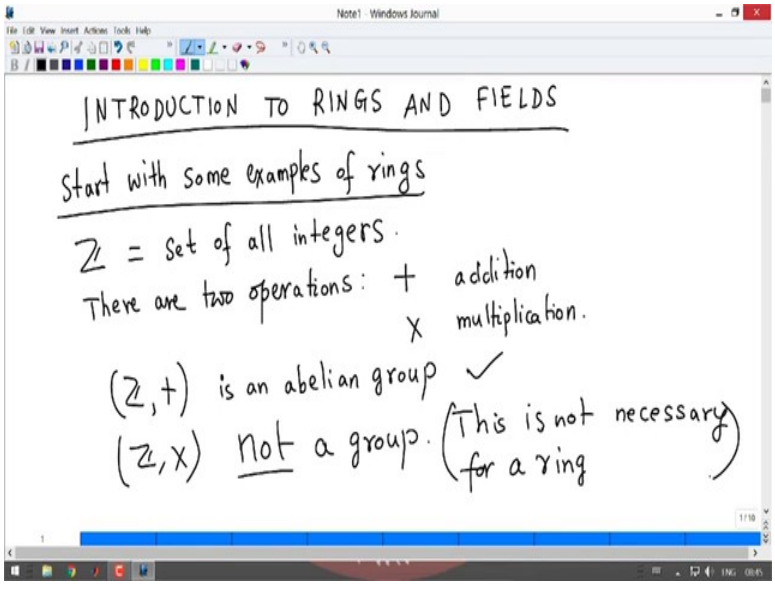
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 01
Introduction, main definitions

Hello. My name is Krishna Hanumanthu. I work in Chennai Mathematical Institute and in this 8 week course we are going to learn basics of rings and fields. Course title is Introduction to Rings and Fields.

(Refer Slide Time: 00:29)



So, rings and fields are algebraic objects which have some operations on them satisfying certain properties. So, this is a course that one does after learning some basic group theory and some linear algebra.

So, this is I am going to keep this as self contained as possible and the course will focus a lot on examples and problems. I will introduce some definitions and do important theorems, but at the same time I will talk about various examples and solve problems in my videos. So, in today's video I will give some examples of rings and then define them and study properties. So, roughly the plan for the course is around half the time about 4 weeks we will do rings, 4 to 5 weeks and the remaining term we will do fields.

Fields are just special cases of rings; they are rings with certain additional properties. So, after studying ring theory we will focus on fields for the last part of the course. So, let us start today with a general introduction to rings. So, I am going to start with basic examples before I give you the formal definition of a ring, ok.

So, you all know what a group is. A group is a set with an operation on it which has certain properties ,which are the properties are: there is an identity element; every element has an inverse. The operation is associative. So, a ring is something which has two operations. It is now it is usually we call these operations addition and multiplication. With respect to addition the ring is supposed to be an abelian group, with multiplication it need not be a group.

So, before I talk more about the definition, let me start with some examples. So, we will start with some examples of rings ok. So, the first example that I want to discuss which is the in some sense the most important ring is the set of integers. So, Z always when I write Z in this way I always mean the set of all integers. We know this as a group under addition, but in fact, it is also an example of what we want to consider as rings.

So, here there are two operations. So, they are the usual addition and multiplication right. So, plus is the addition of an integers and let us denote multiplication by cross. So, multiplication is the usual; multiplication is the usual multiplication of integers. So, with respect to these two, what are the properties of Z?

So, Z comma plus; so that means, the set of integers with addition is an abelian group ok. So, this is something that you would have seen in a course on group theory meaning there is, this operation is closed on the set of integers. Meaning you add two integers you get another integer there

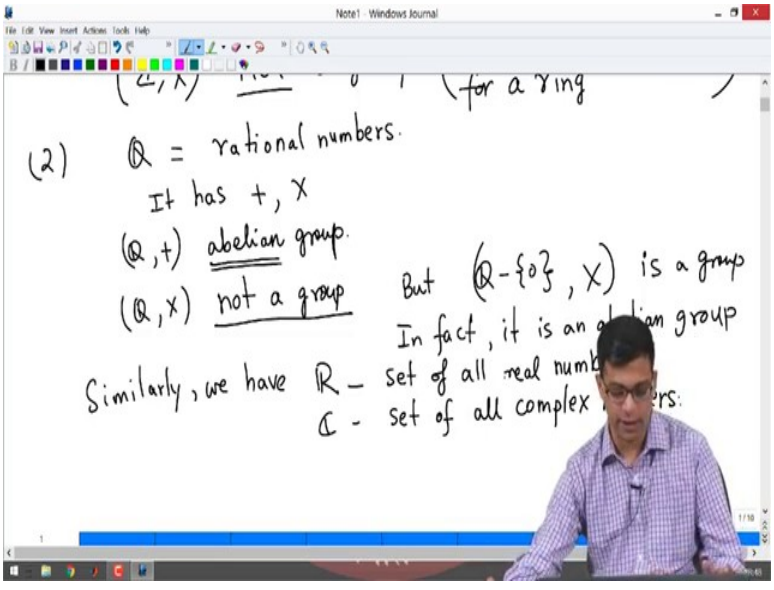
is a identity element namely 0; 0 is a identity element for the addition meaning if you add 0 to any element you get 0.

There is also inverse for every element. Every element has an inverse that you if you add the two you get 0. For example, inverse of 3 is minus 3 inverse of minus 10 is 10. Similarly the addition is associative. So, you add you can add three integers in either of the two natural ways. So, this is an abelian group.

So, this we know. What about the properties of integers under multiplication, so, Z cross. So, clearly this is not a group right. This also something you would have been if a you would be familiar with. This is not a group because it is certainly closed, but there are no inverse as here. There is no identity also because, 0 1 would be the most obvious candidate for the identity element because 2 times 1 is 2, but 0 does not have any inverse know my number when you multiply by 0, you get 1.

Similarly, you do not have inverses. For example, there is no number that you multiply 2 with to get 1 ok. So, it is not a group, but for a ring we do not care whether multiplication is a group or not. So, this is not necessary for a ring. So, this is the first important point. So, we do not need the set to be a group under addition under multiplication rather I should say. So, it is not a group under multiplication ok. So, some other examples; so, Z is our typical example of a group. So, let us look at the next example.

(Refer Slide Time: 06:05)



So, these are also familiar to you. So, the set of rational numbers Q always stands for set of rational numbers. Is this a group? Is this a ring? Let us see. So, clearly it has two operations it has plus and multiplication, Q under addition is an abelian group right. So, if you add two rational numbers you get a rational number. There is a 0 element. The every rational number as an inverse, it is associative and remember also I need the, I am noticing that it is an abelian group. If you have two rational numbers, you can add them in either order and you get the same answer.

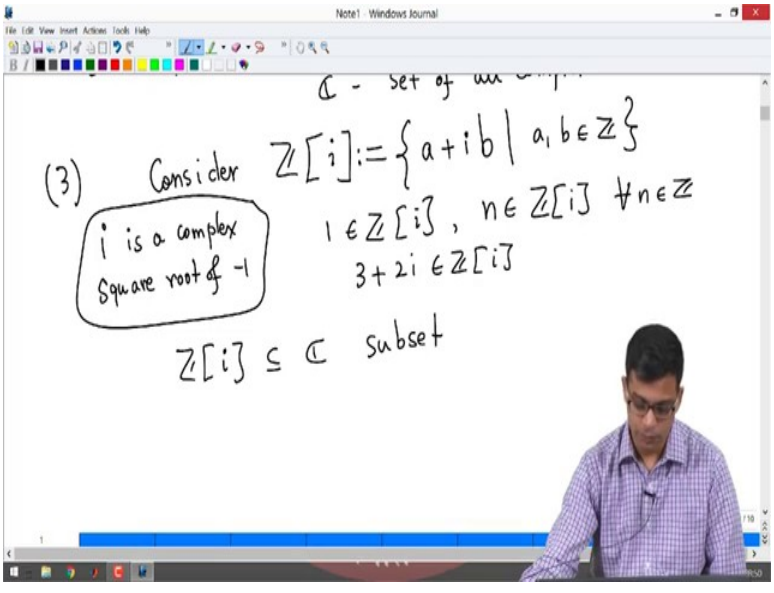
Again, just like with the case of integers, Q with multiplication is not a group. However, it is actually better than Z with multiplication because, if you remove 0 from Q and consider multiplication it is a group right. So, this is something that you would have seen in a course on group theory. Non-zero rational numbers with multiplication is a group under its called multiplicative group of rational numbers; non-zero rational numbers because here one is the identity element. Every rational number as an inverse and it is certainly associative and in fact, it is even an abelian group ok.

So, I will just do one or two more examples. So, similarly so, this is not really a new example. So, similarly we have the real numbers. So, set of real numbers; these are I am introducing these

because also these are important sets for us that provide very important examples for rings and fields that we talk about in this course. So, C stands for set of all complex numbers ok.

So, just like Q these have also two operations namely addition and multiplication. Under addition they are abelian groups and once you remove 0, they become abelian groups under multiplication. With 0 certainly you cannot expect them to be groups under multiplication because 0 does not have any inverse ok.

(Refer Slide Time: 08:49)



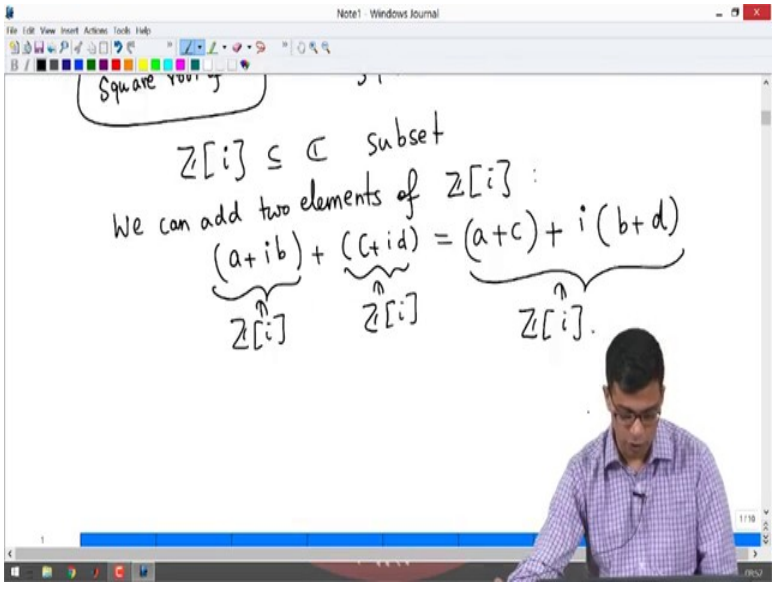
So, now I will just do one more example to not maybe so obvious, but we want to discuss this in more detail later on. So, consider; so, I will write a symbol here and I will explain ok. So, let us look at Z square bracket i where i is a square root of; so, it is a complex square root of; so, as usual we denote i we denote the complex square roots of i, minus 1 by i and minus i. So, square root of ok so, i stands for square root of minus 1.

So, consider this set Z[i]. What is this set? So, I am defining the set to be all elements of the form a plus i b where a and b are integers. So, that Z is playing a role here ok. So, Z i stands for a plus i b where a, b are elements of Z. For example, 1 is an element of Z i minus 1. In fact, any n is an

element of Z i right for all n in Z, because it is n plus i time 0. Similarly, 3 plus 2i is an element of Z and so on. So, you understand. So, you have these elements of Z[i].

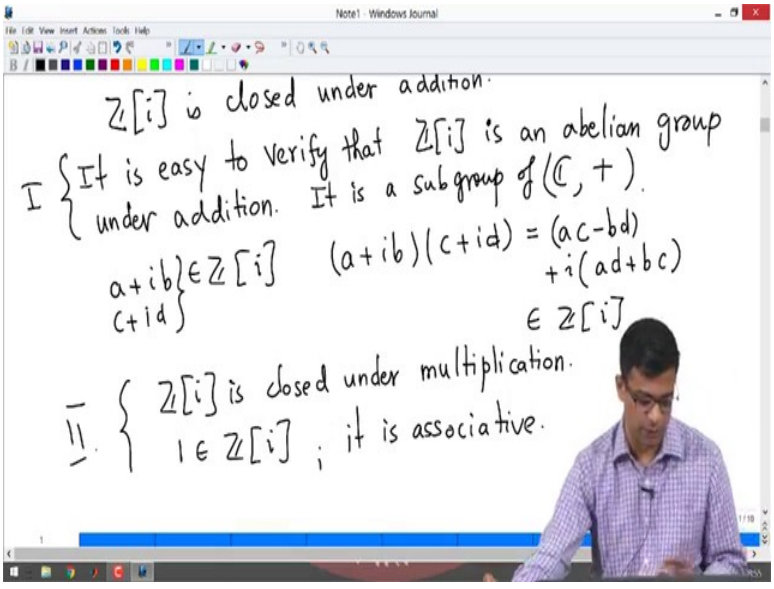
So, it is we understand there are this is a subset of complex numbers right. So, this is a subset of complex numbers because a plus ib is a complex number. Only we are restricting a and b to be integers. In generally a and b are any real numbers that way you get any complex number, now you want to only look at integers a and b are integers. So, it is a subset. I want to think of this as a ring later on.

(Refer Slide Time: 10:57)



So, we can add two elements of Z[i] right. So, there is an obvious addition just like you add them as if they are complex numbers right. So, if you have c plus id and a plus ib you add them, you get a plus c you first add the real parts so to speak and then you will add the imaginary part. So, a plus c plus b plus d right so, b plus d. So, now, if this is in Z i and this is also in Z i; that means what? a and b are integers by definition c and d are integers by definition. So, a plus c is an integer, b plus d is an integer. So, this is also in Z i right.

(Refer Slide Time: 12:05)



So, in other words what we have just showed is Z[i] is closed under addition. So, if you add two elements of Z[i] you get another element of Z i. In fact, you can check quickly that it is easy to check. I will leave this for you to check in detail, it is easy to verify, that Z i is in fact, an abelian group under addition.

So, if you remember your group theory, what I am really saying is that in fact, it is a subgroup of the complex numbers with addition. It is a subgroup of the complex numbers under addition see this is easy to check that it is an abelian group because there is the 0 element; 0 element is of the form a plus b i right, where a and b are integers it is 0 plus i times 0. Every element has an inverse; a plus i b has inverse minus a minus i b that is also in Z i and certainly it is associative because addition of complex numbers is associative and it is closed we checked. So, it is an abelian group.

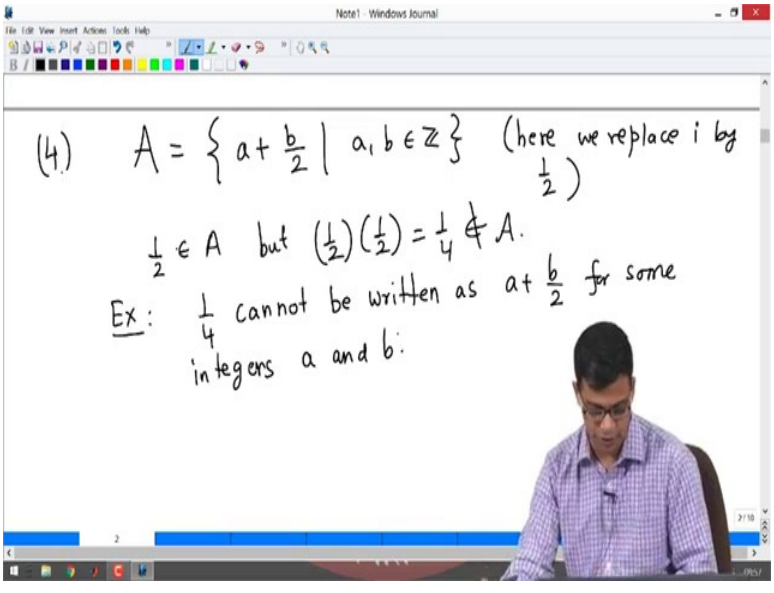
So, that is remember one of the properties we are looking for in a ring. So, it is a group that is old news. So, it is a group. So, this is the first property. We also need another thing for a ring. We need multiplication on the set that we want to consider as a ring. So, there is multiplication on

complex numbers. We need to still verify that Z i is closed under multiplication. So, let us choose two elements of Z i let us say a plus i b c plus id are inside Z i. Let me remind you; that means, in a and b are integers, c and d are integers.

If you multiply them just thinking them as complex numbers what would you get? What is a plus i b times c plus i d. a plus i b times c plus i d is this is the usual multiplication. You will get ac minus bd right because i squared is minus 1, so that will be the real part plus i times ad plus bc. Now, a, b, c, d are integers. So, ac minus bd is an integer, ad plus bc is an integer. So, this is also in Z i. So, first point I want to note is Z i is closed under multiplication we proved that here.

So, it is closed under multiplication which is an important property for a ring. There is a multiplication on the set and it has identity 1 is in Z i and it is associative; associative because this follows directly because complex number multiplication is associative. So, and it has some other properties that I will talk about once I discuss the formal definition of a ring ok. So, now, let me just do one more example where things do not go well. So, this is the second property. So, I will label it as 2. Final example I want to talk about before giving you the definition of a ring.

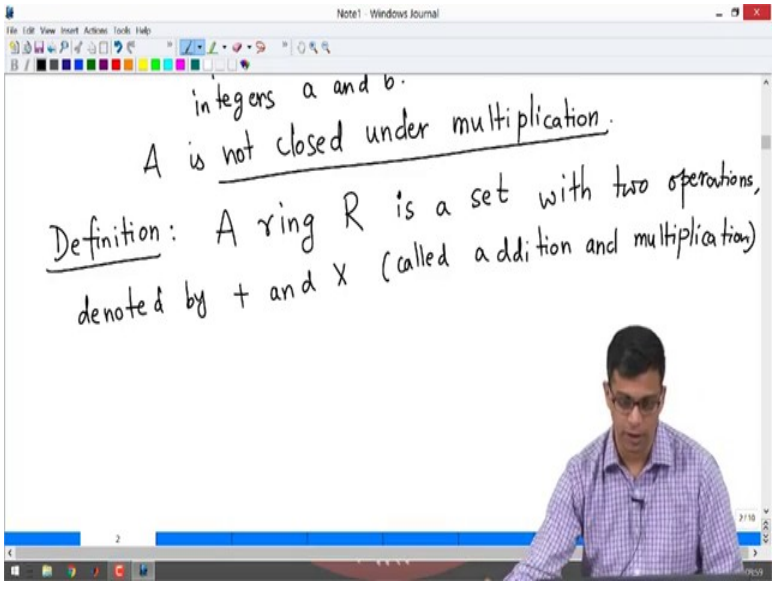
(Refer Slide Time: 15:51)



So, this is example 4. Let us look at similar to Z i let us look at Z let us say 1 by 2. Z 1 by 2, I will just take this; so, actually this is not what I am writing is not correct. So, let me just define any new symbol for this. Let us say A. So, A is I am just replacing i by 1 by 2 in the earlier example. So, here we replace i by 1 by 2. Remember, earlier we took looked at a plus i b where a and b are integers. Here I am taking a plus b times 1 by 2 where a and b are integers ok.

So, here if you multiply two things here for example, 1 by 2 is in A right because that is 0 plus 1 times 1 by 2, but 1 by 2 times 1 by 2 which is 1 by 4 is not in A. So, one can check that 1 by 4 cannot be written as. So, this is an exercise for you it is not a difficult exercise 1 by 4 cannot be as a plus b by 2 for some integers a and b. You write it like this and you clear denominators and check that there is a contradiction.

(Refer Slide Time: 17:49)



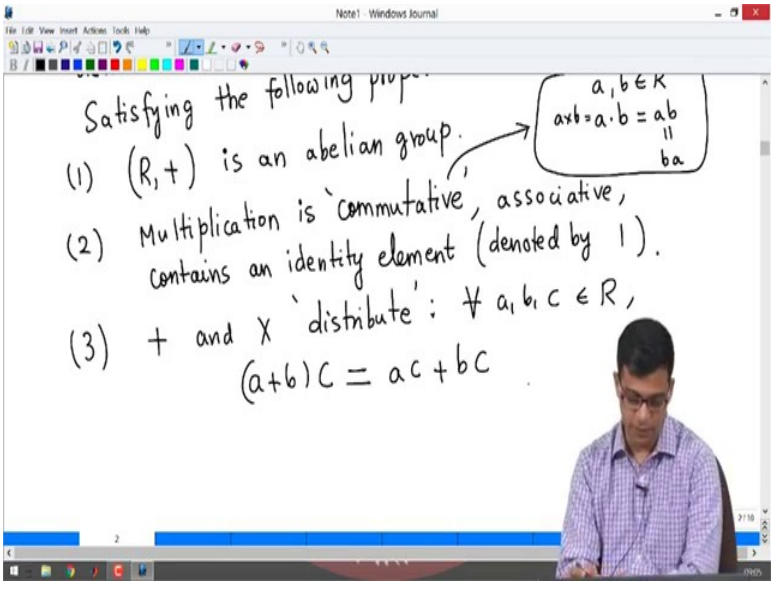
So, that means, what I want to highlight here is that A is not closed under multiplication. So, this fails one of the important properties for a ring that we will define now ok. So, I am just trying to, through these examples indicate to you that being closed under multiplication is a condition that

one has to check in general it does not hold. So now, let us go ahead and define what a ring is. So, we can talk more talk about more examples and properties of them.

So, this course is about rings ok. So, this is the most important example for us. So, a ring we denote rings by symbols R. A ring R is a set with two operations. So, I will write the full definition here. I have already indicated to you what the properties should be a through these examples. So, you will see that they will appear here. A ring R is a set with two operations. So, or binary operations as they are called denoted by plus and times. So, this is these are called addition and multiplication ok.

So, I want to emphasize also that it is a just a convenient way of calling them addition and multiplication. It is not always the addition that we have learned in school. It is not addition of numbers or multiplication of numbers it is an abstract operation ok. So, it is just convenient to call them addition and multiplication.

(Refer Slide Time: 19:53)



Satisfying; so, it has two operations that must satisfy the following properties; what are the properties that these two operations must satisfy? So, as I have already these properties or axioms ok; so, I will write that here properties or axioms. So, there are axioms of rings ok. So, it is a set with two operations denoted a plus and times called addition and multiplication satisfying the following properties or axioms.

First one is that R with addition is an abelian group ok. So, R with addition is an abelian group. This I have mentioned here before. If you just forget about multiplication only look at addition then it just our familiar abelian group. So, with addition it must be an abelian group multiplication need not be with multiplication R need not be a group as we discussed. But, it must still satisfy some conditions. What are they?

Multiplication is commutative. So, I will describe what this is after writing this. Commutative is another word for abelianess. So, what I am saying is that if you multiply two elements of R; so, let us say a and b are so, this I will write here. So, I will just make a box here and write. So, if a and b are in R. So, multiplication is usually denoted by a dot b or just ab for once we start writing more we will write ab. So, this is also a times b. So, this must equal ba. So, remember abelian groups are what we call commutative groups; commutativity is just another word for abelianess.

So, no matter how we multiply the two elements, you get the same answer; ab same as ba. So, multiplication must be commutative. Remember all the examples that we looked at multiplication was commutative because all the examples we looked at were subsets of complex numbers where multiplication is commutative. We also need multiplication to be associative which is a familiar property to you a, b, c if you have two elements you can multiply them by grouping a and b first or grouping b and c first so, either way you get the same answer.

So, it is associative. It contains an identity element denoted by 1. So, again it is convention to denote multiplicative identity just by 1 because in all the examples that we know one is the identity element. Usual number 1 is the identity element. So, it contains an identity element and actually that is all. So, multiplication is commutative, associative contains an identity element.

So, you remember that I have not written the one of the properties for a group namely I did not insist on existence of an inverse. So, I do not need an inverse. Multiplication is not a group operation on the set R. It has all the other properties. It is a binary operation, so, it is closed by definition. It is associative, it contains identity element and actually it has a property that now in general groups need not have namely that it is commutative, but I am not asking for inverses.

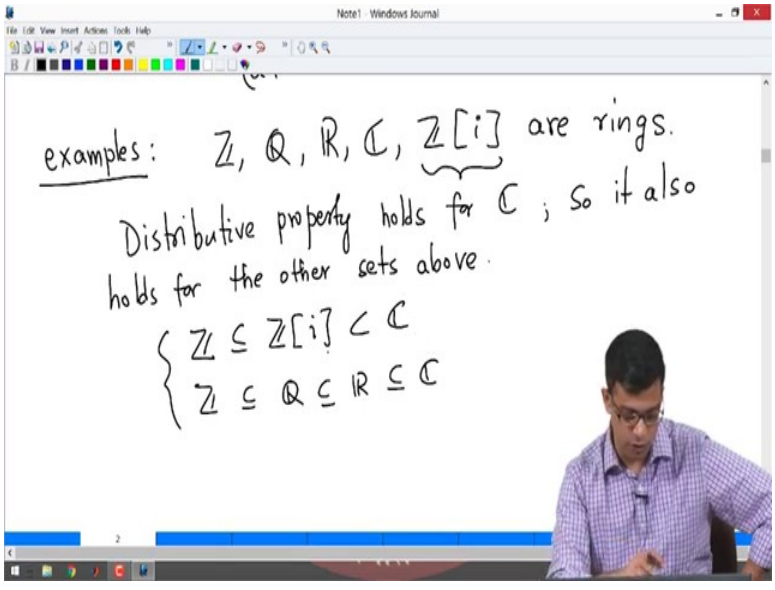
And, the third property is very important. Anytime we have two operations on a set you want these two operations to be well behaved with respect to each other. They should not be completely independent of each other. So, I will say that plus and times distribute. So, let me write distribute. So, this is the usual distributive property of integers or real numbers or complex numbers what is this? For all a, b, c in R a plus b times c; see, remember I have already indicated to you that when I multiply I do not put any symbol between the two elements. I just write ab to denote the multiplication of a and b when you are adding a write a plus b ok.

So, a plus b bracket c means you add a and b first whatever the ring element is you multiply by c that must to equal ac plus bc; that means, you first multiply a and c similarly multiply b and c and add the results. So, ac plus bc must be same as a plus b time c. So, this is a property that is obvious for integers and real numbers and rational numbers, complex numbers that you have seen right, but it is something that we must demand in a ring. It is possible that we can construct operations which is all the properties, but not the distributive property.

So, we need to insists specifically on this property. So, this is a very natural and obvious property in the sets that we are used to, but it is not guaranteed to be true always. So, we need to insist on it. So, these are properties of a ring. So, this is the important example important definition for the whole course.

So, a ring is a set with two operations denoted plus and times that have the properties, with the addition it is just abelian group; multiplication is almost a group except for one property and plus and times have are well behaved in the sense that they satisfy distributive property; a plus b time c is same as ac plus bc.

(Refer Slide Time: 26:11)



So, I want to now revisit the examples that I did in the beginning of the video and now say that Z, Q, R, C, Z[i] are rings. So, now, you might want to go back to the video, see it from the beginning the first part of it when I discussed these examples. In all these examples there are two operations. There you can add two integers, you can multiply two integers; you can add two rational numbers, you can multiply two rational numbers; you can add two real numbers you can multiply. Similarly you can add complex numbers you can multiply complex numbers. In fact, Z, Q, R are all subsets of C.

So, once you know that there is a addition and multiplication on C these sets inherit them. However, you have to check that these sets are closed under that operation. For example, you add two integers you get another integer; you add two rational numbers you get a rational number; you add to real numbers you get a real number; you add two elements of Z[i] you get another element of Z [i]. Similarly, you multiply two elements of Z[i], you get another element of Z[i]; similarly, for Z, Q, R and C.

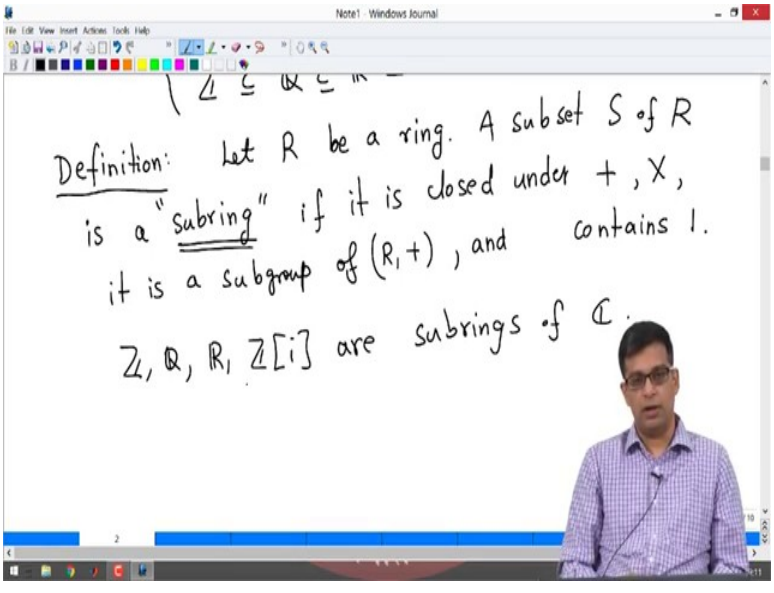
And, with addition these are all abelian groups. I have asserted it is not difficult to check that and with multiplication they are not necessarily groups, but they are the property that they are com-

mutative, they are associative, they contain a identity element in each of these cases, 1 is a identity element and the new property that one can check one can check easily is that distributivity.

So, distributive property holds for C. So, it also holds for the other sets above. Why is that? Remember Z, Q, R, Z[i] are all subsets of C so. In fact, between them there are these following inclusions. So, we have Z inside Z[i] inside C right. Z is certainly contained in Z[i]. You also have the inclusion Z contained in Q contained in R contained in C. Remember Z[i] is not contained in R. So, we have these two inclusions.

So, if the distributive property holds for elements of C, it holds for all the subsets. So, the final definition I want to give in this video and that will allow me to talk about these things here as sub rings of C is the definition of a sub ring. So, once you have a sub ring.

(Refer Slide Time: 28:57)



So, if you recall we have a notion of subgroups of a group. So, what is the subgroup? You start with the group G and a subgroup is just a subset which by itself is a group. So, it has under the same operation that the ambient set group has, it is a group. So, it is closed under that it has identity, it has inverses and it is associative.

So, similarly let R be a ring. A subset S of R; so, we start with a subset is a sub ring. So, it is a sub ring. So, it is a sub object just like sub groups are sub objects of groups. So, is a sub is a sub ring if it is closed under addition and multiplication and it is a and it is. So, it is closed under plus times; it is a subgroup under of. So, it is closed under addition, but more than that it must be a subgroup of the additive group of R and finally, and it and if it and contains 1. So, the multiplicative identity; so, the sub ring is supposed to contain multiplicative identity.

So, a sub ring is a subset if it is closed under addition and multiplication it is a subgroup of the additive group of R and it contains 1 ok. So, finally, I will end the video by saying that Z, Q, R, Z[i] are sub rings of C, right. So, because C is a ring to begin with and these four sets are closed under multiplication and addition. They do form sub groups under addition; they contain 1. So, they are all sub rings of C.

So, I will end the video here and in the next video we will look at more examples of rings. And, we will start looking at properties of rings. Thank you.