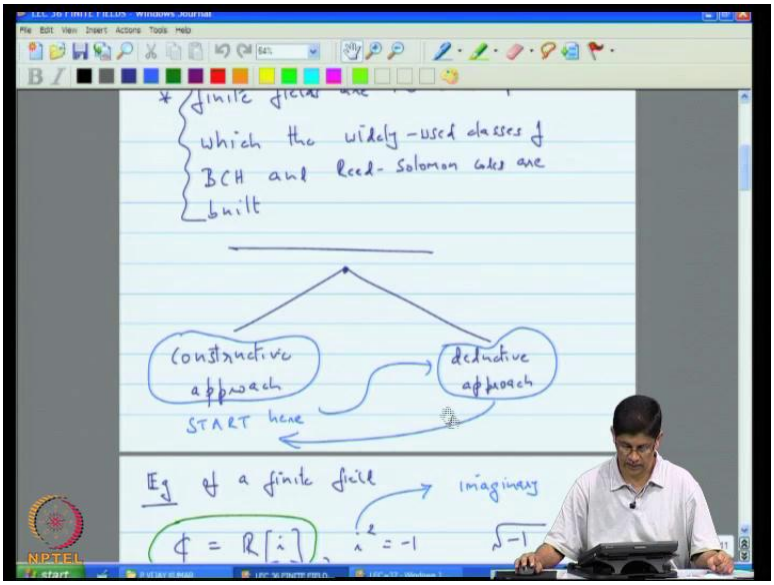
Error Correction Codes
Prof. Dr. P. Vijay Kumar
Electrical Communication Engineering
Indian Institute of Science, Bangalore

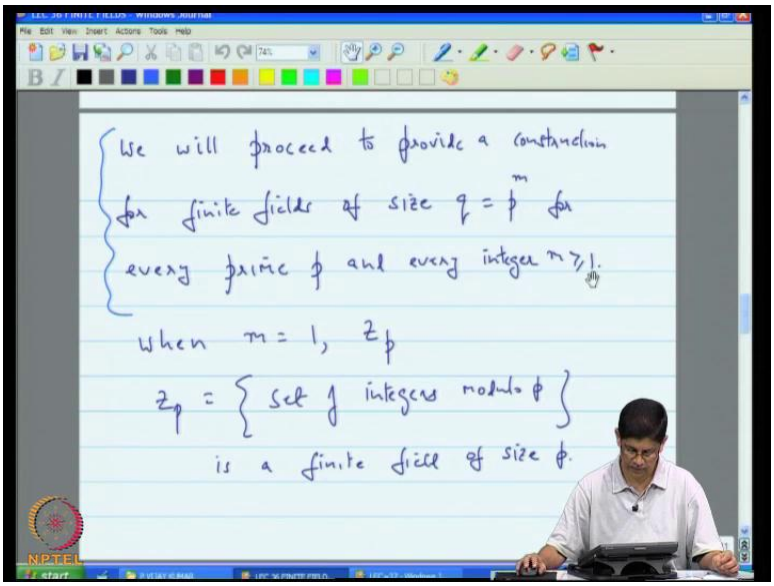
Lecture No. # 37
Finite Fields a Deductive Approach

(Refer Slide Time: 00:33)



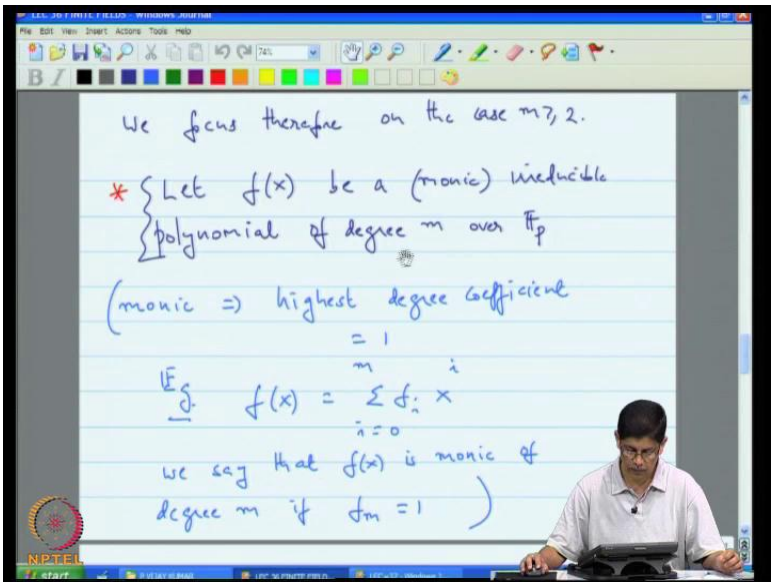
Good afternoon, welcome back. So, today is our lecture thirty seven, and in the last class I began discussion of finite fields. And I had mentioned, let me just quickly take you through the lecture had began by actually saying that you would actually follow two different parts. First will actually show how you can construct finite fields. And then after that we deduce that in fact what is actually true is that the structure of the finite fields of the finite fields that we do construct is in fact typical of the general class of finite fields.

(Refer Slide Time: 01:07)



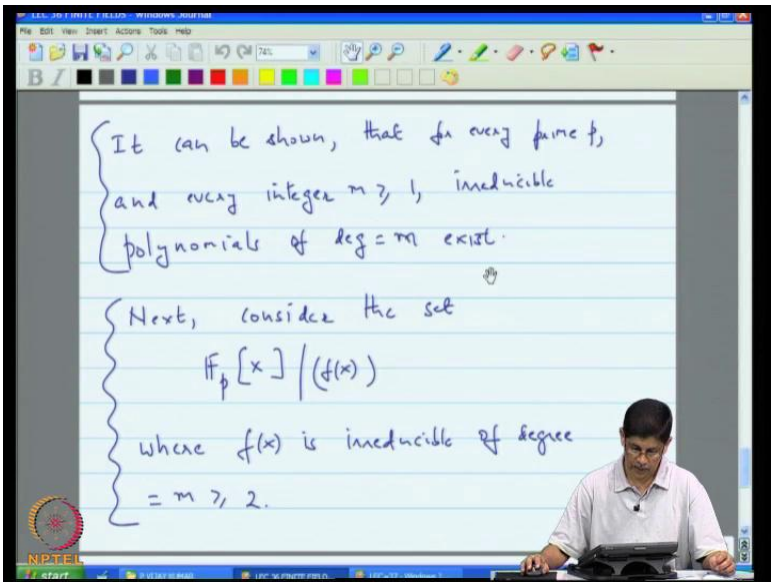
And I motivated my construction of finite fields by making an analogy with the class of complex numbers, but I skip that. And just say that, so we will provide to provide a construction for finite fields of size q equals to p to the power of m, for every prime p and every integer m. And then when m is equal to one, if you take the integer modular p and we know that already forms a finite field. So, the interest is in the case when m is greater than or equal to 2. It turns out that finite fields only exist, when the size of the field is a power of prime. So, there is no lost of generality and restricting to the situation.

(Refer Slide Time: 01:56)



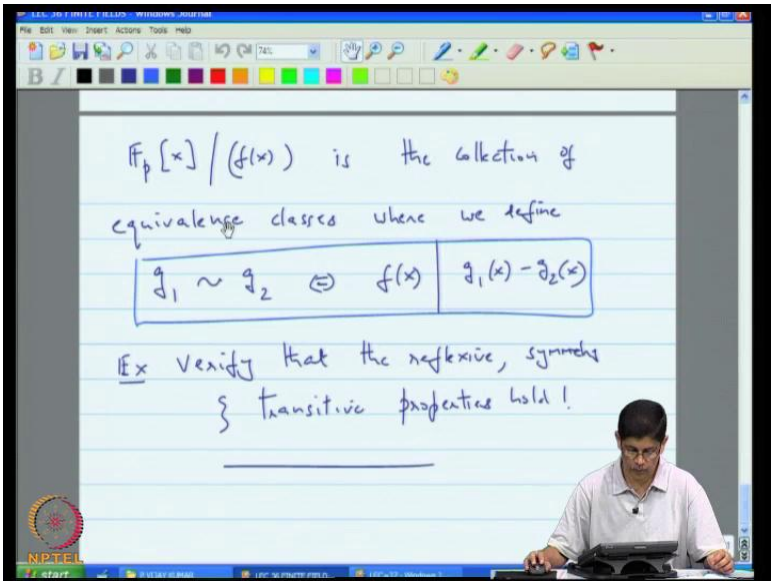
We focus on the case m is greater than or equal to two and the way we do it as we take monic reducible polynomial. So, what is monic means? Monic simply means the highest degree coefficient actually is equal to one. Reducible means that it cannot be fact that product of two polynomials, each of who has degree less than the degree of original polynomial. For example, when p is two and then this is the list of the radiousable polynomial of small degrees; degree 1, 2, 3 and 4. It can be shown that for every prime p and every integer m is greater than or equal to one irreducible polynomial. So, degree equal to m exist.

(Refer Slide Time: 02.31)



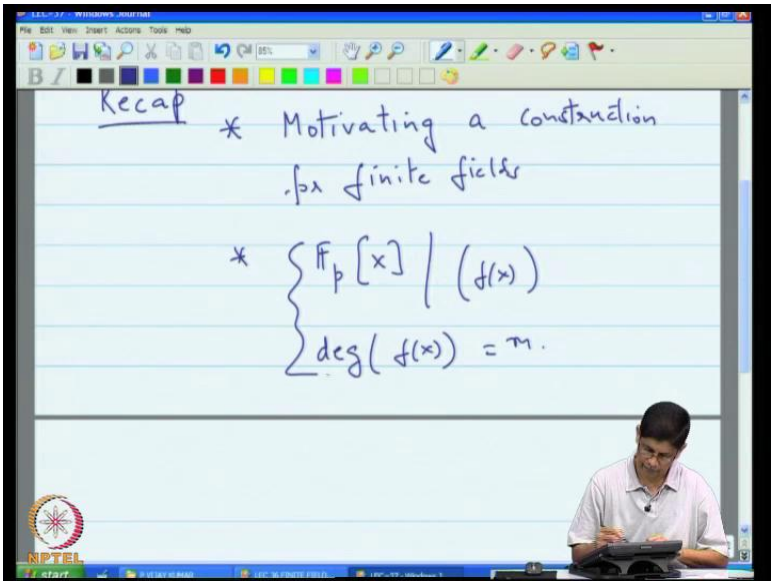
So, we know that such a polynomials exist. Then we consider the following construct; that is we consider the set of all polynomials over the integer modulo p. And we go modulo f of x, where f of x is irreducible of degree equal to m.

(Refer Slide Time: 03:04)



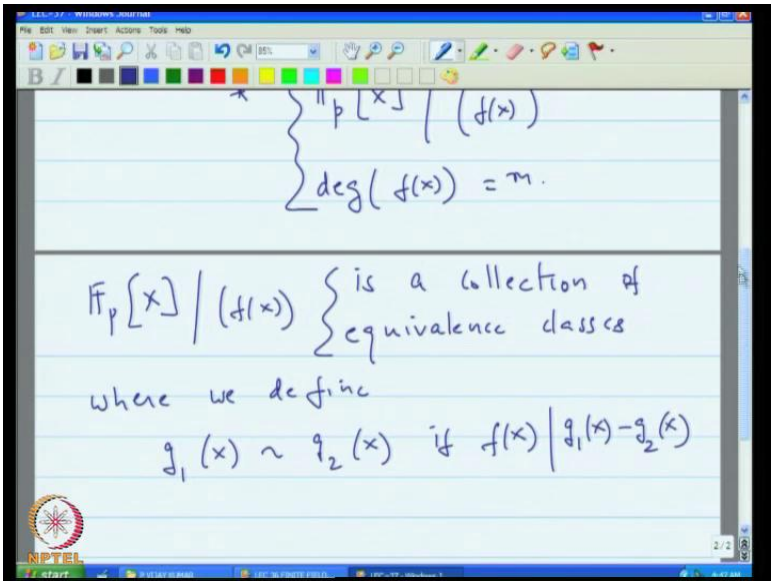
And afterward at the end of the last class, I told you that if you (( )) modulo f of x and these are the collection of equivalence classes where we define g 1 equivalent to g 2, if f divides that difference, so this is where will pick up the discussion. So, just quick recap

(Refer Slide Time: 03:26)



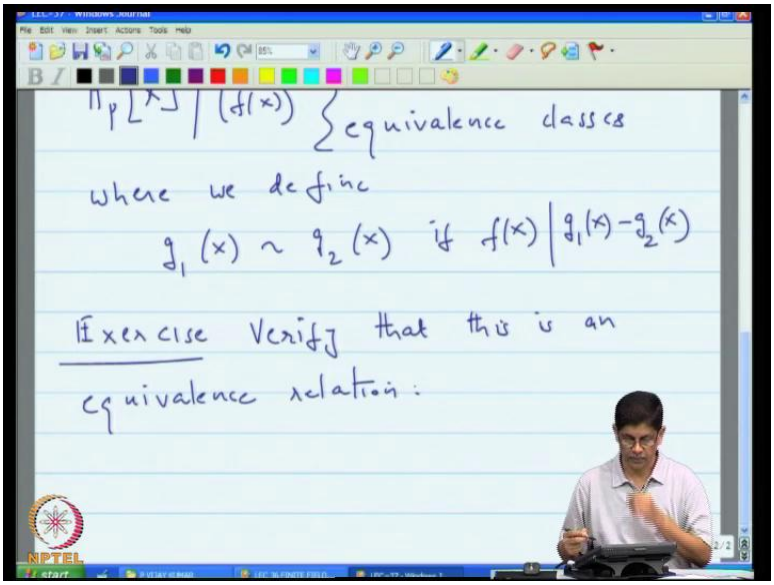
We talked about… So, I can say that we motivated the first began by motivating construction for finite fields.

(Refer Slide Time: 04:46)



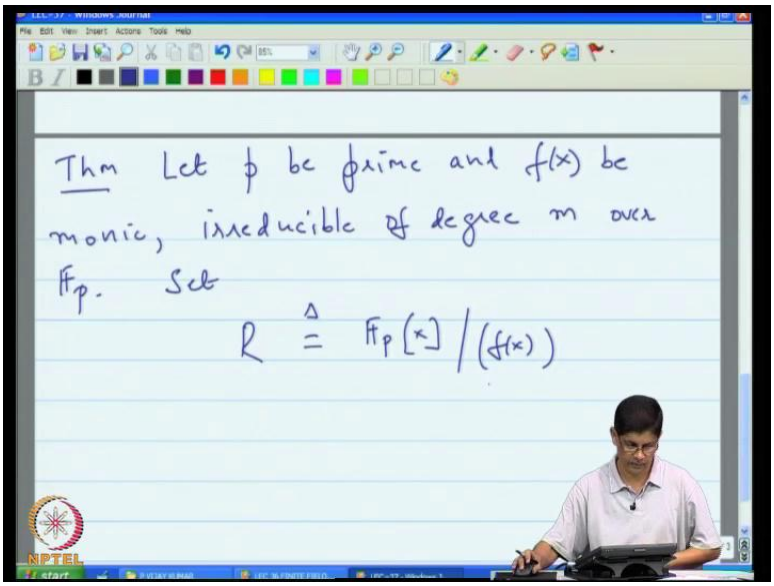
And then the construction itself involved taking F p of x and going modulo f of x, where the degree of f of x is equal to m. So, this is our construction and first of all clarification that is you should regard F p (x) mod of f of x. So, this is the collection of equivalence classes, where we define g 1 of x to be equivalent to g 2 of x, if f of x divides g 1 of x minus g 2 of x.

(Refer Slide Time: 05:55)



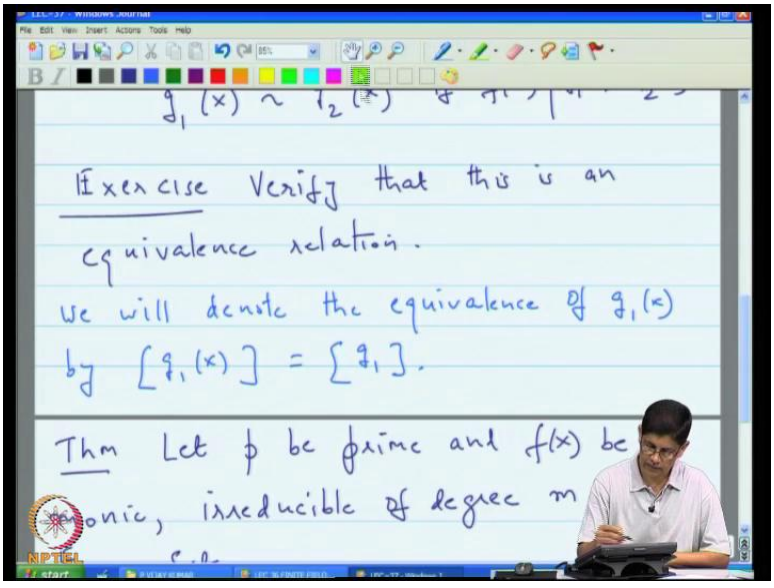
So, I leave it as an exercise and I gave this last time. Verify that this is equivalence… So, what that means is that you have to verify that the reflexive, the symmetry and the transitive property is actually held.

(Refer Slide Time: 06:53)



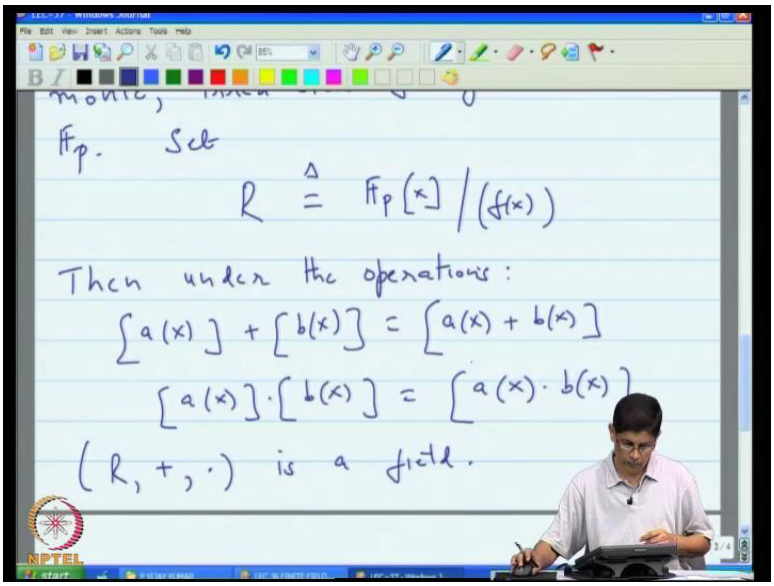
Once you verify that, then we ready for the theorem. Let p be prime and f of x be monic, irreducible of degree m over F p. When you say that polynomial is over F p, what you mean is that the coefficients of polynomial like in F p. And then now we set R we define R to be F p of x divide by f of x, module of f of x.

(Refer Slide Time: 08:13)



We know that, this is the collection of equivalence classes. So, facts should actually note here so we will make a note here. We will denote the equivalence class of g 1 of x by g y. And sometimes, pairs are laziness pairs are because not requires, we simply write this as g 1 and x is understood. This notation here indicates the entire equivalence class. So, now with respect to that notation then under the operations a of x plus b of x is equal to a of x plus b of x. And a of x times b of x is a of x times b of x.

(Refer Slide Time: 08:57)



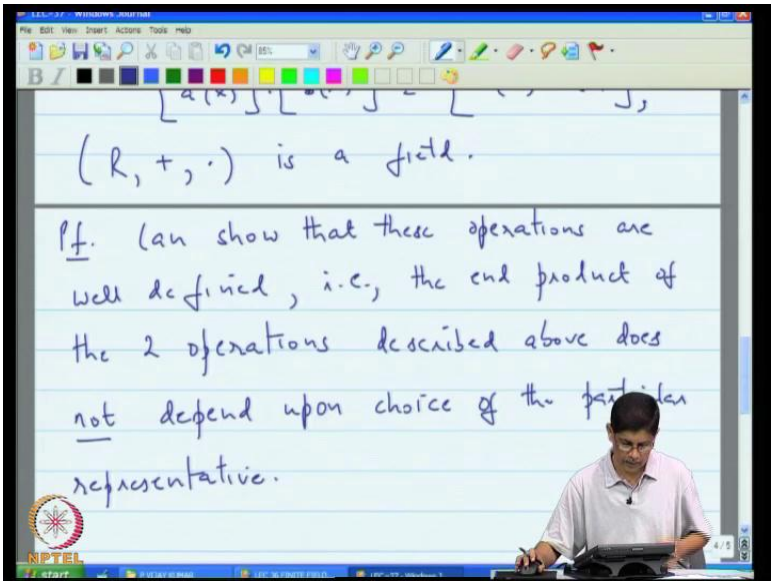
Then under this operation, if you consider R plus dot is a field. Now, when mathematician's first follow let me explain this is saying that look, you define a addition operation between two equivalent classes by taking a representative from each of the equivalent classes, and defining the sum of the equivalent classes to be sum of the representatives.

Similarly, if you want to multiply two equivalent classes, you take a representative from each of the equivalent classes multiply them and pass on to the equivalent classes of their product. And then define this to be the equivalent classes of the product the equivalent class, there is the product of these two or the movement here is that say well you know, you know what? Since a given equivalence class can have several representatives. How do you know the (( )) different representative for the same equivalence class? I want get a different answers, so that a mathematician in mathematical languages, what people you need to says the operations are well

defined. So can show and I think, I am little conscious now, beginning together little conscious of the fact that our time is limited.

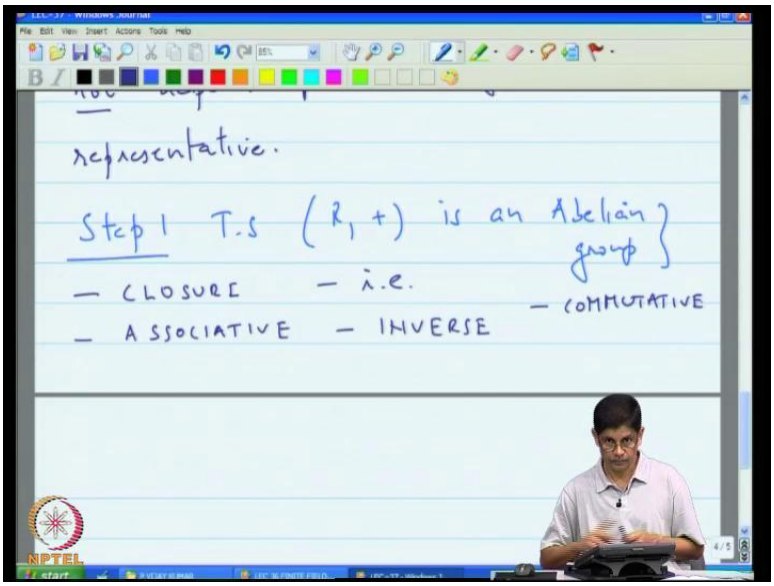
So, I am going to skip all the non essential proofs that, I can spend little bit more time on the course, but this is leading on proofs.

(Refer Slide Time: 11:30)



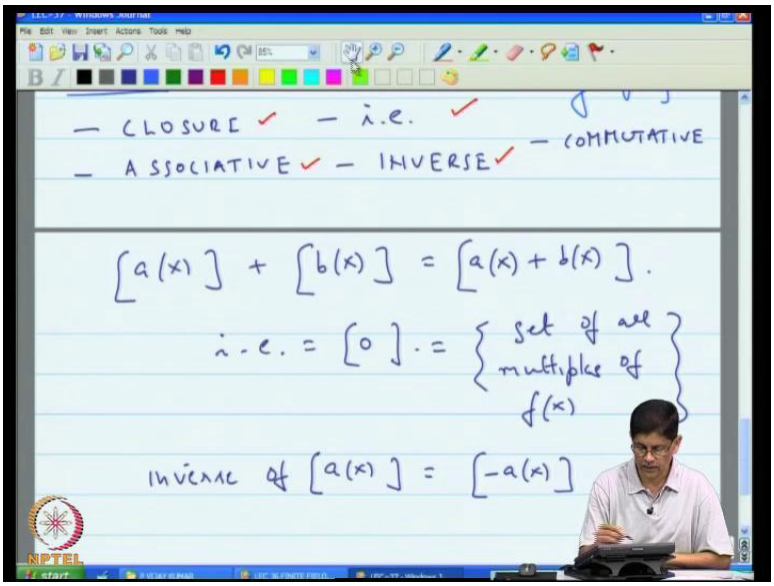
So proofs, first of all can show that these operations are well defined. In other words, the end product of the two operations described above does not depend upon choice of the particular representatives. Now, once we got out if the way the question is this does this give us, does really give us a field?

(Refer Slide Time: 13:09)



So, the first step is step one, we prove this in steps. So step 1, we will show, to show there if take R plus is an Abelian group. Now to show that something is an Abelian group, you need verify the corresponding axioms; you have to check that the axioms of closure of associative of the presence of the identity elements, the presence of the inverse and the commutative axioms all hold. And in other words, what you have to show is that? For example, if you worried about closure, you just need to actually show, so all of this with respect to the following operation.

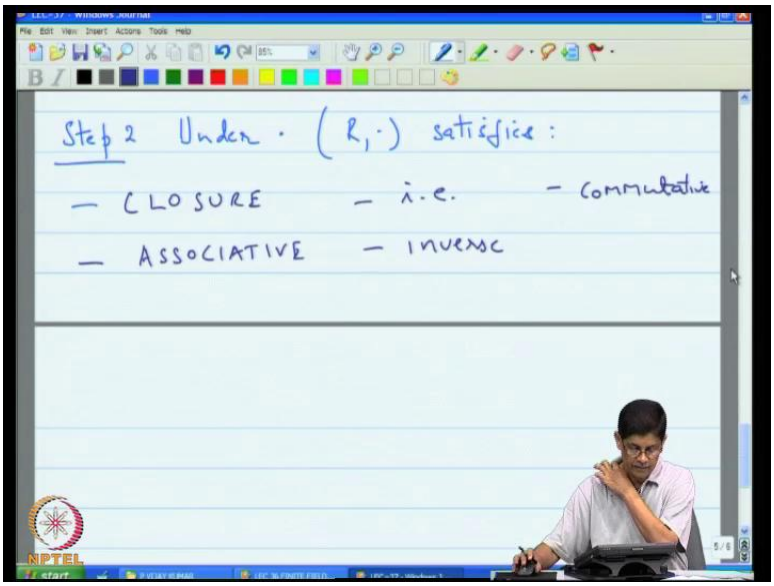
(Refer Slide Time: 14:20)



So, a of x the equivalence class of a plus the equivalence class of b is the equivalence class of a of x plus b of x. Now clearly this well defined, because given any two representatives we construct the some of these as polynomials. So that is closure is find and associatively, if you takes three of the terms, it does not matter in which ordered you add them; that is also clear. So, some of these are quite obvious and need not spend time on that. The identity element, the identity element if you spend little bit of time think about it, you will see the identity element in this case is the equivalence class of zero. I remember that the equivalence class of zero of all those polynomials which of the property that difference is divisible by f of x.

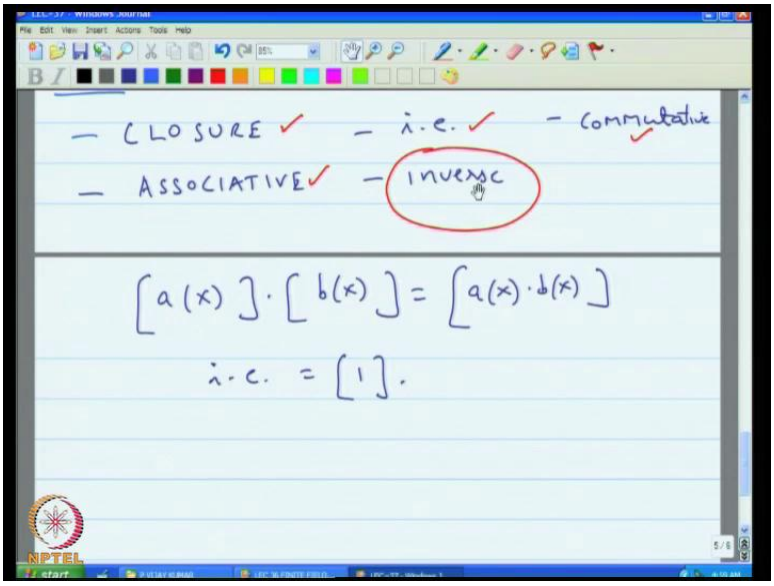
So, this is precisely the set of all multiples of f of x. So, that is your identity elements. So, that is of the straight forward. The inverse well the inverse the inverse of the equivalence class a of x is nothing but the equivalence class of minus of a of x, why because simply because if you add these two actually get the identity element which is the equivalence class. So, now even that has been verified. And commutatively off course, because simply because the addition is in here, the order does not matter is not going to matter here. So, we verified all of these properties. So that is… That shows that our pluses and Abelian groups.

(Refer Slide Time: 16:27)



Next we come to step two, we need to show that under the multiplicative operation that are satisfies the following. One is, it satisfies closure the associatively property, the presence of the identity element once second, the presence of the inverse and the commutative property. So, one second we have five properties to check and closure is immediate.

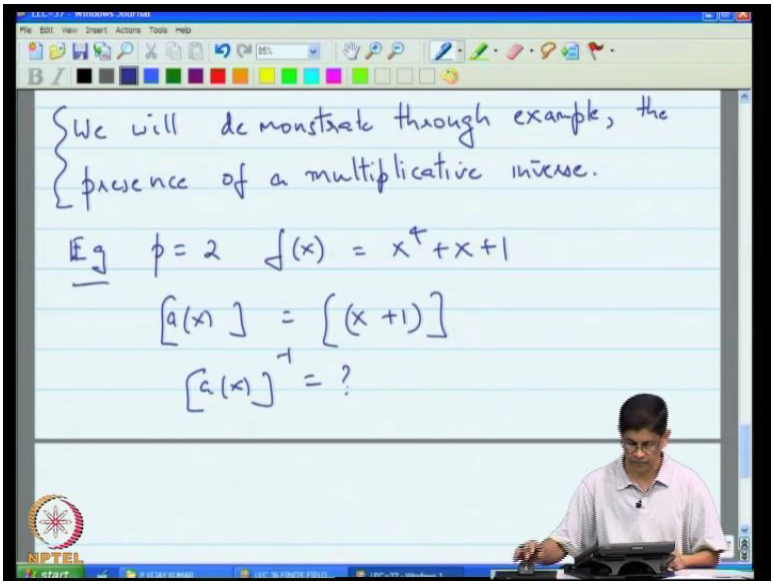
(Refer Slide Time: 17:24)



Now this time, we are talking about the operation which says that equivalence philosophy, times equivalence class of b, a is the equivalence class of a of x times b of x. So, this is what we are actually saying. And closure immediate just from the definition, nothing to prove. Associativity is just easily verified in a multiplicative case. The identity element so the identity element it is easy to see that the identity element is the equivalence class of point so even that a straight forward.

Commutativity is also straight forward. So, the only thing is really requires some work is the inverse. How do you actually get the inverse? And you think about it that up to now, we have not use the fact that this equivalence class was defined with respect to the irreducible polynomial f of x. So when we see, we said that this set is nothing but the collection of equivalence classes, where we define this two polynomial to be equivalent, if f of x divides the difference. And of the first time, we are going to use the property that f of x is irreducible. So, plays a role and ensuring that every element has in inverse.

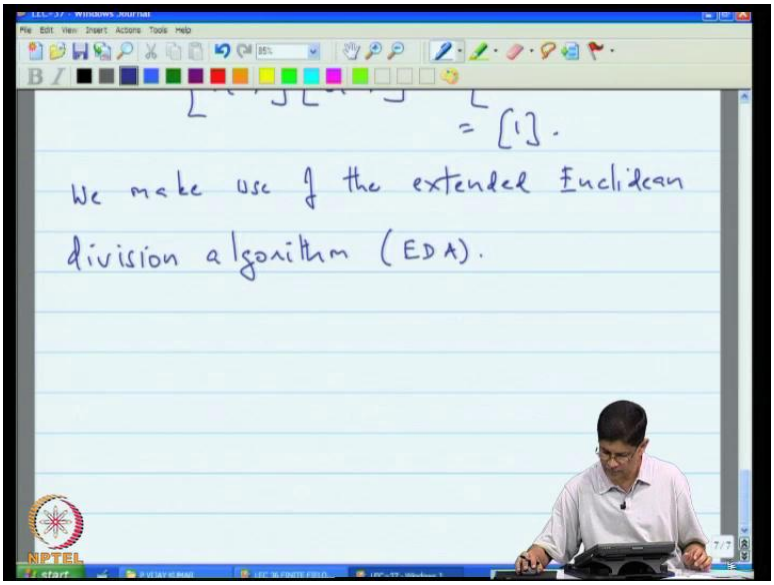
(Refer Slide Time: 18:59)



How do you prove that? So, will actually show do an example to show how one would compute the inverse in general. Two, we will demonstrate through example, the presence of a multiplicative inverse. So in this example, let us take p is equal to two and let us define f (x) to be x 4 plus x plus 1. This was one of the polynomials that were on our least of our irreducible

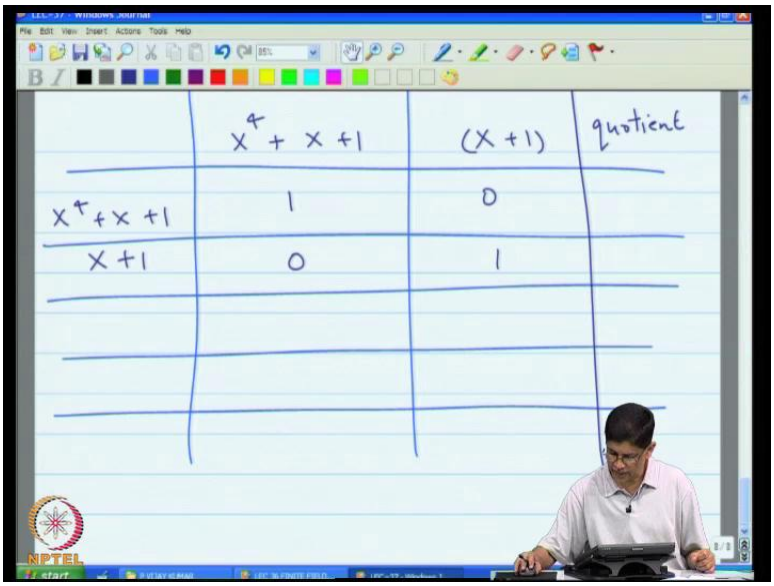
polynomial. This no problem taking this particular one hour and let say that we are interested in let us pick particular equivalence class. Let us say the equivalence class of x plus 1 and ask the question, what is the inverse of this?

(Refer Slide Time: 20:27)



Now the inverse of this means that, we are actually looking for an equivalence class b of x. Such that a of x, b of x which of courses a x b x is equivalent to 1. That means, we are looking for a second polynomial b of x. Such that when you multiply a of x and b of x, then the difference between that polynomial and 1 is divisible by f of x. Here what we do is, we call upon extended Euclidean algorithm which we discuss in time back. We make use of the extended Euclidean division algorithm. So I will abbreviate this EDA and again, I illustrate from example.

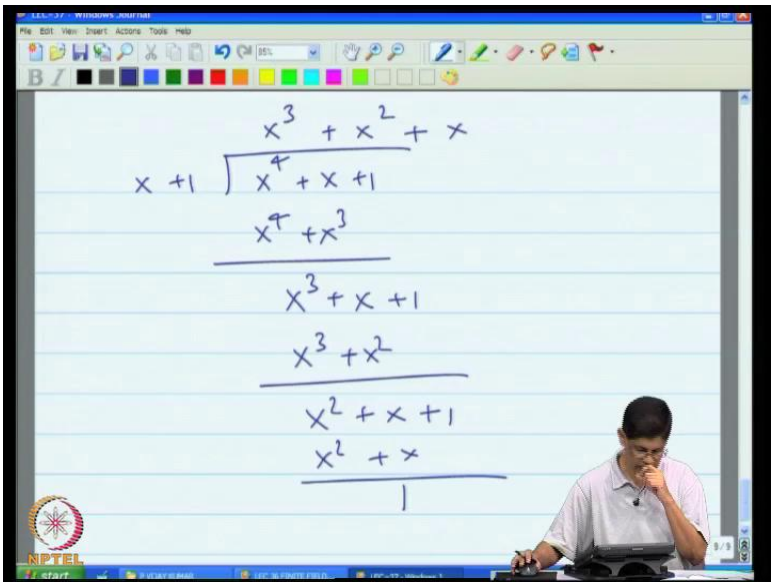
(Refer Slide Time: 21:45)



So what we do is, we form papers of I will do it on a next page to make sure run out of space. So will actually put, x 4 plus x plus 1 and x plus 1, in two separate columns. And then put x 4 plus x plus 1 and x plus 1 on two different rows. There after what we do is, we start a process of dividing.

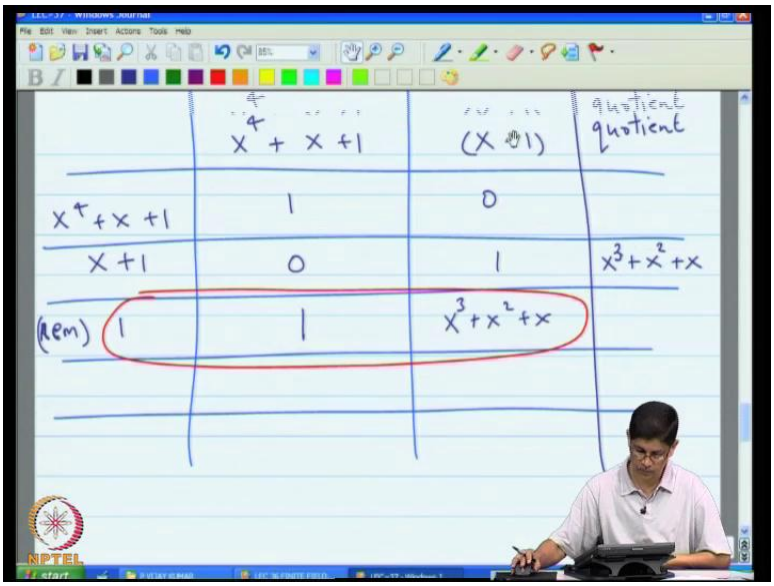
Now first of all x 4 plus x plus 1, we treat this like an excel spread sheet and so we actually, put down this is equals to 1 times this, plus 0 times this. x plus 1 is 0 times, x 4 plus x plus 1 times x plus 1 so actually put 1 here. Now, next what I am going to do is I am going to introduce a third column here which I will write as the quotient.

(Refer Slide Time: 23:05)



What this quotient does is that divides, it divides this polynomial here by this polynomial. You going to divide x 4 plus x plus 1 by x plus 1 and it may be a good idea to do division under this side. So, you have x 4 plus x plus 1 divide by x plus 1, you get x cubed, x four plus x cubed. You get x cubed plus x plus 1 plus x squared; x cube plus x squared, x square plus x plus 1, plus x; x square plus x and you get 1. So, what that tells you is that, when you did this division, you got kind of quotient that is x cube plus x square plus x. and the remainder which is 1. So we will make the note here.

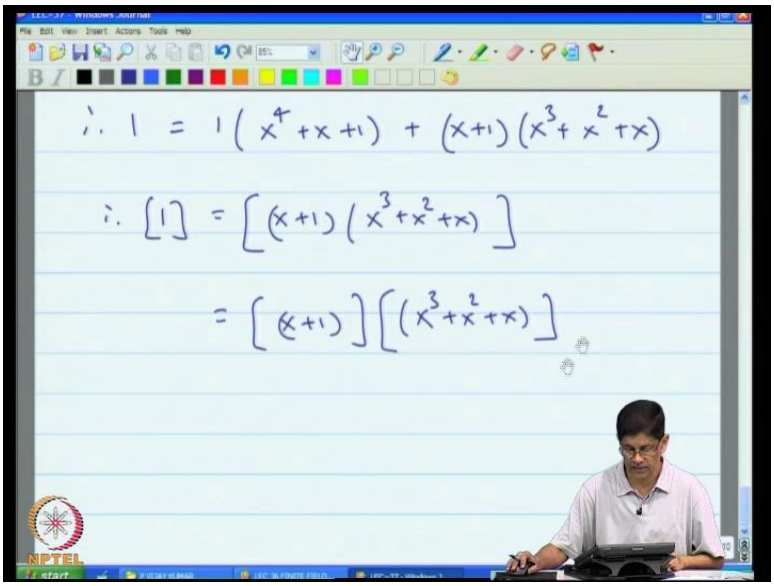
(Refer Slide Time: 23:55)



So, the quotient is x squared or x cubed plus x square plus x and the remainder was 1. So, this is the remainder and this is your quotient. So, the way we want to fill in these two entries here. The way you fill it like an excel spread sheet providing your formula. So for example, here the way got the 1 over here was taking this term here and subtracting this times this. So, the same thing you take 1 minus 0 times this, which is 1. And here, you take 0 minus 1 times this. As since your working in modulo to arithmetic minus 1 and plus 1 are same. So, whether you multiply this into this and add whether you multiply this and subtract where add. There is no difference.

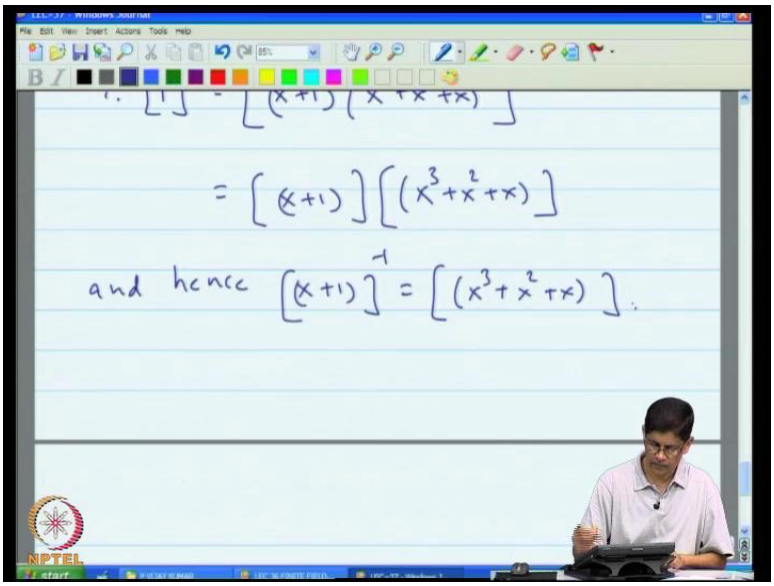
So, without reason what you will pick up here is nothing but x cubed plus x square plus x. So, in this favor what we actually shown is that. So, in this equation is important for us. It adds you there are may be to write there are may be to write 1 here. I may be to write the term 1 here, as something term x 4 plus x plus 1 plus something term x cube plus x square plus x plus 1.

(Refer Slide Time: 25:45)



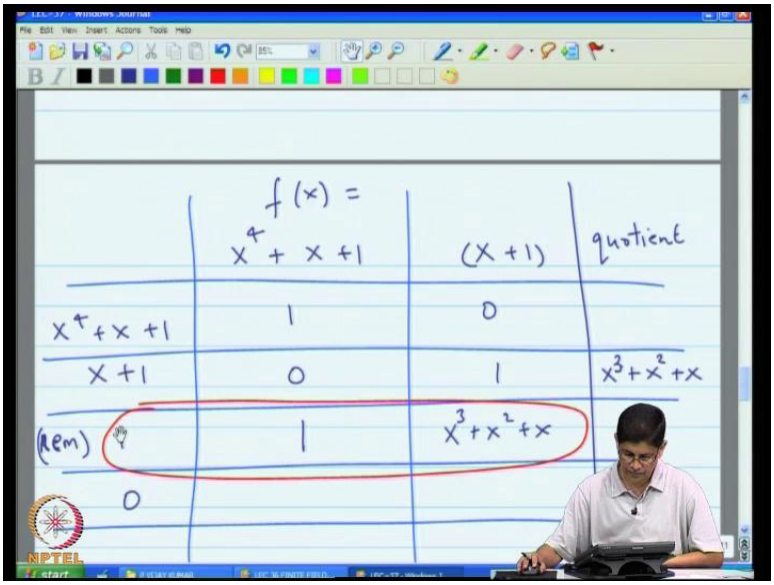
Therefore 1 is equal to x 4 plus x plus 1 into 1; 1 into (x 4 plus x plus 1) plus (x plus 1) into (x cube plus x square plus x). So, therefore this is telling us therefore, there may equivalence class of 1 equal to equivalence class of (x plus 1) times (x cube plus x square plus x), which is telling us the equivalence class of (x plus 1) times equivalence class (x cube plus x square plus x) equal to one. But now, you look at the equation, this equivalence class whose inverse is you want to find. And this is writing here when you multiply the two you get the identity.

(Refer Slide Time: 26:55)



And hence and hence the inverse of the equivalence class of this is the equivalence class of x cube plus x square.

(Refer Slide Time: 27:25)

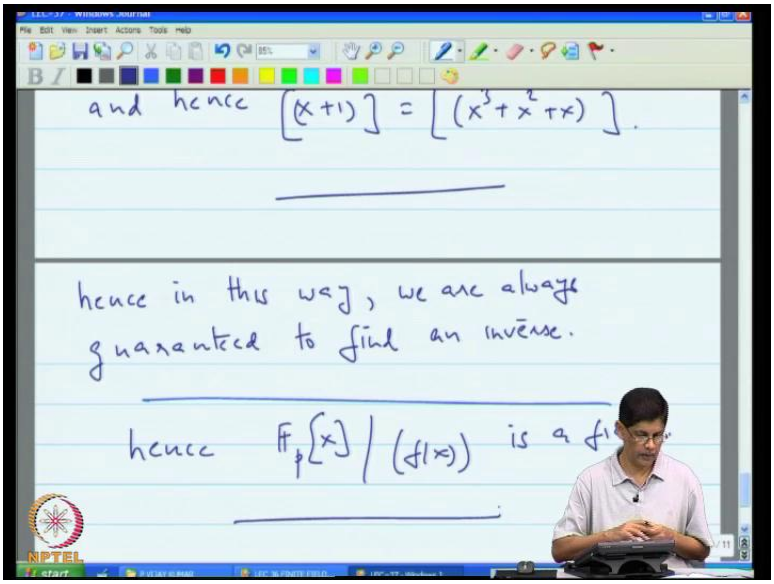


Now, so we have founded in this case, but now where exactly did I use the fact this polynomial f of x here. This was f of x where exactly did we use the fact that f of x was irreducible, where if

you recall the earlier discussion on the greatest common divisor. What we are picking up here in this process is the greatest common divisor of the two polynomial of the top.

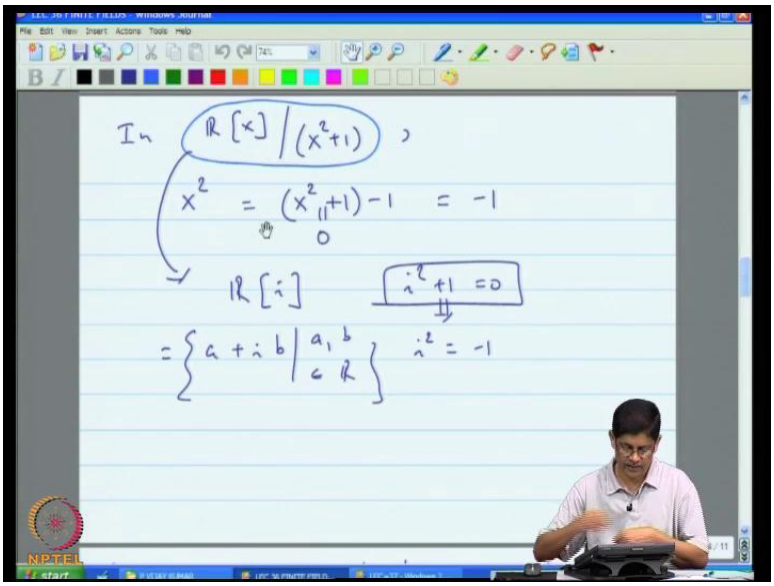
So, we go through all of this and then what you going to do is, if you did proceed one step further, what you should actually get is 0 here. So, the greatest common divisor is just the entry above 0, I think I mention that earlier. So this is the greatest common divisor. But since f of x is irreducible, unless this polynomial is multiple f of x which in our application, it will not be you are the greatest common divisor is going to be 1. So, you are going to end up at some point in the calculation with 1 on this. And that means, something times f of x plus something times of (x plus 1) will give you 1. In this way, you always guaranteed to find an inverse.

(Refer Slide Time: 28:31)



Hence in this way, we are always guaranteed to find and inverse. So, thus hence is a field. Now, I want to actually point out the simplification and I will do this play an example. So, just like let us go back to the discussion in the last lecture, where we were talking about real and complex numbers. So we said, there is actually possible to think of the complex numbers as being often take real numbers, take polynomial of real numbers, go modular x squared plus one. And then you recover the complex numbers and the complex numbers, we think of in terms of the imaginary element i. But that i is nothing but i is played the role of i is played by x over here.

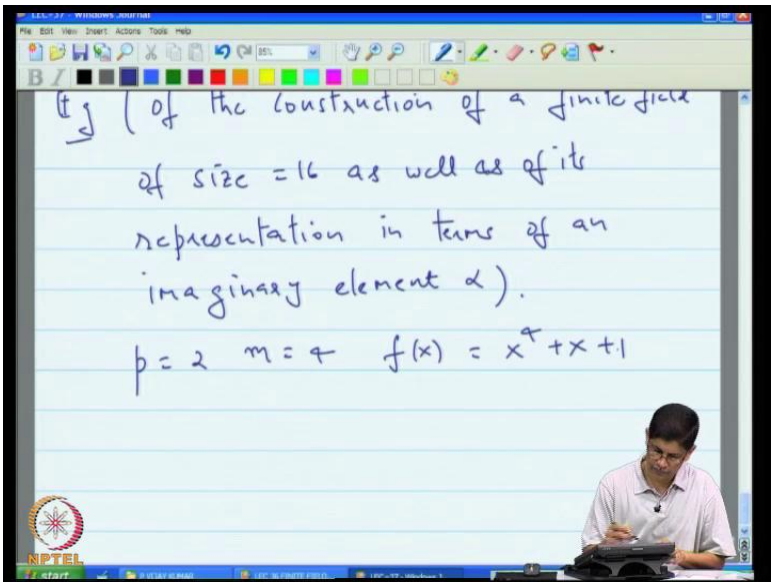
(Refer Slide Time: 30:20)



So, rather than work in polynomial equivalence class of polynomial, people find it easier to just say you know, that is really very combustive is in their easier way out. And in fact there is, because instead of going modular (x square plus 1), because modular (x square plus 1) means, please feel free be discard any multiple (x square plus 1), instead of that we bring in a prestigious element. I am having the property that (i square plus 1) equal to 0. And the movement we do that, this junction this prestigious element because this is equal to 0, it takes requirements that will discard multiples of (x square plus 1).

So, therefore instead of thinking this collection as a set of all polynomial of the form (a plus b x) and where you do multiplication module, you just work with (a plus i b). You just bringing the prestigious element i, and then that means that you do an long as provide you keep in mind the fact (i square plus) is 0. You no long have to actually, keep carrying along this modulo sign. So, in the same way now lecture thirty seven, we know that this is the feel, but combustion to keep thinking of it like this. So, what will do?

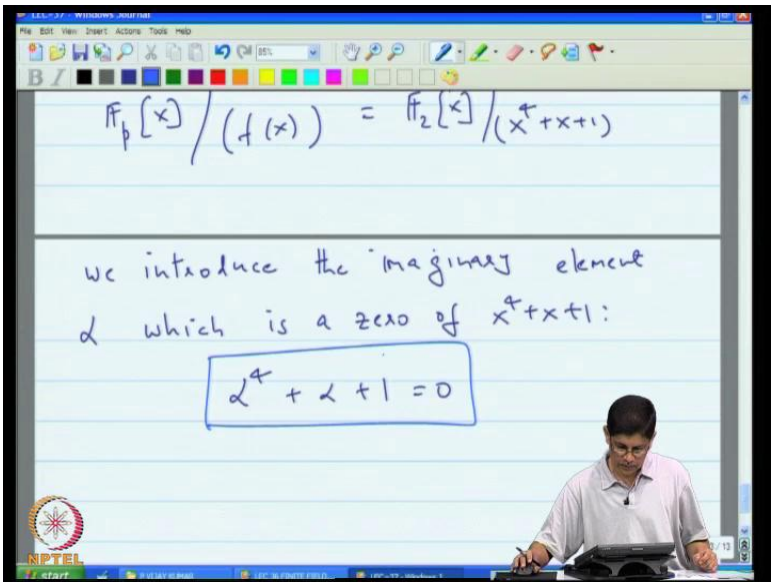
(Refer Slide Time: 31:40)



I will illustrated, this in so example of construction of the construction of a finite field of size equal to 16 as well as of it is your representation in terms of an imaginary element alpha.

So, here p equal to 2, m is equal to 4, f of x is (x 4 plus x plus 1) So, that means that strictly speaking one should consider the F p of x, modulo f of x or in other words, you should consider the set of all binary polynomials modulo (x 4 plus x plus 1) so which means that all your elements would look like polynomial.

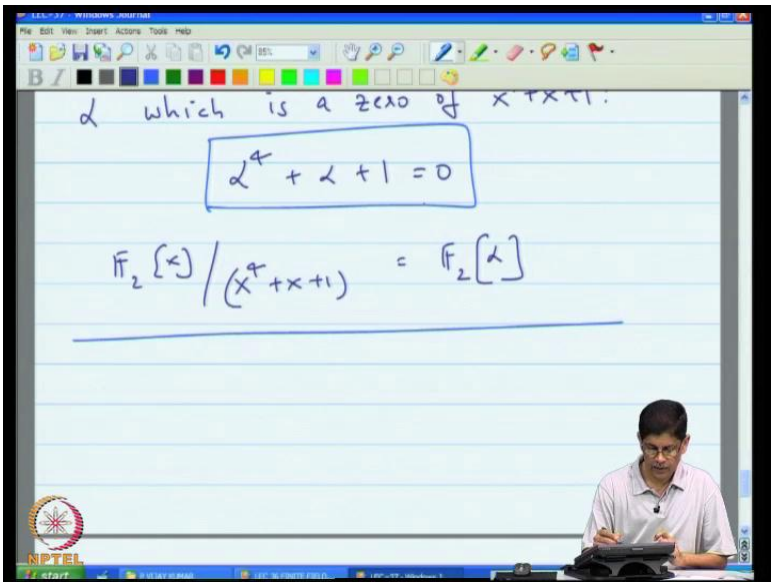
(Refer Slide Time: 33:05)



Now word about this, this is saying that sincere free to discard multiples of (x 4 plus x plus 1). That means that, you can actually replace (x 4 by x plus 1). So, what will do is instead of working in terms of x we introduce, we introduce the imaginary element. The imaginary element alpha, which is a zero of x 4 plus x plus 1, so what we mean is that alpha 4 plus alpha plus 1 is equal 0. We assume that will be the starting point. Now then then what happens is that, because we assume this to hold. Then F 2 of x, modulo (x 4 plus x plus 1) will be precisely the set of all polynomials in alpha. So, what is the finite fields end up looking like?

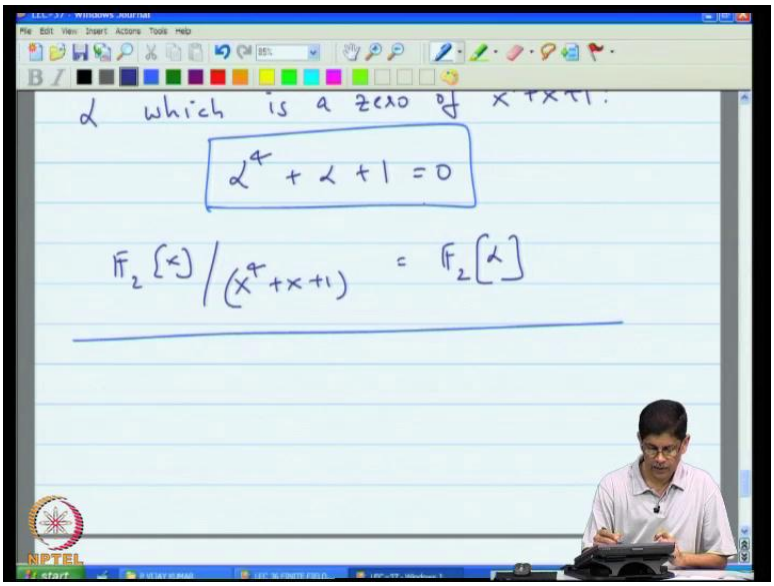
So, we can start, because alpha satisfies polynomial of degree. For every element in the finite field can be represented as the polynomial of degree of three or less.

(Refer Slide Time: 35:20)



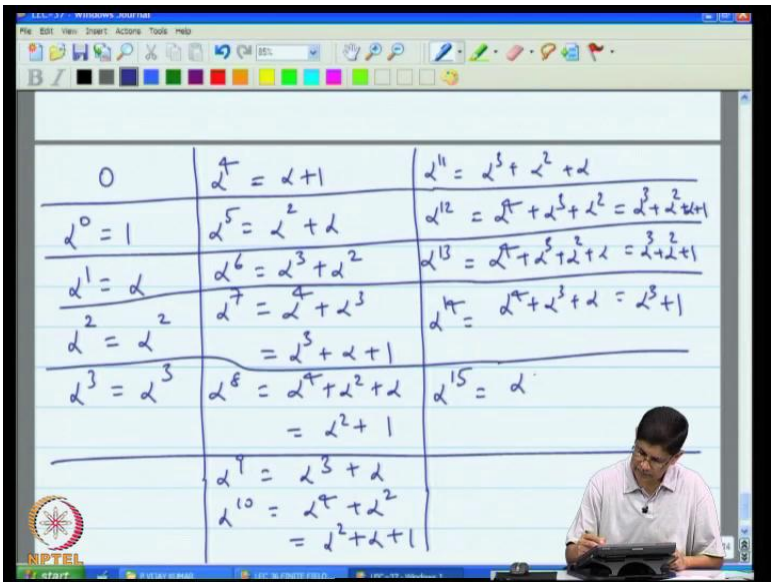
This tells you us that F 2 of alpha, which is finite field is set of all polynomial of the form- a i alpha to the i goes from 0 to 3, where a is be the 0 or 1. And it clearly sense the coefficient allows binary choice there are sixteen such elements. Now, so that would say that are finite field looks like… Now you consider every possible set of these coefficients and you will find out, there are you can think of them (( )). But here something interesting, supposing instead I do not do this by instead for reasons there will become here later.

(Refer Slide Time: 35:55)



What I am doing is, I start computing powers of alpha, because even this polynomial representation of the finite field is in the sense, not simplest representation possible. Because supposing you want to walk away with the mental image of a finite field, then thinking of them is polynomial turns out more complicate that, more complicated than it meet be … And will see that in just a second. So, instead of working with polynomials, let me start by taking powers of alpha.

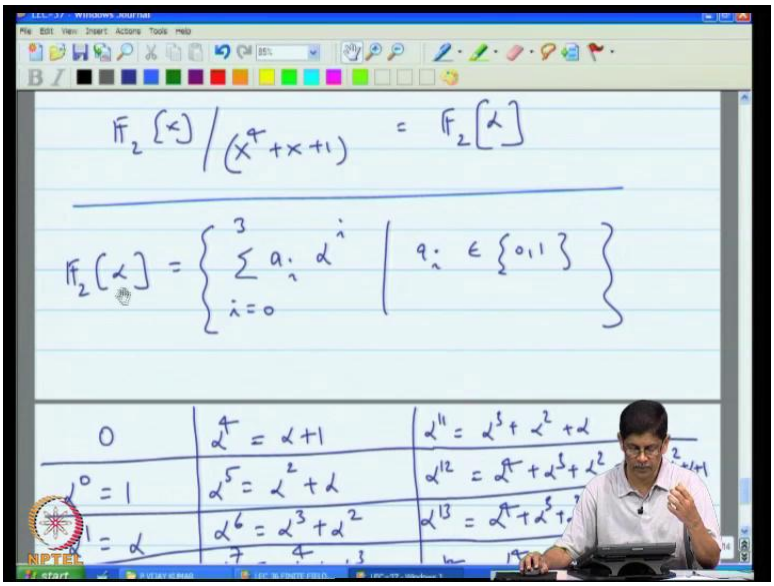
(Refer Slide Time: 36:42)



So, I start with of course let us start with 0 element and then will take alpha to the zero, which is 1; alpha to the 1, which is alpha; alpha to the 2, which is alpha square; alpha cube which is alpha cube. So, sounds like when our doing anything up to this point, but now, when it comes to the alpha to the 4, this is all of us sudden alpha plus 1 reason being, because alpha 4 plus alpha plus 1 is equal to 0 so alpha 4 is alpha plus 1. Then we go to alpha 5 is equal to alpha square plus alpha; alpha six is alpha cubed plus alpha square; alpha seven is alpha four plus alpha cubed. But since alpha cubed is alpha plus 1, this is equal to alpha cubed plus alpha plus 1; alpha eight is alpha four plus alpha square plus alpha, which is alpha squared plus 1. You can verify that, because alpha to the 4 plus alpha is 1 so alpha squared plus 1.

In alpha to the 9, alpha to the 9 is alpha cubed plus alpha. Alpha to the 10 is alpha 4 plus alpha squared, which is alpha squared plus alpha plus 1. Alpha to the 11 is alpha cubed plus alpha squared plus alpha. Alpha to the 12 is alpha 4 plus alpha cubed plus alpha square, which is alpha cubed plus alpha squared plus alpha plus 1. Alpha to the 13 is alpha 4 plus alpha cubed plus alpha squared plus alpha, which is alpha cube plus alpha squared plus 1. Alpha to the 14 is alpha 4 plus alpha cubed plus alpha, which is alpha cubed plus 1. And now, you have your lets go one more step and then I will say, I am say what I am going to say?

(Refer Slide Time: 39:58)

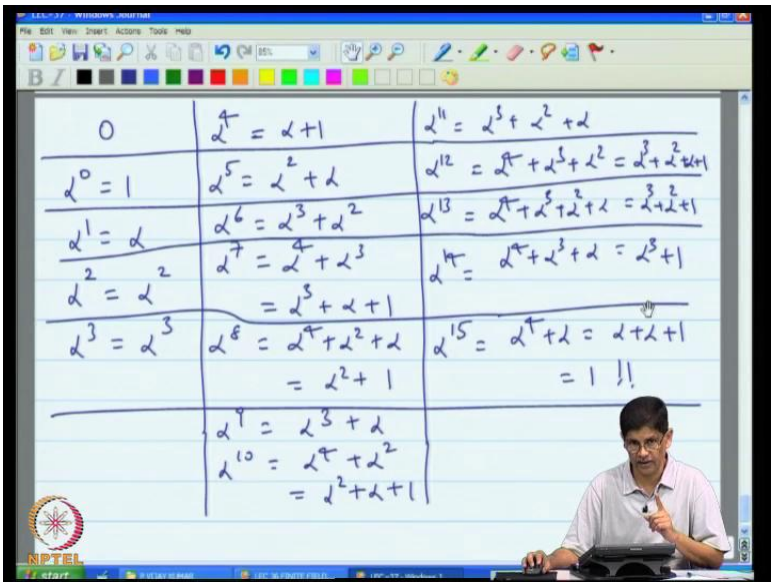


So, this is alpha 4 plus alpha, which is alpha plus alpha plus 1 which is 1. What is this? This looks most mystifying what exactly will we trying to do. Now, what I was trying to do is saying that, we started by saying the finite field looks like this. And we said we do not look like this. So, replace x by alpha and assume that alpha satisfies this equation. So this is very much like saying i square plus 1 is equal to 0, in the case the real and complex numbers. We just assume and we keep this the back up of mind satisfies this, then it is very easy to see that every element in the finite field, because it is polynomial in alpha. And whenever you get the degree 4, you can fold back using this expression. Using the fact this is zero that means alpha to the 4 is alpha plus 1. So, anytime you get up degree four, you can bring down the degree again. So, that means that you never have to go up to degree greater than 3. And on the other hand, it is clearly that every such element belongs to the finite field. The finite field that contains of these sixteen elements,

but next I would said wait a minute. That is not most convenient representation of finite field, because let us take a look, this is like magic. So, at least it magic if you looking at the first time so this is zero.

We are know, there is the zero is rather special element. All the other elements are non- zero. So, we put zero aside and then start working on non- zero elements. We begin with the alpha to the 0, which is 1 and then alpha square and we keep multiplying.

(Refer Slide Time: 41:23)

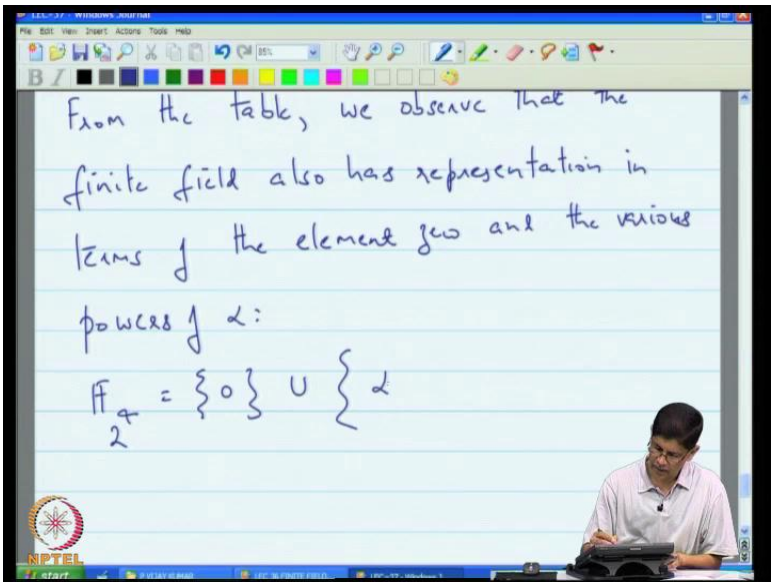


And we notice that as we keep multiplying, you keep every time you keep carrying new polynomial degree of 3. Every of degree 3 or less, you always end up with degree 3 or less polynomial, you can check. And number of such polynomial is sixteen and every one of them is going to appear here. You can check one, two, three, four, five, six, seven, eight, nine, ten, eleven, twelve, thirteen, fourteen, fifteen, and sixteen so they should have been sixteen polynomial degrees of three or less. And every one of them applied here

For example, you might say what about alpha cube plus alpha squared plus 1? Let us look for it, we look for it and then sure enough you see that alpha cube plus alpha squared plus 1. Any polynomial degree of three or less is to be found. But at the same time, that we see from this table is only one representation of the element from a finite field.

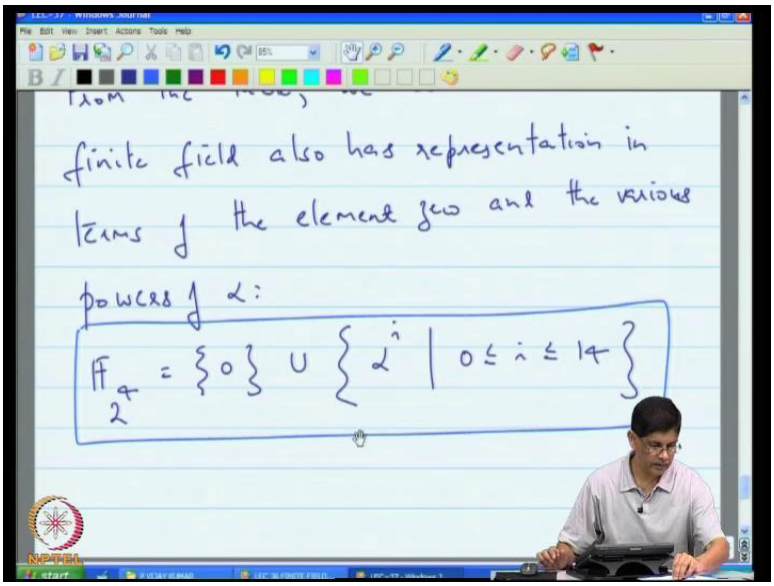
There is another surprising representation in that is in terms of powers of alpha; ranging from alpha to the 0 to alpha to the 14. Alpha to the 15, we have to ignore, because after all this is the duplication of a previous element. But of the there are two elements here. This is the duplication of the previous element. So, we do not compare is the different element. So, the conclusion is that now, this is interesting phenomenon. But later on, we see that this is the part of the structure of finite field. That every finite field has the beautifully simply structure.

(Refer Slide Time: 42:49)



From the table, we observe that the finite field also has representation in terms of the element 0, and the various and various powers alpha.

(Refer Slide Time: 43:52)



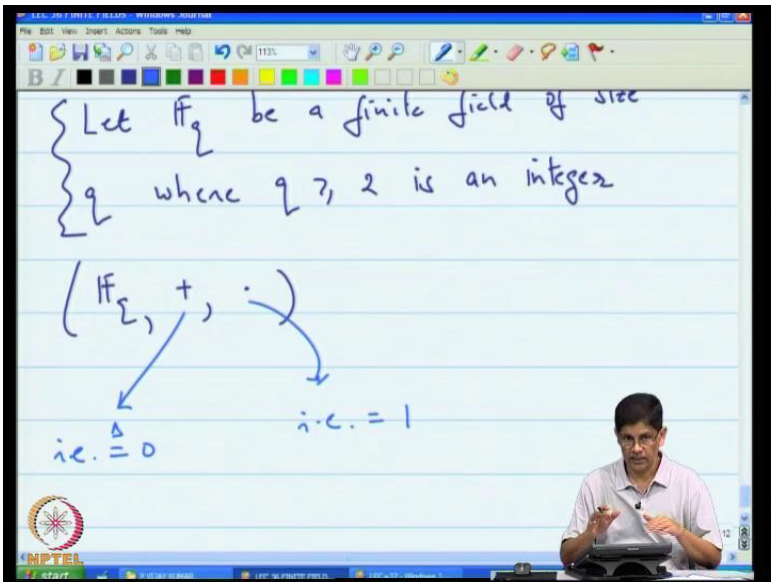
So, that means that is your F the finite field of 2 to the 4 element can be represented form 0 union alpha to the i, where i ranges between 0 and 14. And the interesting and very useful point is every finite field has such a representation. So, in fact the finite field can be represented every finite field can be represented in these two ways. That is one is, where all the elements are represented in terms of polynomials in this imaginary element alpha. On other hand, they can also be represented as powers of an imaginary element alpha. Now these imaginary element alpha, there is you have to exercise little bit of care in choosing it. But not too much and it is not difficult.

So, that is so now giving you constructions for finite fields and hopefully, now you know to construct a finite field of any size of the form p to the n. For any prime p and any integer m greater than or equal to one. Now what we want to do is, remember I told you that we are going to take two different approaches of finite field and the first is the constructive approach. We just completed the constructive approach. Now we actually going to take on the deductive approach, we are going to put on different hat on say okay.

Supposing I am in armchair, I am just relaxed and I am say okay, I know that I am in finite field. And I know that it has to have satisfies certain actions, what I can deduce? Just from the

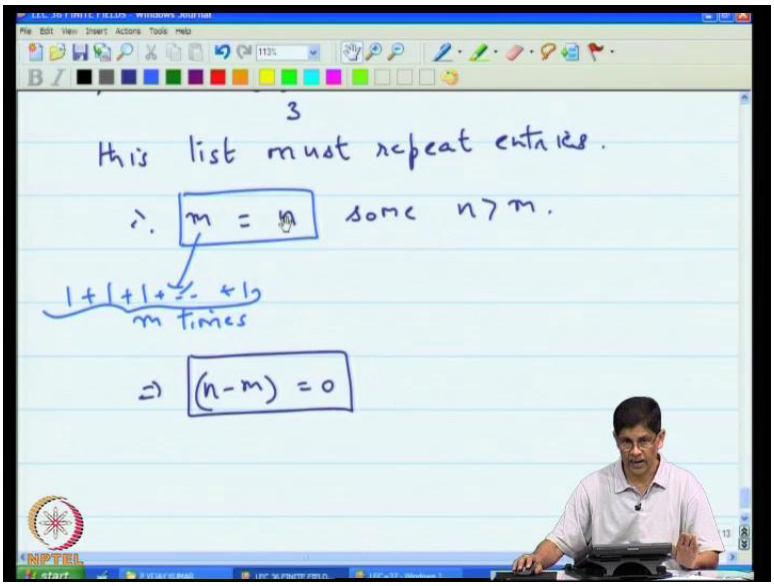
knowledge, there is the finite field. So, that is what will try to do next. So, I call this deductive approach to finite fields.

(Refer Slide Time: 46:00)



So, all that we do a starting point is here. Let F q be a finite field of size q where q greater than or equal to 2 is an integer. Now, we know that the finite field since it the finite field, we know that there are two operations plus and this. And we know that associatively each of these operations, you have the identity element. So, under plus there is an identity element, which we will take to be 0. And under multiplication, this is an identity element which we will take to be 1. Now, look at the obstruct object and all that we know above it is that it is a finite field. But we know, because it must satisfies the axioms of finite field, that they must be an identify identity and they must be a multiplicative identity. So, in terms of notation, we are going to denote multiplicative identity by 1 and the (( )) identity by 0.

(Refer Slide Time: 48:03)

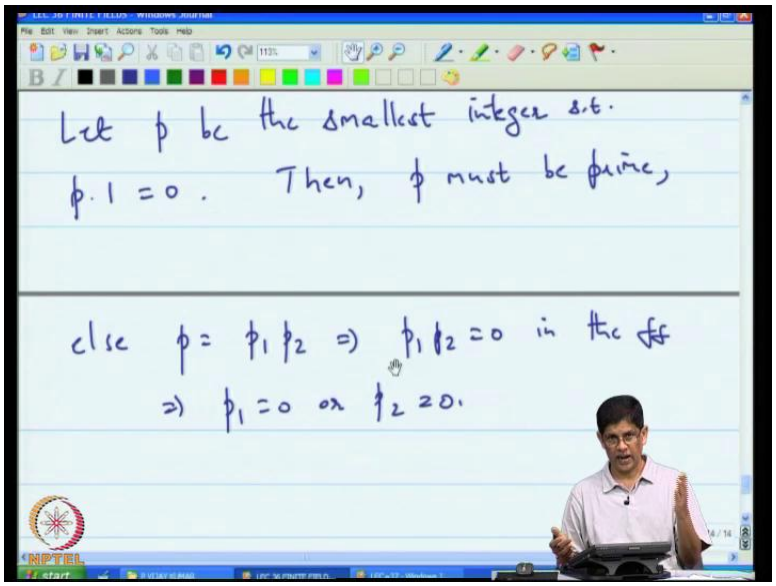


Now, let us to let say if this finite field contains one so F q we know there it contains 1. Therefore, it contains 1, 1 plus 1, 1 plus 1 plus 1, 1 plus 1 plus 1 plus 1 and so on. Now, let us when we will write this have 3 means, 1 plus 1 plus 1. That is what we mean in the finite field. Now since the field is finite, this list keeps going on and on and on forever. So, it must be there must be some repetition in this list. So, this list must repeat entries, which means that all the entries in the list cannot be distinct. Therefore, m is equal to n for some n greater than m. It must be that never do mean by m; m simply means m 1 plus 1 plus 1 plus 1, m times. That is what we mean when we say m.

And similarly, when I say n what I really mean is, 1 plus 1 plus 1 plus 1, n times. But if this is true, this implies that n minus m is equal to 0. Why do I say that? What I really mean is that? Look, here you are adding n one. So, think of n is seven m is five; here you adding seven ones and here you adding five ones.

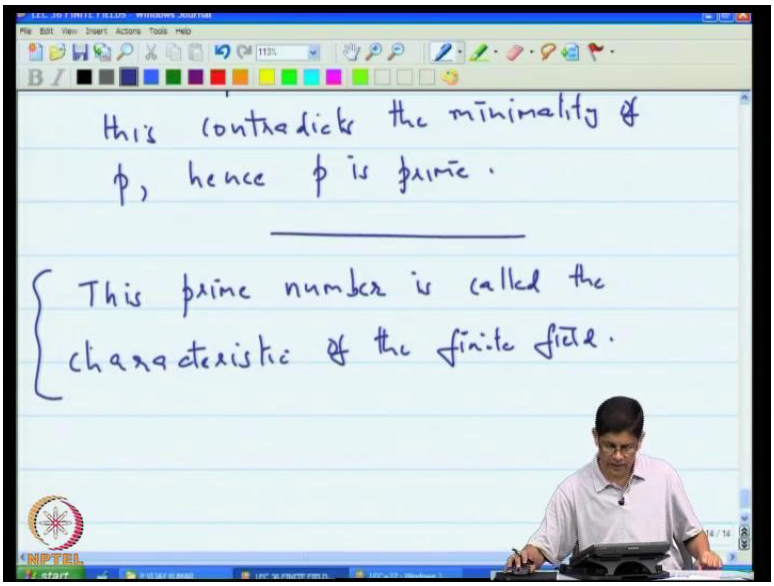
So, the difference between the two is two ones. If five ones are equal to seven ones, then I can cancel five of the ones by adding minus one five times to the left and to the right. And I am left to the fact that two ones is equal to 0, of two is equal to zero. That means that n minus m is equal to 0.

(Refer Slide Time: 50:22)



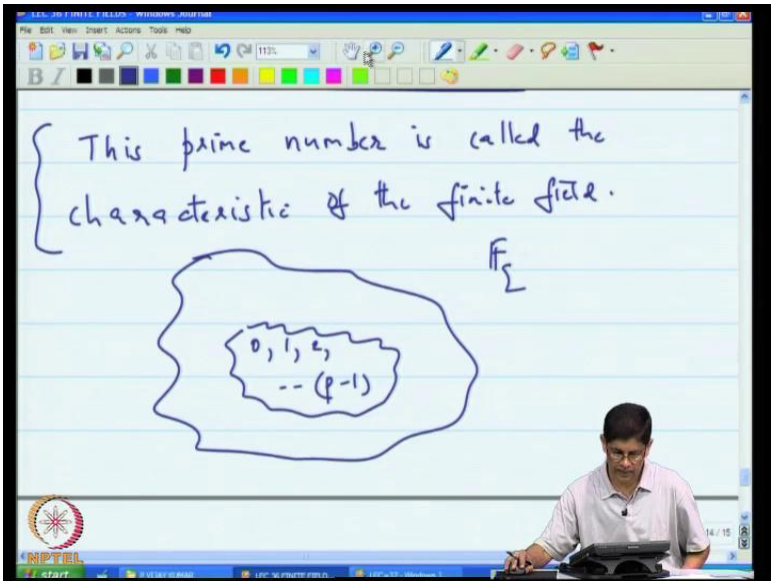
So, let you can think of this n minus 1 time 1 is equal to 0. Let p be the smallest integer such that p times 1 is equal to 0. Then p must be prime, why because else if not p is p 1 p 2 implies that p 1 p 2 is equal to 0 in the finite field. But that forces p 1 equal to 0 or p 2 equal to 0. Because every integer which is not prime can be factor into product of two integers, each of which is less than p. So for example, if you add six if p was six, let say you could say that three times two was equal to zero. But then either three ones had to add zero, two ones had to add two zero. That means either so that is the contradiction. Because we assume that p was smallest integer with this property. This contradicts the minimality of p, hence p is a prime.

(Refer Slide Time: 51:50)



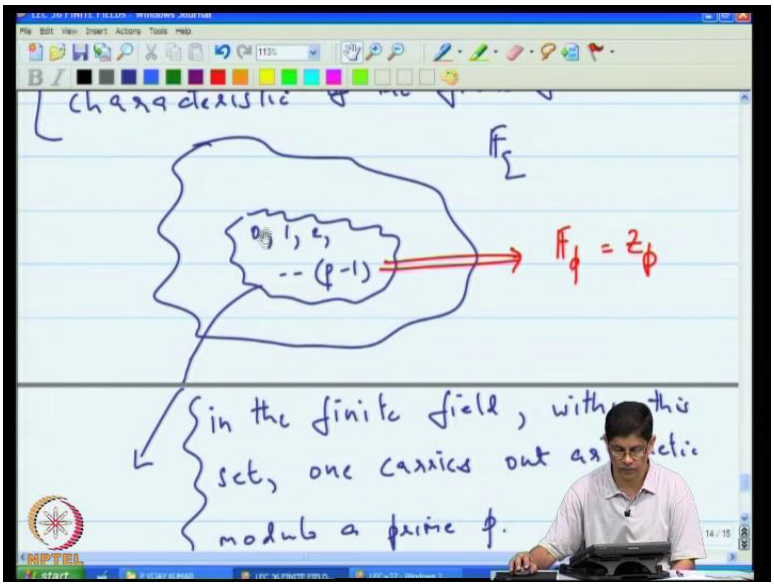
So, we found out the first we deduced the first fact about the finite field. The interesting fact that any finite field whatever size q, there is some prime number such that, if you add the identity element to itself, the prime number of times you get zero. And will just say that p is zero, so this prime is called the characteristic of the finite field.

(Refer Slide Time: 52:40)



This prime is called the characteristic of the finite field. But if you think about it so here you have the big finite field. Then inside it, you have certain reasons 0, 1, 2 up to p minus 1. What do I mean weather two, I mean one plus one and p minus one I mean is one plus one plus one plus p minus one. Now however p is zero within the set the way I add and subtract is according to modulo carry arithmetic.

(Refer Slide Time: 53:55)



So, in this set so in the finite field, in the finite field within the set, one carries out arithmetic modulo a prime p. What that means is that think about it, that this is really nothing but the finite field sign p which is the integer mod p.

So, that means because for all purposes, you can pretend that you work with integer modulo p. Why is that, because the same rules apply in the integer modulo p as well as set here, p is 0. You treat p as 0 as here well and you adding just integer here, you are adding integers there. So, that means now what you do is you identify this the subset with the integers modulo p. And then what you have is interesting situation, when you have the lager finite field F q containing the smaller finite field f p.

So, that is the point which we start today. So, today what we did? So, as that we completed our construction of the finite field. So now, you have with your method of constructing any finite

field of size p to the n of any prime p and any integer m. The only ingredients that you need are the irreducible polynomial of degree m over f p. But that can be found through text books. So, now you have to construct the finite field of the size p to n. Then we said okay. Let us now go back to the deductive approach and see what can we deduce about the finite field? Just from the knowledge, that the field is finite. And we already seen that the finite field must then contain a prime number, a very special prime number called characteristic. And there it contains a smaller field whose size is equal to the characteristic and will pick up the discussion from here and next class.