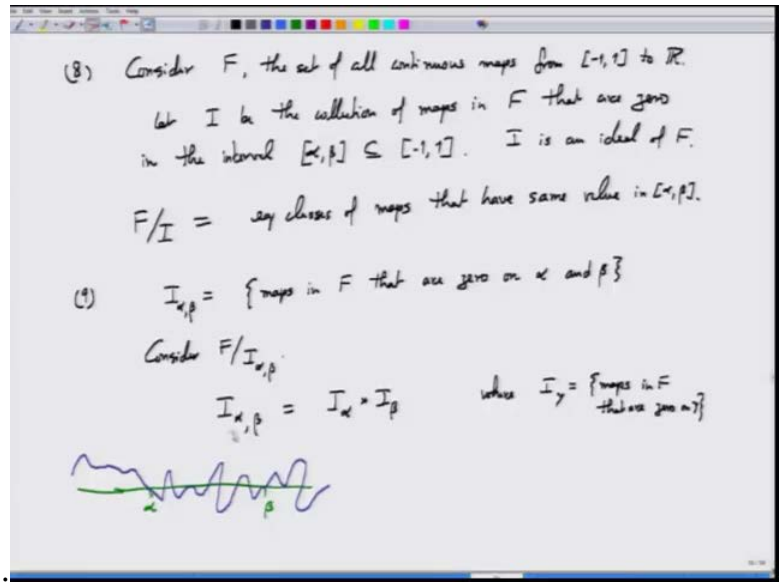
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

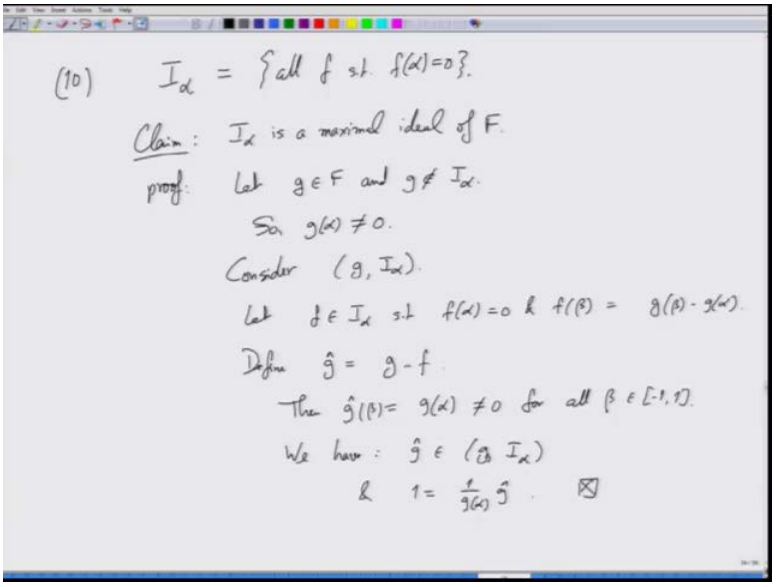
Lecture – 14
Fields

(Refer Slide Time: 00:18)



So we were at this point last time, where the ideal I alpha beta were defined as the product of I alpha and I beta, and rather I alpha, we get proved to the product of I alpha and I beta and at given this is an exercise.

(Refer Slide Time: 00:40)



Now, let us look at as our next example - I alpha, which is all functions that vanish on alpha, this is an ideal. And I claim that this is a maximal ideal of this ring F. We will see the proof of this. So, what do you need to show to conclude that I alpha is the maximal ideal, and any ideal that contains properly I alpha is the entire ring which means it contains one as well the identity.

Students: (Refer Time: 01:48).

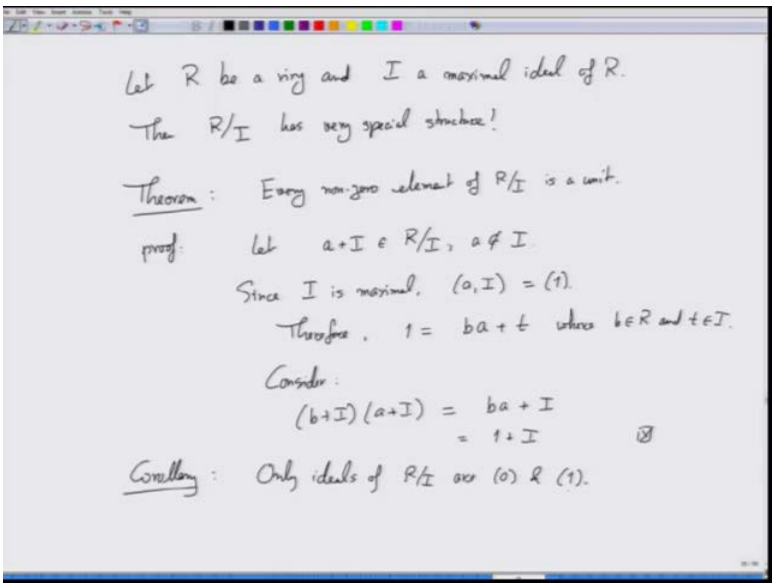
No, it is contained in I alpha; I alpha comma beta is actually contain I alpha intersection I beta. So, it is a very simple proof, but it is a instructive proof. So, let say let some g be in G, and g naught in I alpha which means a g of alpha is not zero. Now, consider this ideal. So, this is an ideal which certainly contains I alpha, and it contains this one extra function g, and whatever is the ideal generated by that.

Now let us pick up a n f in I alpha such that f of alpha is 0 and f of beta is g beta minus g alpha. In this ideal, as a g hat to be g minus f that is simple calculation that g hat of beta is a fixed number, which is nonzero, everywhere in the interval. So, g hat beta or g hat in the function that is not zero anywhere in the interval, and actually is the fixed value, so I can define it has g hat is in this ideal by its definition is g minus f. And g hat is simply

the well all not quite g hat, but 1 is 1 over g alpha times g hat. So, this shows that the I alpha is the maximal ideal, so there is a nice connection that all the function that the ideal of all function that vanish on one point is a maximal ideal, and we will extend this a little later.

But for now let us stop here with example, and let us look at two special kinds of questions particularly they start with maximal ideal.

(Refer Slide Time: 04:53)



And let us start with an (Refer Time: 04:53). And then you look at the quotient R by I. This quotient ring has very special structure, because I is a maximal ideal. And this special structure is that every nonzero element of this ring is a unit; typically in a ring units are few most of the example we have seen most of the element are non units, but this is a ring where every nonzero element is a unit. How do you prove this, let us pick up an element, let a plus I be in R quotient with I. This is a typical element. So, this, a plus I is a non-zero element in this quotient ring. The element, the I is that corresponds to the 0 element.

Now, I is a maximal ideal element in the ring R, and a is not in I, which means there if you add a to the ideal I, and look at the bigger ideal - this ideal this is the whole ring in

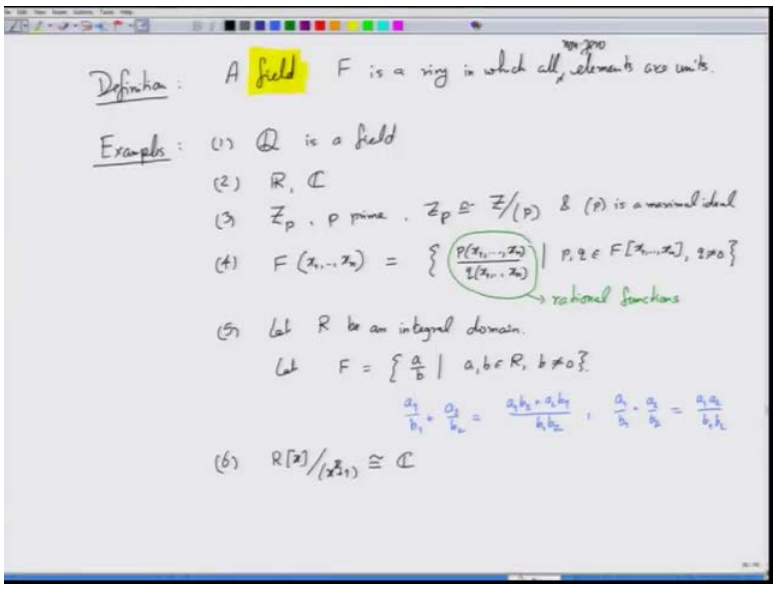
which means in particular 1 equals some b times a plus t, these two rings are this ideals are same that means, the element one which is in this ideal is also in this ideal. The element one being in this ideal simply means that it is of this form b times a plus some t being in the ideal I.

So, now, consider this product. This is an element of the quotient ring b plus I, a plus I is an element of the quotient ring what is their product, it is b a plus I. What is b a plus I, look at this equation, this is an element of b a plus I, so that means, one is in this. It is 1 plus I it is a simple proof, but it is making use of the properties of this quotient ring that if two elements differ by the any element in the ideal I then they belong to the same equivalence class.

So, here 1 and b a differ by t which is an ideal I, so the equivalence class b a plus I and 1 plus I are the same. This is the identity in the quotient ring. So, this is all we need to prove that a plus I is a unit because there is an element b plus I was a product with this is 1 plus I. This is (Refer Time: 09:44) while constructive argument well it would not necessarily a, it will be can be formulated in terms of constructive argument, but then we will have to go into this the generators of the ideal itself I itself. And how do you construct the general element of that ideal, because then you use the generators of the ideal I and then (Refer Time: 10:13) it depends on the ring R.

How complex is this ring. If the ring r is simple, then finding inverse is easy; if it is not simple then it is going to be more difficult. So, this proof generalizes to all rings it does not matter what ring is in and why they existential R (Refer Time: 10:36) better. This also means there in this quotient ring, there are no non-trivial ideals. Every ring has this two ideals the ideal was zero which is just contains zero, and the ideal one which contains the whole ring. This quotient ring has no other ideal, because any other element any non zero element if it is there in the ideal then since it is a unit then entire ring will be in that ideal, so there the ideal is one.

(Refer Slide Time: 11:29)



Now these are very special kind of rings and these are called fields. Examples, set of rational numbers is a field, all non-zero elements being units is equivalent to saying that division is possible in the ring. You can divide by itself, because if you have an element a then 1 by a is also in the ring, because the since a is unit, so there is a b is present b times a is 1, so b is 1 by a. So, if you have to divide by a, you simply multiply by 1 by a. Hence, so the division complete division is possible, and we have already know that in rational complete division is possible except by division by 0 is not possible, division by any non-zero element is possible; other examples.

Student: (Refer Time: 13:18).

Real numbers complex numbers absolutely real numbers, complex numbers these already. Any other example you can Z is not a field Z p is a (Refer Time: 13:29) yes Z p is a (Refer Time: 13:30) where p is prime. Why Z p a field.

Student: Every element maybe (Refer Time: 13:42) one more.

You can note that, but we invoke that it is in previous theorem also.

Student: P primary, it is maximal ideal.

p is a maximal ideal see Z p is isometric to Z quotient with the ideal generated by prime number p. Now this is a maximal ideal here p is prime, and so the quotient of the ring Z with this is field; any other example.

Student: (Refer Time: 14:25).

They do not form the field; not discoverative.

Student: (Refer Time: 14:39)

If you add two non singular matrices, the result may not be non singular, but then it is a not field, test we ring first. There is interesting polynomials, polynomials would not be a field, but a quotient of two polynomials, recollect all, which are called rational functions, they form a field. Yes, so for example, let me write that this is just for example, you can take any field F, and you take this stands for all functions of this form.

So, take polynomials p and q in this ring, this ring you know F bracket x 1 to x n this is the ring of polynomials, coefficients coming from the field F and the (Refer Time: 16:03) was being a x 1 to x n. Take two polynomials p and q and take their quotient p by q, q should not be 0, this is a field. Why, this is a ring because you can add two such functions then you get a function anywhere, it is committed a group under addition, you can multiply also. And there is a multiplicative inverse here p by q is multiplicative inverse is q by p, as long as this is not a zero polynomial; p should not be, otherwise a 0 in a where p is 0, and all cause at that is on the field f anywhere.

Student: (Refer Time: 16:52).

Then it would not be, if there so there ring R and there is a problem yes. And that we have taking care of by it is a very trivially this is exactly the same way we go from integers to rational numbers. It is a same process, so these are the called as somebody

pointed out these are called rational functions, ratio of two polynomial.

Student: (Refer Time: 16:52).

Very good question that he said is there a ring whose maximum and their maximal ideal so that is the quotient of that that is the very good question. And the answer is in one sense it is trivial, but if you do not get into triviality then it is not always true. For example, in rational, we cannot always say that the rationals we can view as a ring and the maximal ideal in the ring quotient that maximal ideal is (Refer Time: 18:19).

Student: (Refer Time: 18:24).

Well, that is trivial value because we are starting with q that is why that is what I wanted to eliminate, otherwise q x quotient with maximal ideal generated by x of course, that is q (Refer Time: 18:44) we always define q. In fact, there are three ways of creating fields from x, one is take a maximal ideal quotient that gives you a field. The other two ways they are specialized, they do not hold for all rings. This q and F the fourth example they are constructed using that way and that is through the following.

Suppose we start with an integral domain as a ring, then we let F be a by b a, b in R b not zero. So, just take the quotient of pairs of elements, so f as a by b a, b in R, this is a field. These verify the addistitative multiplicativity a 1 by b 1 plus a 2 by b 2 is this, this is an element of the ring b 1, b 2 is an element of the ring. And since I is an integral domain b 1 b 2 is not 0, since we started with b 1 and b 2 being nonzero.

Similarly a 1 by b 1 times a 2 by b 2 is a 1 a 2 by b 1 b 2, again b 1 b 2 is not zero, so it is an element of F and all other properties follow pretty straight forwarded way. This is the only two places where I need the fact that R is an integral domain. And this is exactly how we formed rationals and this field of rational functions. Z is an integral domain, F bracket x 1 to x n is also an integral domain and there is why we need to do this. And the third way is to extend a field, look at the c; we derive the motivation from there. How do you create c?

Student: pi n (Refer Time: 21:43) polynomial.

Although it is in a sense it is falls back to that quotienting, so it is basically R x quotiented with x square plus 1 this is isomer to c. So, this way actually is the same, one could say that as quotient ring. How do you create r that is trickier, how do you create r, how do you create r?

Student: (Refer Time: 22:21).

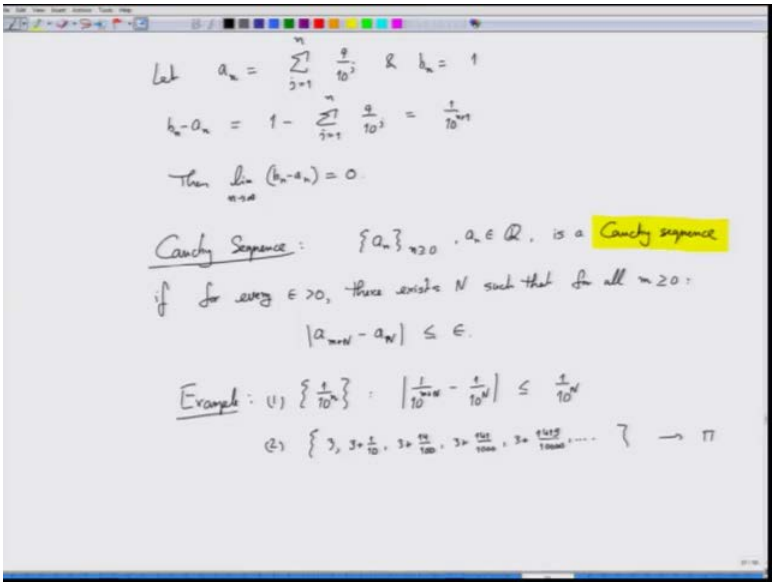
How do you hear, so basically we start with as a q and we want to create R from q. If you can do that then we will have some I have a complete picture that fundamentally we having integers. And then from starting with those integers, we are now creating by certain operations all of this q is a sector fractional field and then from q we can go to R, R go to c, why this quotient ring yeah that is it, how do we do that. In fact, what are real number, do any of you know the definition of real number?

Student: (Refer Time: 23:14).

But there is a slight problem with that definition. So, for example, the number 0.999999 forever and 1.00000 forever are these distinct numbers, they are distinct, why.

Student: (Refer Time: 16:52).

(Refer Slide Time: 24:02)



Let us look at that fine; let us look at that. Let us say a n be summation j from 1 to n, so b n is just number 1, this represents that 1 or 1.0 all zeros, a n is 0.999 n times n of n nines are there, that is what this definition is. So, we have two infinite sequences, a 1, a 2, a 3 up to all the way this is the infinite sequences, and b 1, b 2 to be infinite, these are infinite sequence. What is a n minus b n, or b n minus a n, let say, no, sorry should have written j here n 1 minus 9 by 10 is 1 by 10, 1 minus 0.99 is 0.01, 1 minus 0.999 is 0.001, so this is the general form of the difference. Then what is the limit of the difference as the n tends to infinity. In fact, I do not even need to take the absolute value because this is always positive, so I can simply write this as limit of the difference.

Student: (Refer Time: 26:21).

Yes, that is another trick, so x is 1 that is another, so these two are the same number, because this number a n is an approximation of the number we had really are looking at, 0.9999 forever. So, to construct that number, I have to look at in going to infinity and when i am goes to infinity this difference is 0. So, there is this confusion that in the sense that we have this decimal notation of real numbers thus lists all the numbers, but it seems to be listing a number more than once.

So, then we have to worry about a, which numbers are equal in this sequence, which are not equal and only the non-equal numbers are the once that we want it is not a very neat representation of real numbers. Although we use it very all the time, but if we think about it we only uses rational numbers, we never use real numbers. So, what if you really want real numbers, then this representation is not a very good one, so the defining real numbers in the sense in this way it is also not very appropriate.

Say in fact, this problem troubled the mathematicians of no ancient times 17 and 18 century, because that is when they realized that real numbers exist that is irrational numbers. So firstly, they were the belief for that there only a rational numbers, then it was pointed out that square root 2 is not a rational number. You can prove that simple very easily and that was considered as a huge wrong because until then odd, even thought about this. And then it is people started, the square root 2 certainly is a number so what kind of number it is like, when they irrational number and real numbers were introduced; but then, we one needed a very clean definition of real number and that was given by Cauchy.

So, this we are got into this although I did not want to let me complete this story. What Cauchy did was he defined Cauchy sequences. It is a sequence of infinitely many rational numbers, slightly complicated looking definition. But if you think about it the meaning will become very clear. This infinite sequence of rational numbers a n is called a Cauchy sequence, if for every epsilon greater than 0, no matter how small epsilon is.

There exist a large enough N, capital N which I am calling so in that I am dropping essentially the first capital N minus 1 numbers from this sequence, and considering the numbers after that the difference between a capital N and a n plus capital N for any n is like at most epsilon. Which essentially saying that if you first drop the first capital N minus 1 numbers look at the difference of any pair of numbers in the remaining sequence that difference is very, very small it is smaller than an epsilon. And this epsilon we can make as small as follows. Any small epsilon, there will be a large enough n, beyond which the difference between any pair of numbers is less than epsilon.

So, which is saying essentially one of the conclusion of this is there if you look at the

limit of this sequence, there it is informally at least converging to some number, because all the numbers become closer and closer to each other, and so it is starts converging to a particular number. And the number it converges to be a real number. So, an example of this is just this for example, this 1 by 10 to the power n, this is a Cauchy sequence. Why, pick any epsilon, and then the difference of beyond let say difference of 1 by 10 to the m plus N 10 to the N, this difference in absolute value is at most, how much, it 1 by 10 power N. So, for any epsilon, I can always choose a large enough n capital N, so that the difference is less in epsilon. What does this sequence converts to 0, it is going towards 0.

On the other hand, if you have this Cauchy sequence, let say so if you have this sequence is this look familiar. Firstly, this would be a Cauchy sequence. I am not essentially I am in the numerator here is the decimal expansion of pi, so this is 3, 3.1, 3.14, 3.141, 3.1415 whatever is the expansion of pi is. The difference between any two after beyond a point the numbers is very tiny, it generally goes to become smaller and smaller, and this converges to pi that is why that is why the expansion will be infinitely 0. We have infinitely for every successive digit in the decimal expansion of pi will have one number here; each one of this number is the rational number, and it is getting closer and closer to the number pi.

Student: (Refer Time: 35:24).

Which definition?

Student: (Refer Time: 35:29).

Yes, yes that problem exist here also, yes, but it is if you have to tends also say which we have to classify that which of these numbers are not unique, and they are equal, so we have to create equivalence classes of these real numbers, which corresponds to a unique number. So, we will have we will need a way of clearly describing you know this form after all when we says real numbers is a field, you want one element to the represent why a unique one representation to the present unique element. Whereas, in this representation there are not uniqueness property is not there.

So of course, we understand what real numbers are if there is a real line and every number in there is a real number what that is an informal understanding. And you want to formally define it; we would like to do it in a very precise way which gives a unique representation for every number. There is lacking in that representation, so that is what Cauchy did.

I will continue with this tomorrow.