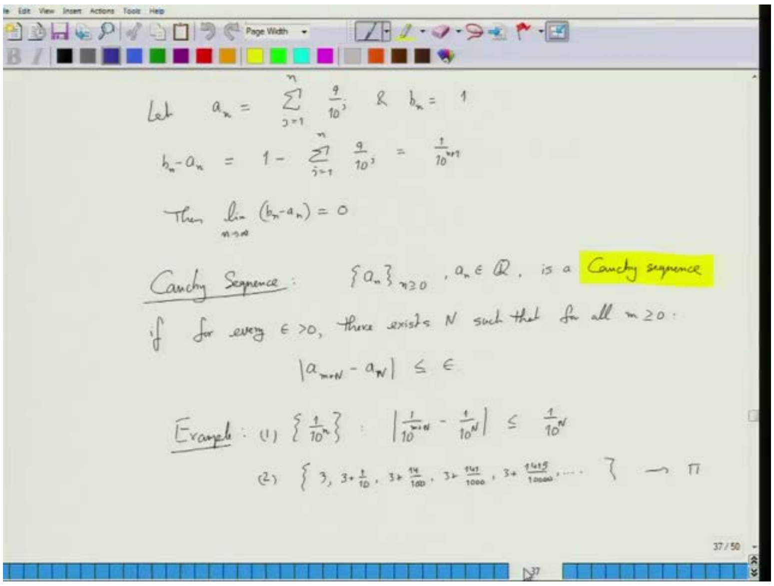
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture – 15
Cauchy sequences and real numbers

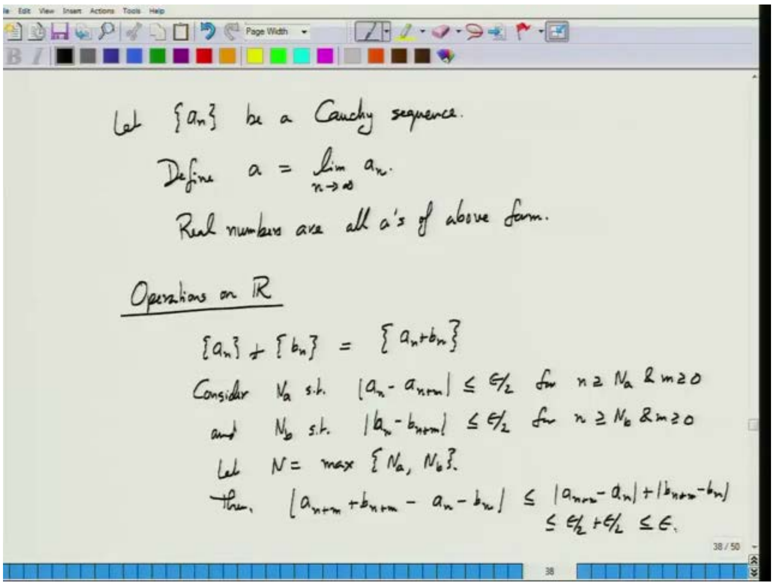
Yesterday, we defined Cauchy sequences.

(Refer Slide Time: 00:18)



And, I am going to use this to define real numbers.

(Refer Slide Time: 00:33)



So, any Cauchy sequence by its definition in the limit. So, let give this, take the limit and tends to infinity of the numbers, which are rational numbers a n, in the sequence. This limit exists by virtue of the fact that successive numbers in the sequence are closer and closer to each other.

So, it is going to converge to a number, and that number is I am defining to be a. And, one can show again by using the property that its successive numbers are closer and closer to each other. That this limit is unique; that is, if there are two numbers with the same limit, then their difference will go to 0. And, this number a is we call the real number.

Student: (Refer Time: 01:49).

OK.

Student: (Refer Time: 01:52).

Some of it is then converged. Where if you just look at the harmonic, a n is one by n that take the limit; it goes to 0.

Student: Term goes to 0.

Term goes to 0. So, that limit of harmonic series kind of Cauchy sequence is 0. So, what is the advantage of defining a real number in this way? One thing, we can say that are all real number can be expressed in this fashion. And everything that is expressed in this fashion is a real number. Let us that intuitive motion of real number does match with this definition.

But, what is clear is that there are multiple Cauchy sequences converging to the same real number like one by n; that limit converges to 0 one by n square; limit converges to 0 one by n cube converge to 0. So, that is not really solving the problem that I stated earlier. But, it solves one or two other problems about real numbers, which I am fairly sure you did not pay lot of attention to whenever you came across real numbers.

So, let me ask you. If I give you two real numbers, can you add them? If yes, then how? Can you add two real numbers? How? You know, how to start with? Where is the right most? There is no right most. It is forever for infinitely low sequence.

Student: (Refer Time: 03:53).

It is not computationally; I am not asking to design an algorithm. Of course, you cannot design an algorithm. But, if it is conceptually, can you figure out a way of writing them?

Student: (Refer Time: 04:13).

OK.

Student: (Refer Time: 04:25).

That you can write. Sure. Given real number, let say this kind of infinite size inputs can be viewed as following that you are given access to a black box, where if you put number m, you get the m th digit of that real number; m th digit after the decimal point, let say. So, if you are given such an access to two real numbers and you want to, now you can actually talk about an algorithm. Add these two and this algorithm takes a input, of course these two black boxes and also a digit number k. And, produces the kth digit of the sum after the decimal point. How do you do that?

Student: (Refer Time: 03:59).

That is how the representation of the decimal representation of real number. That is what it means that it should be able to produce; given a k, it should be able to produce the kth digit of the number after the decimal point.

Student: (Refer Time: 05:56).

Any number, whatever, not just kth digit, but we can say give me k plus first digit k plus second digit two kth; all the digit we can access it. But, the question is what are the carries. How do you know?

Student: (Refer Time: 06:10).

The carries you would not too; because it goes for forever. And, there is no pattern in that in general. So, we cannot really; with this noted the understanding or of the representation, we have real numbers. We cannot even add them. Of course, we cannot multiply them either.

Student: I can give a narrow bound.

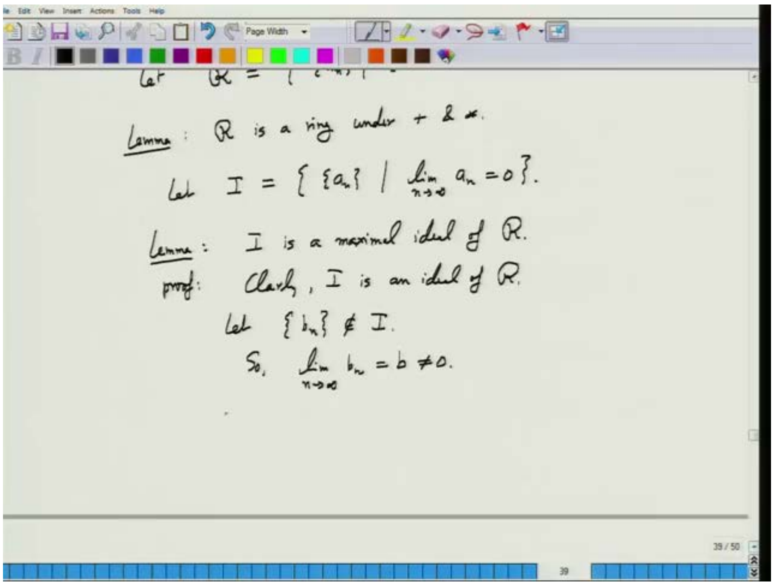
You can give a narrow bound. Yes. But, nothing beyond, so even addition or multiplication on real numbers in that representation is not well defined. And, that is a bigger problem with that representations as correspondence or how we intuitive to an extent. But, it does not quite work for real numbers. It only works for rational numbers. So, that is why you need an alternative representation to define such operations and Cauchy sequences. I have the best such representation. The simplest such representation because now it can define now that a Cauchy sequence represents a real number. So, now addition of (Refer Time: 07:34) real numbers.

So, we are given Cauchy sequences. So, let say a n and b n, plus b n. I can define it as simply as this sequence. This component by addition; and, this is a Cauchy sequence; a n plus bn. Why? We just need to verify that property that given an epsilon; there should be a large enough n, such that a n plus b n, the difference of this with a n plus m plus b n plus m is smaller than epsilon. And that is done simply for; Let me show it for this. And then, I will not do for multiplication. You can do it yourself.

Student: (Refer Time: 08:42)

Consider that n. So, pickthat N a for a n sequence. So, is that the difference is utmost epsilon by two after N a; and, similarly N b for b n, so that the difference is also less than epsilon by two. And, let N be the max of N a, N b. Then, a n plus m plus b n plus m minus a n minus b n, this, less than equal to. Look at this difference; that is bounded by epsilon. So, we have shown that same property for this sum sequence. And, similarly we define multiplication.

(Refer Slide Time: 10:42)



Just the component wise product and the same property can be shown that this is also a Cauchy sequence. And, it converges to the product numbers. And that is easy to say.

So, now it is very easily defined. And, that is one great advantage of now at least, we know what addition and multiplication means or the Cauchy sequences. Now, that we have it. So, we therefore get. If we define, let say R script to be set of all Cauchy sequences. And, we have this lemma that script R is a ring under addition and multiplication; because there is one sequence; that is, see if you look at the addition, all 0 sequence which is the identity of addition, the negative a n and this is inverse of a n. And, for multiplication all one sequence is the identity of multiplication. And, the multiplication commutes, sorry, distributes or addition because component wise, you just say multiplication and addition of rational numbers. So, all those properties are satisfied that could get a commutative ring.

Student: (Refer Time: 13:14).

It is an infinite sequence. Yes.

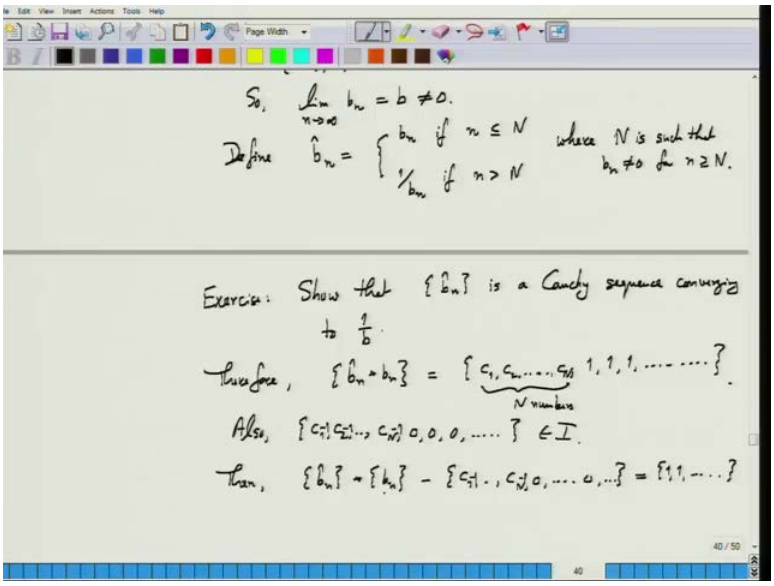
Student: That is also (Refer Time: 13:18).

Formal power is a infinite sequence. Yes, but their coefficients need not have a particular pattern or the kind we want. So, here we want very strong pattern, that is, successive numbers must get closer and closer to each other. So, we have a ring, but we still have not resolve the problem of multiple representations. In fact, yes, look at all representations, all Cauchy sequence that represent the number 0.

So, let I be the set of all Cauchy sequences, which converges to 0. The name gives it away. This is going to be an ideal. Not only any ideal, it is a maximal ideal. Firstly, why that an ideal? Is it a commutative group under addition? And, that is closure under addition. If you have a two Cauchy sequence both converging to 0, then their sum also converges to 0.

If you have the Cauchy sequence in I and multiple any other sequence to this that would also converge to 0 because if a n converges to 0, then a n times b n, as long as b n s are bounded above by some number, it also converges to 0. So, clearly I is an ideal. Why is it a maximal ideal? That is good. Well, let us pick up any Cauchy sequence that is not in i. What does this mean that b n is not in i? It means that b n converges to; this converges to let say b and b is not equal to 0.

(Refer Slide Time: 16:18)



Now, let us define the following Cauchy sequence, which is, let us define another sequence or numbers; these are rational b n. And which take the value b n, whenever n is less than equal to capital N and one bar b n; whenever n is greater than N and capital N is number chosen, so that after capital N, b n is not 0 that such a capital N exist follows from the fact that the b n sequence converges to a non-0 number.

So, there will always be a large enough capital N, beyond which b n is not never going to be 0; because it comes, it has come so close to b. Then, it can never become 0. Now, so here let me give you as an exercise. Let b hat n is also a Cauchy sequence converging to one by b. Once we have shown this, then the rest is straight forward. Even this exercise is not difficult at all. But once we have this, and then just consider the Cauchy sequence which is obtained by multiplying b hat and with b n. This is a Cauchy sequence. How does this look like? Equals some numbers up to first capital N numbers, after that it is all ones, directly by definition; multiplication of b hat and bn.

Student: Multiplication of b hat and b.

Yes. See, if you look at the definition of b hat n, above capital N it is 1 over b n. So, 1 over b n times b n is just 1. So, all the numbers beyond capital N will be 1. The numbers below that may or may not be 1. And, let me write this. Given name to this let us call them C 1, C 2 to C N. These are some rational numbers.

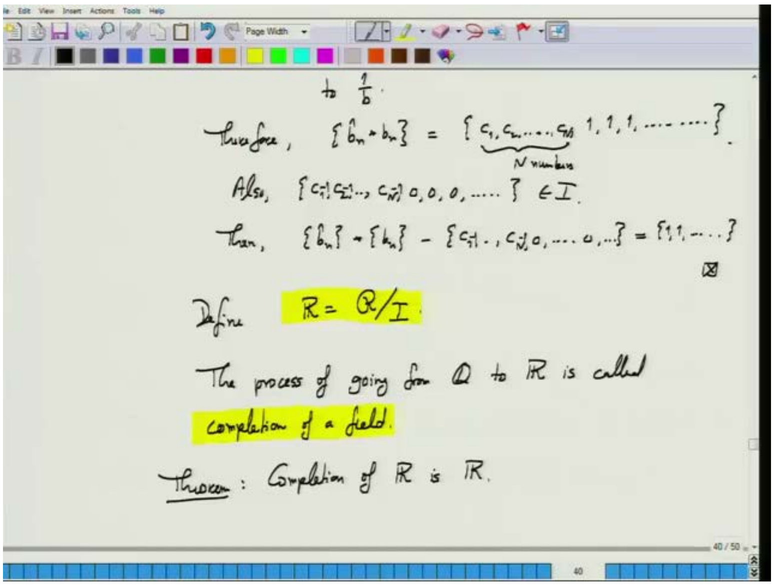
Also, now note that this number or this sequence which is first N numbers is C 1 to C N. And, all the subsequent numbers are 0s. This is a Cauchy sequence clearly because it is converging to 0 and beyond a point, everything is 0. All differences are 0. And, this belongs to the ideal I.

Now, what is the difference between these two? So, let us call this sequence C. Then, b hat n times b n minus C 1 to C N. This is; the first N numbers are C 1 minus one, C 2 minus one, up to C N minus one. All other numbers are 0. It is still a Cauchy sequence. Agree? Cauchy sequences has the property that first few numbers can be (Refer Time: 21:46) It does not matter. As long as after certain point, everything is starts converging. So, this is a Cauchy sequence. It converges to 0. So, it is in the ideal I and the difference between this is all ones.

Student: (Refer Time: 21:54).

This is the one. So, now, we have the b n was in and a Cauchy sequence which is outside the ideal. This is in the ideal. So, in the ideal generated by b n and I, we get the one, which is therefore it is an entire ring. And therefore, this shows that I is a maximal ideal. Add any other additional, any new element to I, you get the whole ring. Now, we can define our class of real numbers.

(Refer Slide Time: 22:40)



R to be script R quotiented i; this will have a unique number or unique element corresponding to every real number. And, since I is the maximal ideal, it is a field. So, this is the formal definition of real numbers. Somewhat non-intuitive or little more complicated. But, this is the way you can properly define real number. Not, in earlier, the school definition is very informal.

Student: (Refer Time: 23:17).

Sorry.

Student: (Refer Time: 23:19).

That is always with. When you are working with numbers, then they are always rational numbers. So, that is why that is fine.

Student: Now, additional (Refer Time: 23:34).

In the quotient ring, yes.

Student: (Refer Time: 23:38).

And, now multiplicative inverse also exists. By virtual, this (Refer Time: 23:54).

So these processes, the whole thing that I went through, you know, starting with rational, defining the Cauchy sequences. Then, quotienting in the ring of Cauchy sequences with a maximal ideal to get another field. So, of course this also involves that quotienting an ideal with the maximal field together and maximal ideal together, the ring, together the field, but there is something all that is done. You start with the field, you introduce Cauchy sequence of that field and then you do at this. This process is called a completion of a field. And this, we can define for many other field, not just with rationals.

As long as we have a notion defined of nearness; right, two numbers are close to each other. And, they get closer and closer to each other. So, that notion must be available on that field and we can define completion.

So, in particular, for example, we can ask what is the completion of R itself. Whether you start with R, define Cauchy sequences with elements of R, get that ring quotient, maximal ideal quotiented, and get a field what you get. And, it turns out that; let us say a theorem. Get nothing new, you get back R. So, here is; we are not. It is R in therefore, in the sense the ultimate that the final point where we can extend this completion starting from rational sequence.

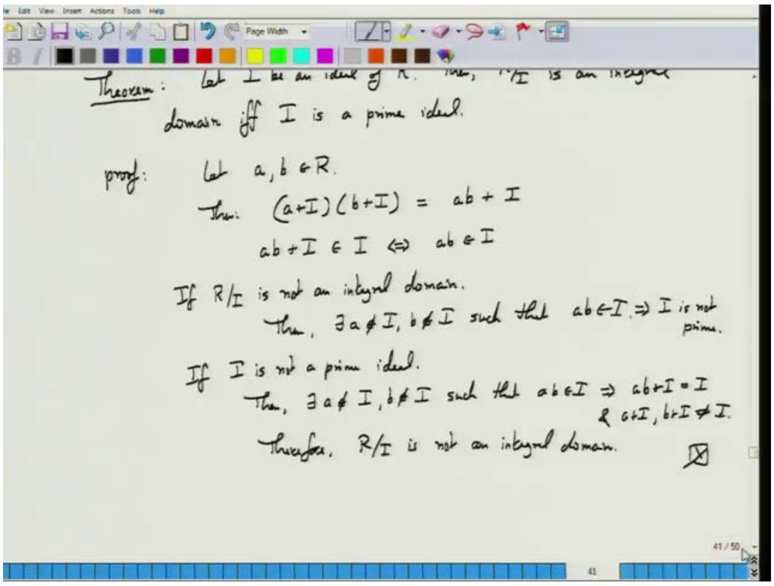
Student: (Refer Time: 26:18).

That is right. That is what the completion is. That is how the name derives that you have. You complete this gap between ratios. That is right. And, this whole process if you see Cauchy sequences, etcetera, that is trying to fill that gap. So, that is all I will talk about in this completion.

Let me get back to the fields. And, we were discussing the ways of getting fields from rings. One way was quotienting with maximal ideal and another way was starting with the integral domain and taking the fractions; that is also a field.

Now, in order to do that we have to start with integral domains, which not all rings are. But, do they starting with the general ring, we can actually get very nicely integral domains. There is a next theorem.

(Refer Slide Time: 27:34)



Take here ring R. Take this ideal I and quotient R with I. The ring you get is an integral domain, if and only if I is a prime ideal. Proof is straight forward. Let us say a, b be elements of the ring, not in I. Now, consider the quotient ring. The quotient ring will have elements of this form; this is equal to a b plus I. Now, if in fact why we start, so let start with a general two ring elements. And, in general this is. Now, if ab plus I is I, this implies that ab is an i. Infact, this is if and only, or by both ways.

And, now let us say suppose R by I is not an integral domain. What is that mean? That means that there exist a and b, so that a plus I and b plus I are non-0 elements of this quotient ring, whose product is 0. So that means, a plus I time b plus I, which is a b plus I is 0, which means there is a 0 being mean that ab is in I. right. And, a plus I and b plus I are non-0, which is equivalent to saying that a is not in I and b is not in I, such that ab is on I. And, these imply that I is not prime. That is by definition. Conversely, if I is not a prime ideal; that means, there exist such that ab is in I. And, this implies if ab is in I, then ab plus I is equal to I. And, this implies?

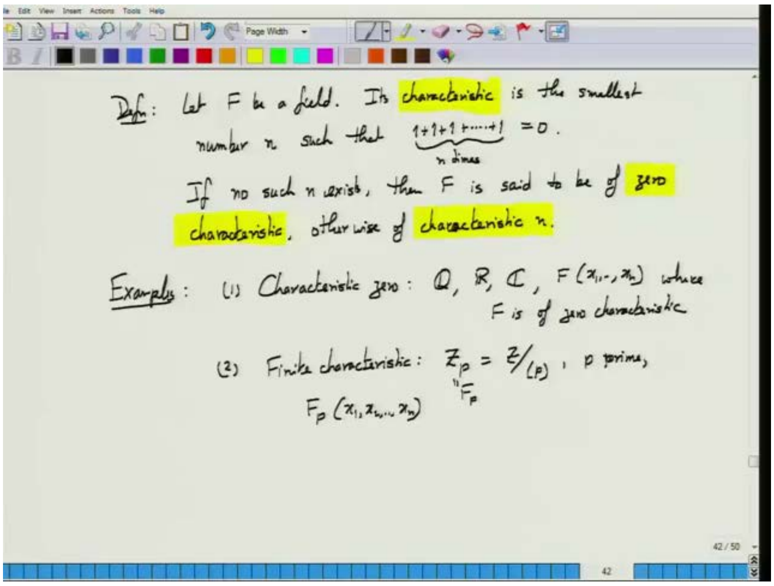
Student: It is not an integral domain.

It is not an integral domain, a pretty straight forward. So, now we have this way of creating fields as well. Start with any arbitrary ring; take any prime ideal, quotient with the prime ideal, you get the integral domain and then take the field of fractions.

Now, the fields are queries; a special kind of rings, of course. They are very interesting because the full arithmetic can be done here. They are only of structures where the complete arithmetic is possible. All four operations; addition, division, multiplication, subtraction can be carried out completely. And therefore, they are extremely useful.

So, we would like to understand their structure as well. You just like we try to understand the structure of groups and rings. So, let us try to understand structure of fields. And, one of the key parameters associated with the field because firstly, you first realise that fields have more structures than rings; because division is also available. They have to satisfy. Now, everything is the unit, so those strange elements which are non-units do not exist in a field. So, it is expected that it should have more structures. And, it is indeed true that fields have more structure. More things can be proven about fields than for rings. And, one of the key thing or key parameters associated with the field is its characteristics.

(Refer Slide Time: 33:17)



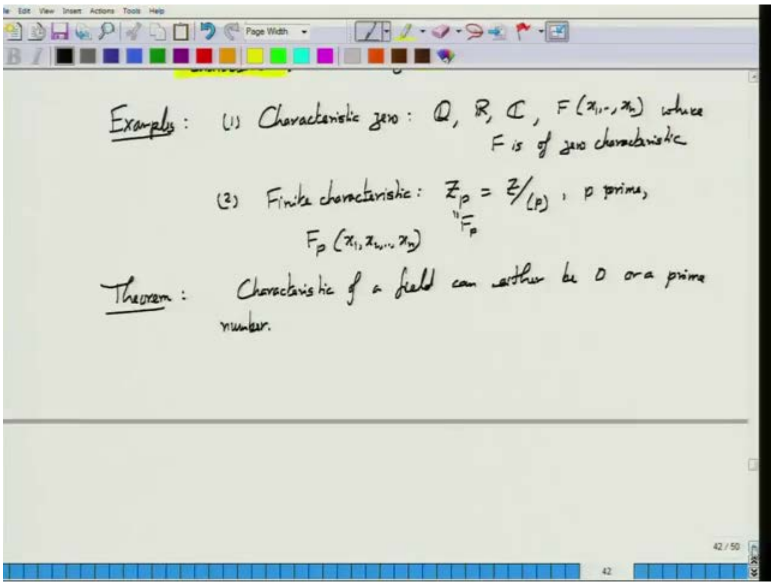
The characteristics of a field is the smallest number n, such that when you add one to itself n times, you get 0. Now, this one and 0 are the identities of the field. And, there would be fields where no such sum would ever be 0. For example, for rational numbers, you keep adding one; you keep the number, keeps growing up. It will never become 0. So, let me add that. If no such n exists, then F is said to be of 0 characteristic, otherwise of characteristic n; because 0 characteristics because it is does not quite fit into that.

But really this, if you add one to itself 0 times, of course you get 0. That is true with everything. But that is the only way possible in some fields. So, that is why we call 0 characteristic. So, examples; Characteristic 0, these are rationals, reals, complex numbers, field of rational functions over F. These are all characteristics 0. Wait a minute; F, where, this field where F is of 0 characteristic. Otherwise, finite characteristic Z p; this is a field. This is obtained by z quotienting with prime or maximal ideal p. And, this is of finite characteristics because in this field if we add one to itself P times; that 0.

Student: (Refer Time: 37:29).

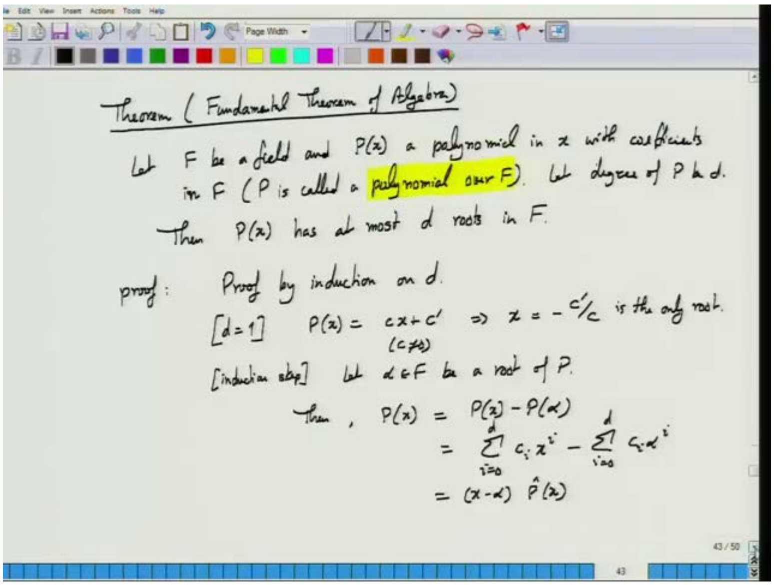
R, yes, then more often written as F P to highlight the fact that they are fields of characteristics F p; this also as characteristic, in fact, another simple to prove theorem, but important one.

(Refer Slide Time: 37:55)



That characteristic of the field can be either 0 or a prime number. I leave the proof to you. It is very easy to show. So, what is the structure of fields, in general? The answer is not straight forward at all. Even though fields have more structure, there is all kind of fields, particularly in, when we talk about infinite fields. There are various kinds, while you want to highlight one special kind, which is algebraically closed.

(Refer Slide Time: 39:18)



But, before that let us highlight one very important property of fields, which is the funda are also called fundamental theorem of algebra. Have you come across this, the fundamental theorem of algebra? No; I am sure, you have come across it. When I state it, you will realise.

So, take a field F and take a polynomial P in one variable x with coefficients coming from the field F, such a polynomial is called a polynomial over the field F; because its coefficients are from the field. Let degree of P is d. You have seen this? That is the fundamental theorem of algebra.

You must have seen this for specialised to specific fields; reals or complex numbers. But, this holds in general over call fields. And, the proof is same as the proof for your special case, in case you recall it. So let, we can prove this by induction. So, for d equals one, P is c x plus c prime. This implies that there is exactly one root. Correct. And, what is that? C is not 0 because it is of degree one. So, x is, you know, is the only root.

Now, induction step. Assume for d minus one. Now, you want to prove for d. Let alpha in F be a root, then P x is same as P x minus P alpha, which is same as summation i going from 0 to d; which is c i x to i alpha to the i. This is P of alpha is 0, by assumption. So, I can just write it in this way. Now, if you look at this two difference, you can take term by term, a common factor of x minus alpha; ci x to the i minus c i x alpha to the i.

Take a factor of x minus alpha out and collect with the rest in this P hat x. Now, P hat x is a polynomial of degree d minus 1.

Now, the rest is straight forward. Now, you just invoke the induction. This will have at most d minus one roots, P hat x by induction. And, what are the roots of P? Any root of P hat x plus alpha that is possibly the dth root or one more and no other. Any other value of x, where x minus alpha is non-0 and P hat of x is non-0 will result a non-0 value because it is an integral domain. So, product of two non-0 value will remain non-0. In fact, this properly holds not only for field, but for any integral domain. So, that is all for today. We will continue tomorrow.