicative inverse. So it is a unit.

The set of units in $\mathbb{Q} = \mathbb{Q} - \{0\}$.

So, a by b has a multiplicative inverse. So, it is a unit. So, multiplicative every non zero rational number has a multiplicative inverse. So, every non zero rational number is a unit in the ring of rational numbers. So, set of units in \mathbb{Q} is equal to \mathbb{Q} minus 0 . So, rings which have this property are very important, they have a special name and they are called fields.

(Refer Slide Time: 30:45)



So, let me end this video with this definition: a field is a ring R in which every non zero element is a unit. So, one thing I should mention the set of units in \mathbb{Q} is \mathbb{Q} minus 0 , I proved that every non zero rational number is a unit. I should also say that 0 is not a unit, but that is obvious right 0 is not a unit, because what is the meaning of 0 not being a unit. I am claiming that 0 does not have a multiplicative inverse that is because if we multiply 0 with any rational number you get 0 . You will never get 1 so, 0 certainly cannot have a multiplicative inverse.

So, in any ring you do not expect 0 to be a unit. What is the next best that can happen? Every non zero element can be a unit. So, if that happens we call it a field. So, examples of fields are, \mathbb{Q} is a field because of the example I did, similarly \mathbb{R} is a field \mathbb{C} is a field; so, are fields.

So, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields \mathbb{Z} is not a field, right. The example also makes it clear that \mathbb{Z} is not a field, because there are non zero elements of \mathbb{Z} that are not fields for example, 2 is not a field ok. So, let me stop this video here. I will in this video we

looked at more examples of rings and I defined important objects called units, and I talked about fields, which are special kinds of rings and we looked at examples of fields. So, in the next video we will consider one of the most important classes of rings, called polynomial rings.

Thank you.