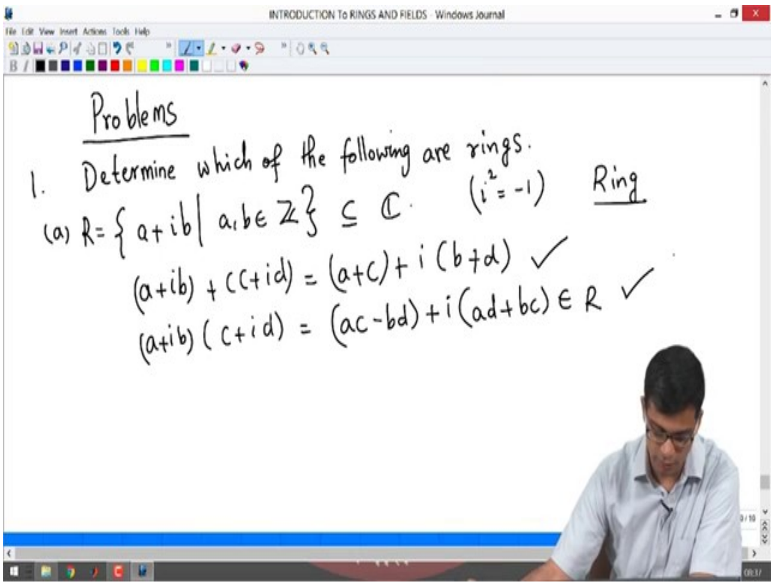
Introduction To Rings And Fields

Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 08
Problems 1

In this video, we are going to do some problems. So, far in the course, we have studied rings, definition of rings, examples of rings, homomorphism of a rings and then I introduce ideals. So, to learn the subject very well, you have to do lots and lots and of problems. So, let us start with some problems today. I will try to explain in detail how to solve these problems. So, this will hopefully help you understand the material much better.

(Refer Slide Time: 00:45)

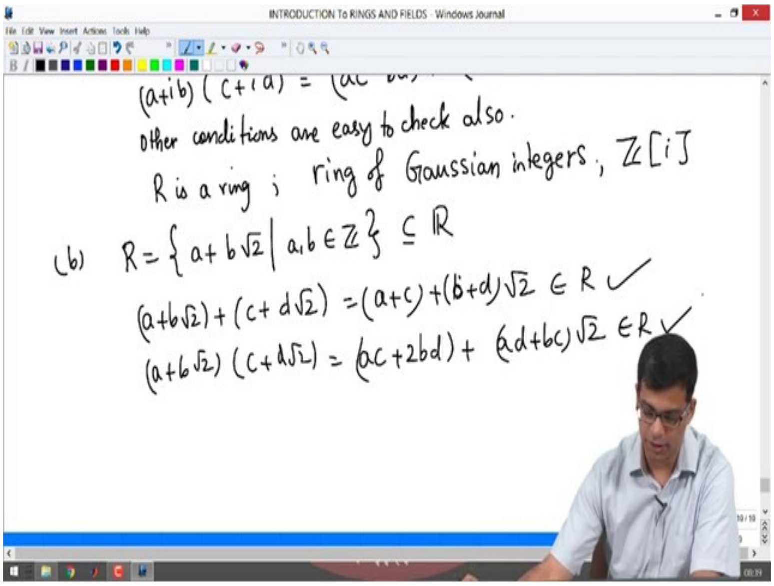


So, today's video is about problems, ok. So, let us start with something about definition of rings. So, let us say the question is determine which of the following are rings, ok. So, we I will give you some sets and we will decide if they are rings or not.

So, let us look at the following set: a plus ib, where a and b are integers. So, actually this is a sub ring of C right. So, i remember is the square root of is the square root of minus 1. So, i is an imaginary complex number. I am looking at a plus ib, where a b are integers So, in fact, this I have already discussed this example before. This is a ring right, and let me quickly recall why and then, we will move on to the other problems. So, here the point is to check that the set is closed under products and sums and there are inverses for addition, there is multiplicative identity and so on.

So, if you obviously add two such things, you get a plus c b plus d right, this is certainly if a b c d are integers, a plus c and b plus c d are also integers. More interestingly, if you take the product of any arbitrary elements, you get a c minus b d plus i times a d plus b c. So, this is also in the set if you call this R R and I will let you to check; I will let you check the other conditions, other conditions are easy to check also. Typically, the key things to check would be product and identity element and inverses.

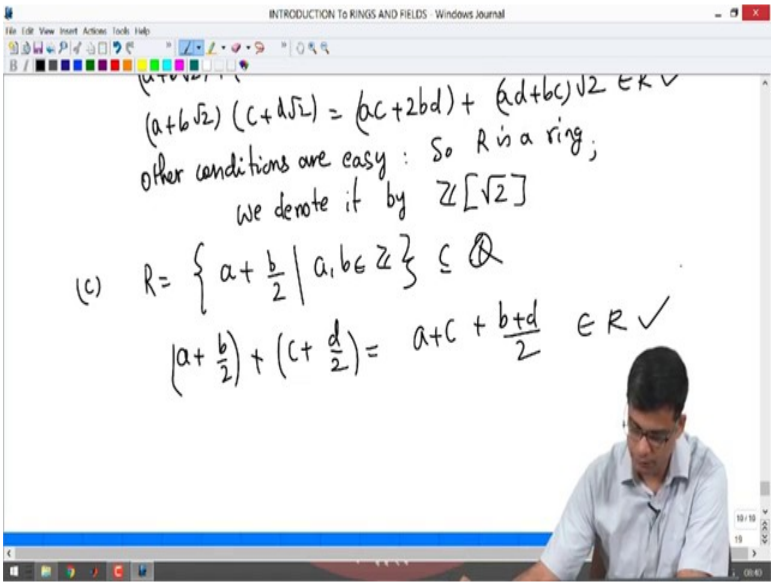
(Refer Slide Time: 02:45)



So, a plus is of course, identity elements is there it is 1. It is of the correct form. So, R is a ring and remember it is called the "Gaussian integers"; ring of Gaussian integers and it is denoted by Z[i]. So, this is a familiar ring to us. We will come back to this ring later in the video today. So, let us look at another ring. I will keep denoting all these by R. So, I think I called yeah so, this is the second ring. So, let us take a plus now instead of i, I am going to take root 2. I will keep a b in Z again ok. So, this is in fact a sub ring of R now right; subset of R, we have to still determine if it is a ring or not.

So, I am taking real numbers of the form a plus b times root 2, where a and b are integers. So, is this a ring? So, again we can check easily that the sum is a plus c plus b plus d root 2; that is no problem right that is in R. So, let us check the product a plus b root 2 times c plus d root 2. So, this would be, now root 2 times root 2 is 2. So, it will be a c plus b d times 2. So, that is a c plus 2 b d plus the root 2 term will be a d plus b c right. This is also in R and the other conditions are also easy ok.

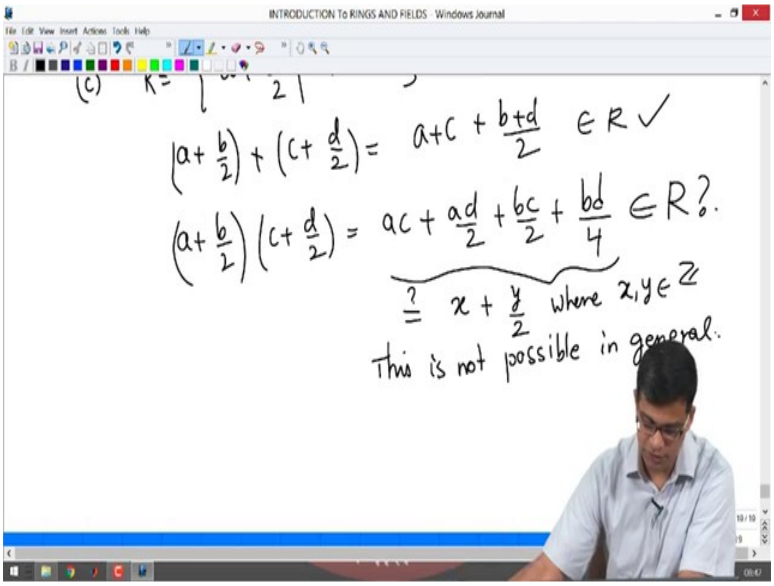
(Refer Slide Time: 04:55)



That I am going to leave for you. The crucial thing as I said is the product. So, R is a ring. We denote it, just following the earlier notation, we put it Z square bracket root 2 ok. So, let us now look at the following. So, here I will replace i and root 2 of the last two examples by 1 by 2. So, let us say a plus b by 2, a and b are in Z ok. So, this is actually inside the rational numbers.

Now, write each of them is a rational number, is this a ring? So, let us do, the sum first. So, this is actually not a problem because it will be a plus c plus b plus d by 2; this is in R. So, this is right. So, this is fine. What about the product ok?

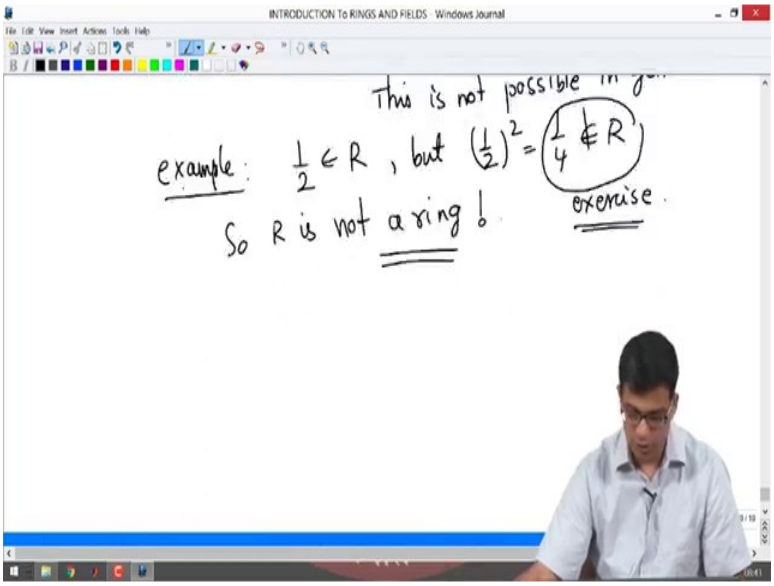
(Refer Slide Time: 06:01)



So, now I actually we will run into some problems because if you multiply these, you get a c ad by 2 bc by 2. So, far no problem, but the next term will be bd by 4 right. Now, is this an element of R? Can you write this as a plus something an integer plus another integer divided by 2? So, can this be written as some x plus y by 2, where so, is this equal to where x and y are integers. You certainly cannot; that is the point.

Because if you write it like this, the denominator will be 2; if you add them and write it as a single rational number; whereas, denominator is 4 provided b and d are not going to cancel 2. So, for example so, this is not possible in general. I will write, this is not possible in general. So, I am going to just illustrate. So, if you say that something does not happen or some property is not satisfied or something is not a ring, you have to give an example to show that the property fails in that particular example.

(Refer Slide Time: 07:25)

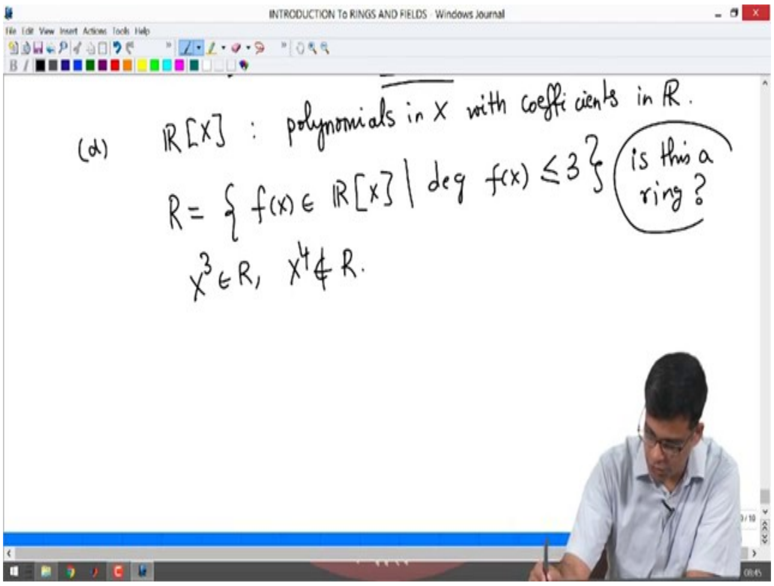


So, example: 1 by 2 is in R right because 1 by 2 is of the form 0 plus 1 by 2, but 1 by 2 squared which is 1 by 4 is not in R right. If R is a ring, 1 by 2 squared is supposed to be inside 1 by is inside on also inside R. But 1 by 4 cannot be written as a plus b by 2 that is very easy to check. 1 by 4 is not in R. So, R is not a ring ok. So, and this particular point I leave for you as an exercise.

It is not difficult to check. Suppose, there is a and b with this property a plus b by 2 is 1 by 4, you cancel, I mean you cross multiply and check that there is a problem because one side will be divisible by 2, one side will be divisible by 4 and there is some contradiction that you will get. So, R is not a ring. So, this example shows that you have to be careful about taking whatever you want. If you take a plus b i in this example or a plus b root 2 in this example, you will be fine; but a plus b by 2 is not going to give you a ring.

The difficulty in this third example was 1 by 2 times 1 by 2 is not inside this set again. Whereas, root 2 times root 2 is also is again in this set; i times i is again in this sets. So, that is the difference in these 3 examples, between these 3 examples. Let us look at another example.

(Refer Slide Time: 09:09)

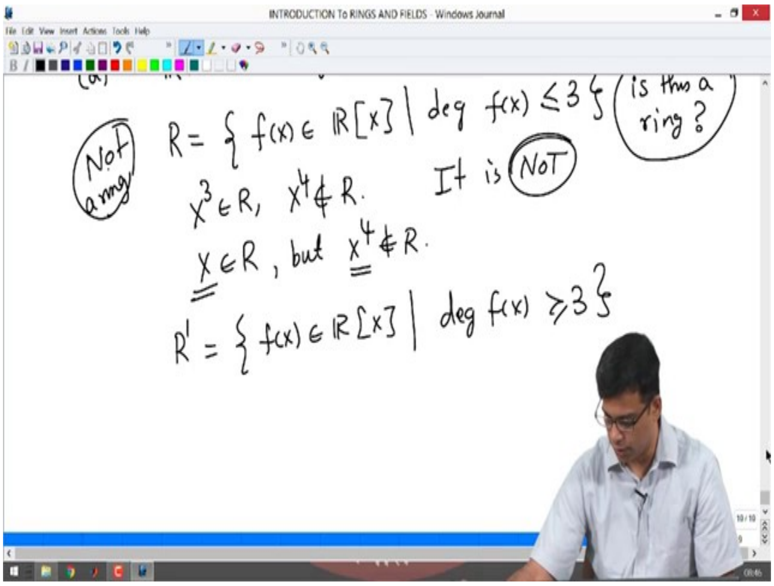


So, if you think about it all of these are actually. So, this question is about if something is a ring, but they can also be considered as questions about sub rings. So, I have given you subsets of well known rings. The first one is a subset of complex numbers and the question is it a sub ring? The answer to that question and the question whether R is a ring or not is the same because a sub ring is simply a ring with the same operations.

So, here we are taking the same operations, as the operations on C. Similarly, here R is a subset of R, it happens to be sub ring of R. Here R is a subset of Q and it is not a sub ring of R. Now, let us look at, let us say polynomial ring right. So, this is polynomials in X with coefficients in R right. So, these are real number polynomials; real polynomials in one variable called X. So, in this let us look at the subset of f of X in R X, degree of f of X is less than or equal to 3 ok. So, here I am taking all polynomials whose degree is at most 3.

For example, X cubed is in R X power 4 is not in R right; so, X power 4 has degree 4; so, it cannot be inside R. Now, is this a ring? That is a question right and you can clearly see that it is not, it is not a ring.

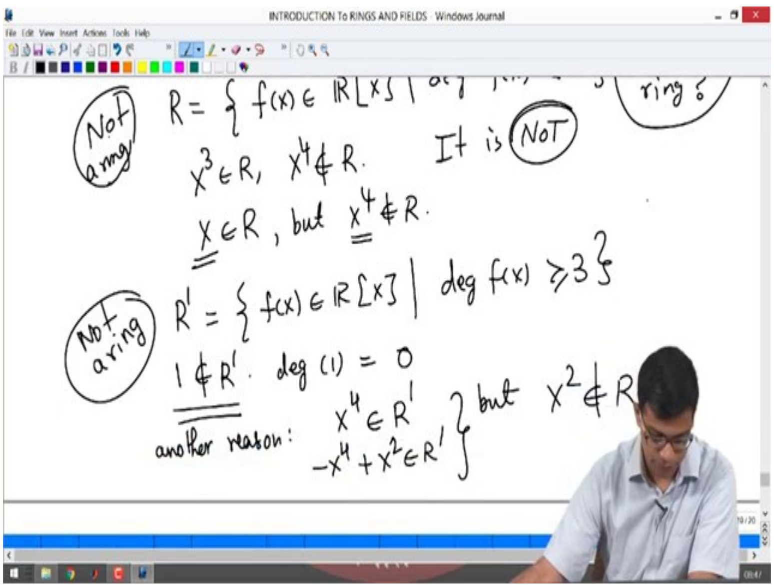
(Refer Slide Time: 10:57)



Why not? Because X is in R, but X power 4 is not in R right. If R is a ring it is supposed to be closed under addition, you have one element if you multiply it with itself 4 times, it is supposed to be inside the set again, but it is not. So, it is not a ring.

So, let us modify this. So, this is not ring. What about I will modify inside still the polynomial ring over real numbers. Let us look at f X inside R X degree of f X is at least 3. So, I am just inverting the inequality. So, here I am taking degree at least 3, is this a ring? I claim this is also not a ring.

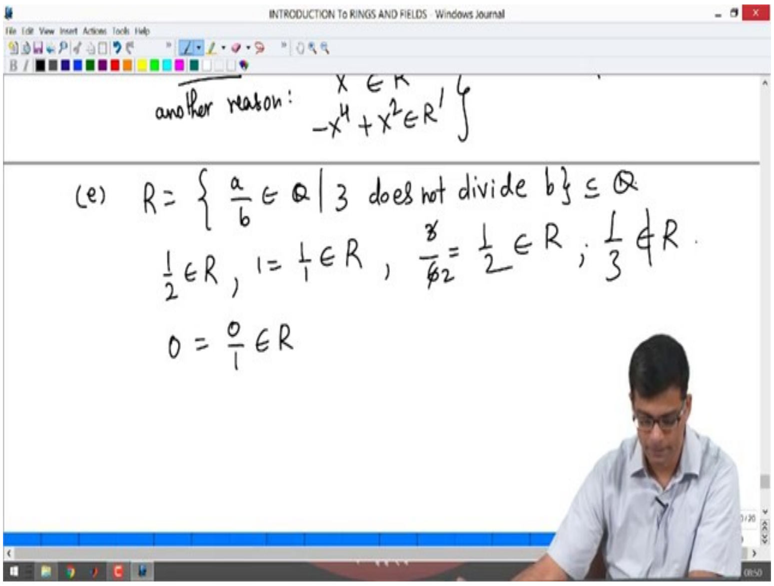
(Refer Slide Time: 12:01)



Why not? There are several reasons why it is not a ring. I will give you two reasons; one is not in R prime right, because what is the degree of 1; remember 1 is the constant polynomial. So, its degree is 0. So, one is not in R prime. Also it is not closed under addition.

Another reason is, if for example, X power 4 is in R prime, X power minus X power 4 plus X squared in R prime, but if you add these two, but what is the sum of these two? If you add these two, you get X square which is not in R right. So, you see that it is not closed under addition also. So, it is not a ring. So, if you just arbitrarily say degree at most something at least something, it is not a ring ok.

(Refer Slide Time: 13:11)



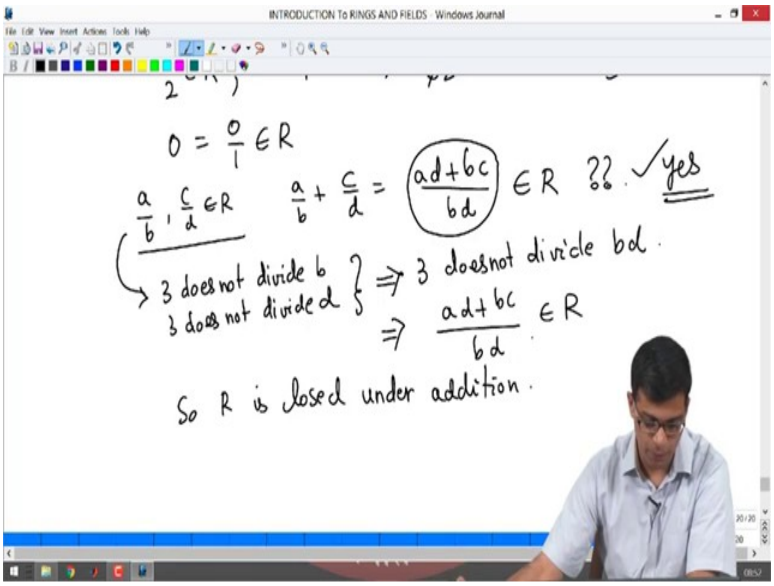
Let us look at two more examples so, e. Let us look at the subset R consisting of rational numbers. So, a and b are integers and a by b is in Q. So, I am already implicitly assuming that a and b have no common factors ok. So, whenever you write a in a element of rational numbers, you cancel all common factors. 3 does not divide let us say the condition is 3 does not divide b. This is the definition of R.

So, for example, 1 by 2 is in R right. 1 is in R because 1 is 1 by 1 right. 1 equals 1 by 1 because 3 does not divide 1. On the other hand, if you take let us say 2 by let us take 3 by 6. Let us take 3 by 6, is it in R? See if you think about it 3 divides 6. So, it looks like it is not in a R, but remember before you can check the whether 3 divides the denominator or not you have to cancel the common factors.

So, you cancel common factors 1 by 2 is what you get and then, 3 does not divide the denominator. So, it is in R. So, you have to check whether 3 divides the denominator or not after you cancel the common factor of numerator and denominator and after you cancel the common factors, if 3 does not divide the denominator, it is there. If 3 divides the denominator it is not there ok.

So, I hope the set is clear. So, the set is this. It has 1 there. It also has 0 right because 0 can be thought of as 0 by 1. So, 0 is also there. Now, is this a ring that is a question. So, to check this let us check actually the conditions for a ring. So, remember again the question whether this is a ring or not is same as the question whether this is a sub ring of Q or not. So, it has 0 and 1.

(Refer Slide Time: 15:23)



Now, let us take two elements in R ok. So, let us consider their sum and see if it is also in R. What is a by b plus c by d? It is a d plus bc divided by bd. Now, is this in R right? We know a by b and c by d in R.

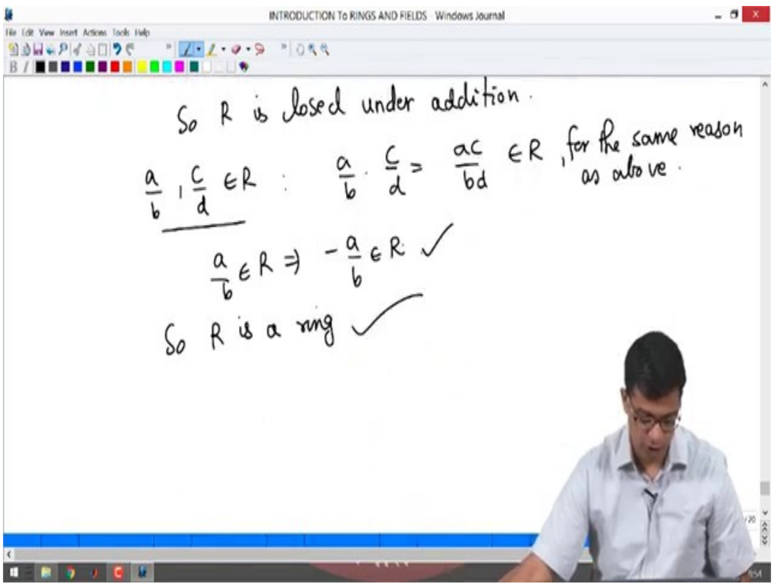
So, now this condition implies 3 does not divide b; 3 does not divide d also by definition right. 3 does not divide b; 3 does not divide d because a by b c by d in their simple forms after cancelling common factors are in R. So, 3 does not divide b and d. But because 3 is a prime number, this implies 3 does not divide the product also. See this is a property of prime numbers. So, if 3 because 3 is a prime number, it does not divide b and d; that means, 3 does not divide b d also.

Now, let us look at the sum. Now, I know that in this form 3 does not divide the denominator, but of course, it is possible that it is not in its simplest form. Meaning there might be common factors between a d plus bc and bd. But does not matter because, if you cancel the common factors, what you will get in the denominator is something which is the divisor of b d. b d itself is not divisible by 3. So, after cancelling common factors, it will remain, it will retain that property right.

So, 3 will not divide whatever is the denominator after you cancel the common factors. So, in other words ad plus bc by bd is in R right. So, the answer to this question is yes ok. Just to recap again 3 does not divide b and d. So, 3 does not divide the product b d. Here 3 is a prime is used and after cancelling common factors of this quotient, a d plus bc by bd whatever is the new denominator being a factor of b d will, will continue to be not divisible by 3 ok.

So, this is not a multiple of 3. So, a by b plus c by d is in R that is good. So, R is closed in closed under the addition. R is closed under addition. So, now, let us look at product, is it closed under multiplication?

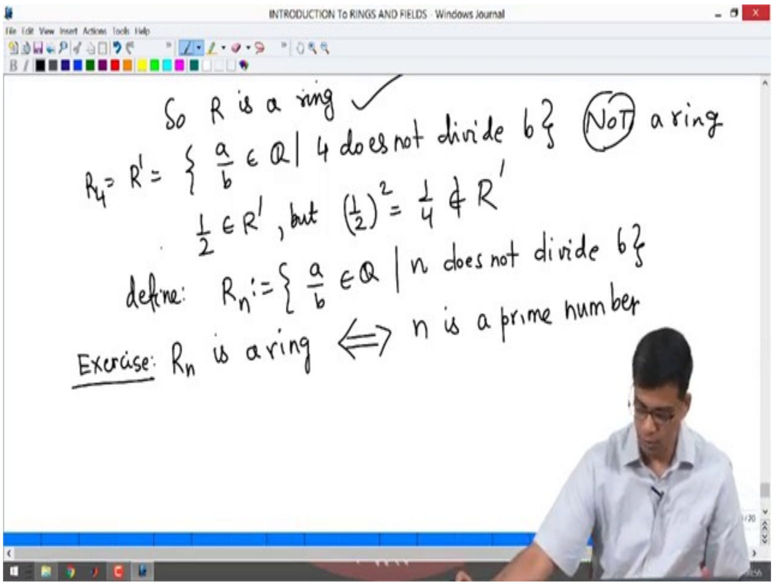
(Refer Slide Time: 18:03)



So, let us again take a by b c by d in R. Now, let us take a by b times c by d. So, this is a c by bd; for the same reason as before. So, here also denominator is bd which is not divisible by 3 and after cancelling common factors what you get is still not divisible by 3. So, ac by bd is in R. So, once you check these conditions of course, if a by b is in R minus a by b is also in R ok. So, that is also seen by taking the, using the closer under multiplication property because minus 1 is there, the product is there minus 1 time say a by b which is minus a b is in R.

So, we have checked all the condition; remember associativity of addition, multiplication, distributive property of addition, multiplication are automatically true because this is sitting inside Q which has all the required properties. So, R is a ring right. So, R is a ring. So, I hope this example is clear and to just to clarify this a little more, let us modify this slightly.

(Refer Slide Time: 19:19)

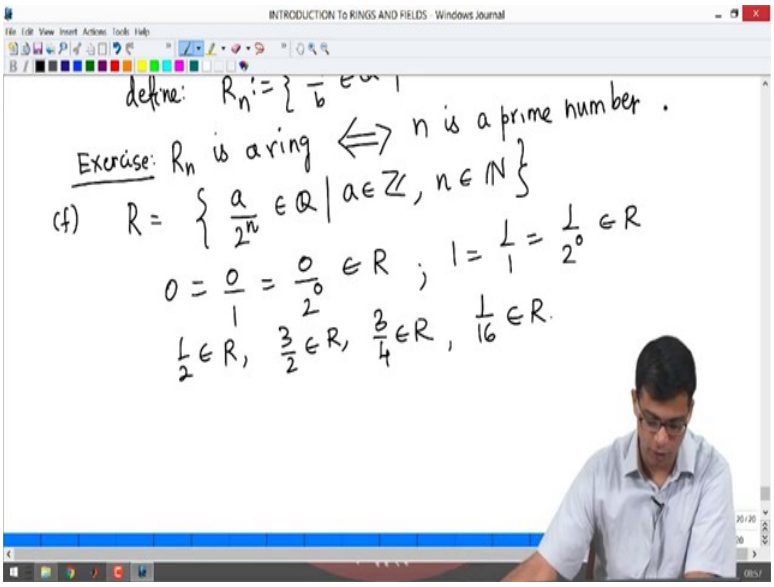


And I will call this R prime. So, I will take as before a by b in Q, but instead of saying 3 does not divide b, I will say 4 does not divide b ok. So, here I will say 4 does not divide b after you cancel common factors. So, this is not a ring I claim because 1 by 2 is in R prime right, in its simplest form which 1 by 2 is in already simplest form, 4 does not divide 2. So, 1 by 2 is R prime. But, if you take 1 by 2 squared you get 1 by 4 and 1 by 2 is also in its simplest form and 4 does divide R prime. So, it is not sorry 4 does divide 4. So, 1 by 4 is not in R prime.

So, R prime is not a ring say again because I said 3 does not divide b I got a ring where and because 3 is a prime. So, I will end this by simply saying define it is a R sub p to be a b a by b in Q, p does not divide b ok. So, here p is an integer. So, I claim that actually let us write it like R n n sorry p b is here this is n. So, let us define R n to be all rational numbers, where n does not divide b. So, here R n is a ring, I claim if and only if n is a prime number. You can prove this as an exercise. Using the ideas in this problem, you can prove this. I have given you one example, two examples of R n when n equal to 3 and 4; so R prime is R 4 right in my notation now and here R is R 3.

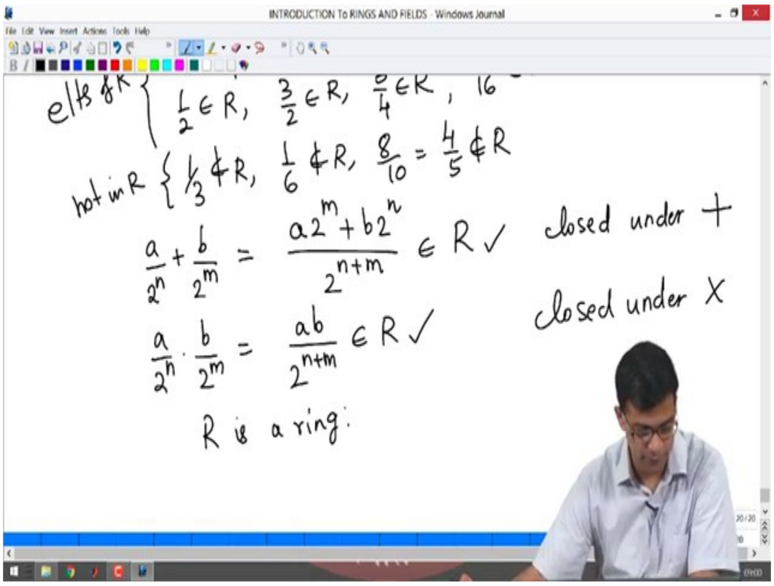
So, R 3 was a ring, we checked. R 4 was not a ring, we checked. So now, I am asking you to prove the general statement R n is a ring if and only if n is a prime number. So, exactly the same idea if n is not a prime number, it is a product of 2 numbers and then, you can use what I have done here for 1 by 2 to show that R n is not a ring. If n is a prime number, use the problem about R 3 to prove this. So, this is a good exercise for you to do ok. So, let us do one more final thing about whether something is a ring or not. So, this is f.

(Refer Slide Time: 22:11)



So, let us look at R now to be rational numbers of this form. So, I am taking rational numbers. So, a is any integer and n is a natural number. So, I am taking a rational numbers of the form a by 2 power n. So, denominator must be a power of 2 in other words. So, for example, 0 which is 0 by 1 which is 0 by 2 power 0 is in R. Similarly, 1 which is 1 by 1 which is 1 by 2 power 0 is in R. 1 by 2 is of course, in R right; 3 by 2 is also in R; 3 by 4 is in R and 1 by 16 is in R. So, these are all elements of R.

(Refer Slide Time: 23:13)



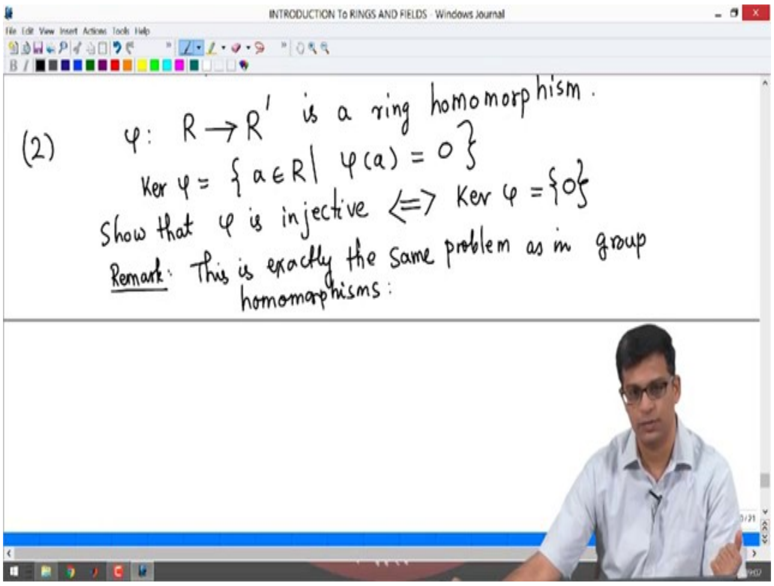
On other hand, 1 by 3 is not in R; 1 by 6 is not in R right; 8 by 10 is not in R and so on. So, these are elements of R; these are not in R. So, again the test is very clear. To be in R, in the simplest form. So, of course, again I have to simplify. So, 8 by 10; so, this is let us cancel the common factors here. So, you had 4 by 5 right.

So, after you cancel the common factors, what remains; denominator of what remains should be a power of 2. So, is this a ring? So, that is the question. Is this a ring? So, we have already checked that 1 is there and 0 is there. So, let us check closure under addition and multiplication. So, you have a by 2 power of n. Let us say and b by 2 power m. If you take the product, it will be a times 2 power m plus b times 2 power n divided by 2 power m plus n plus m right because that is 2 power n times 2 power m.

Now, is that in the correct form? Yes, it is again as before it possible that this is not in the simplest form, but you can cancel the common factors. Only factor of denominator is 2. If you cancel some of those factors, you will remain; then what remains will be still of the form 2 power something. Similarly, a by 2 power n times b by 2 power m will be a b by power 2 power n plus m. In this case, it is actually of the, in the simplest form because a and b are odd because these two are in simplest form.

So, this is also anyway that is not important. The denominator is a power of 2 and even if you have to cancel, what remains will be a power of 2. So, this is in R. So, this is closed under addition; closed under addition; closed under multiplication. So, R is a ring. So, I will leave the verification for you. R is a ring. So, these are some of the examples, I wanted to do which show that you have how to verify if a few given sets are rings or not ok. So now, to continue with the next problem, let us look at something about ideals and this is something that is related to, so, this is the second problem.

(Refer Slide Time: 25:55)

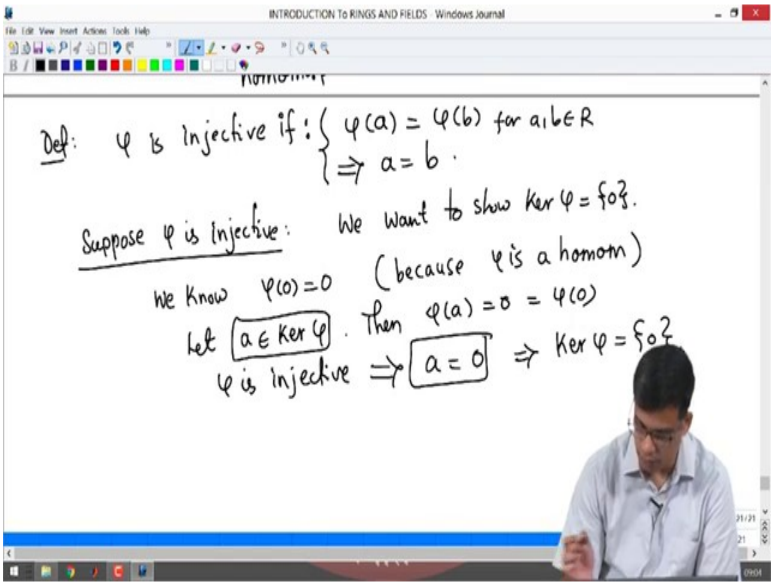


So, this is something related to homomorphisms and ideals. So, recall what is a group ring homomorphism. Let us say R to R prime is a ring homomorphism. So, let us say phi from R to R prime is a ring homomorphism and recall what is a kernel? Kernel is the set of all elements in R which map to the 0 element of R prime right. So, this is the definition of the kernel. So, and we know that it is what we call in ideal.

So, the problem here is show that phi is injective if and only if kernel phi is 0 ok. So, this I will remind you if you have taken a course in group theory. This is exactly so this is a remark for you; this is exactly the same. This is exactly the same problem as in group homomorphisms ok. So, this is exactly the same problem has been group homomorphisms. So, what I mean is so let me write that here.

If you have a group homomorphism that also has a notion of a ring, kernel, the group homomorphism happens to be a injective map if and only if the kernel is 0. And, the reason that is exactly the same is because whether something is in the kernel or not is really a group theoretic issue here. Because it has nothing to do with the additive multiplication on R, it as everything to do with addition in R and under addition R is a group and whether phi injective or not is purely a set theoretic property. So, let me quickly solve this problem.

(Refer Slide Time: 28:15)

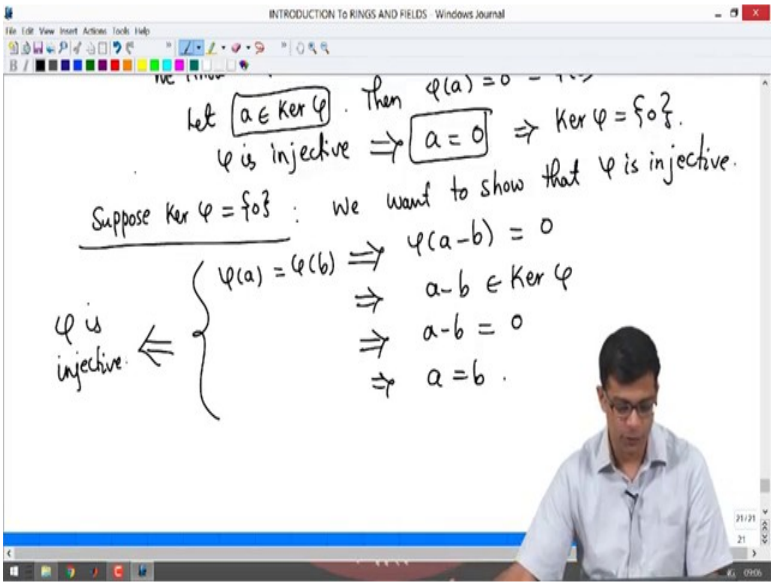


So, what is injective mean, so I should probably remind you what is injective mean. Phi is injective, definition in case you forgot this: phi is injective if two distinct elements go to two distinct elements. So, if phi of a is equal to phi of b for a b in R implies, right. So, phi is injective if two elements of R map to the same elements phi of a is equal to phi of b; those two elements are equal to begin with ok.

So, let us prove now. Suppose, phi is injective; we want to show kernel phi is 0 ok. So, suppose so first of all we know that phi of 0 is 0 because ok. So, I will simply write phi is a homomorphism right. It is a ring homeomorphism; in particular, it is a group homomorphism and it sends the additive identity to additive identity.

Now, suppose phi, a is in the kernel of phi; then phi of a is 0, but 0 is also phi of 0 as I noted there. But, now since phi is injective which is the hypothesis and I recalled for you the definition of injective maps phi of a is equal to phi of 0; that means, a equal to 0. That means, the only element of kernel phi is the 0 element right. So, I have taken an arbitrary element of kernel phi and I have concluded that a is 0. So that means, kernel phi is equal to 0. Certainly 0 is in the kernel because phi of 0 is 0. So, kernel is just the 0 element, there is nothing else.

(Refer Slide Time: 30:19)



So, now suppose kernel phi is 0. We want to show that phi is injective, ok. So, this is also straight forward using the same ideas as before. Suppose we want to show phi injective. So, assume or let phi of a equals phi of b right. So, the definition of injectivity is if phi of a is equal to phi of b, we want to show a is equal to b. But if phi of a is equal to phi of b.

So, I will write it like this, by definition of ring homomorphism, I have this phi of a minus b is equal to 0 because phi of a minus b phi of a minus phi of b which is 0. That means, a minus b is in kernel phi, which is again the definition of the kernel. If a minus b is in the kernel, I have assumed kernel is just the 0 element. So, a minus b is equal to 0; that means, a minus b equal to 0. That means, a equal to b. So, this whole thing implies phi is injective.

So, the problem is solved. I will only make the final remark that nowhere in this proof we have used multiplication on R. The fact that R is a ring which has multiplication is completely irrelevant for this problem. We only needed additive structure. So, we have shown that a ring homomorphism is injective if and only if its kernel is 0. So, we will use this problem in some special cases in next set of problems. So, I will end this video here today.

Thank you.