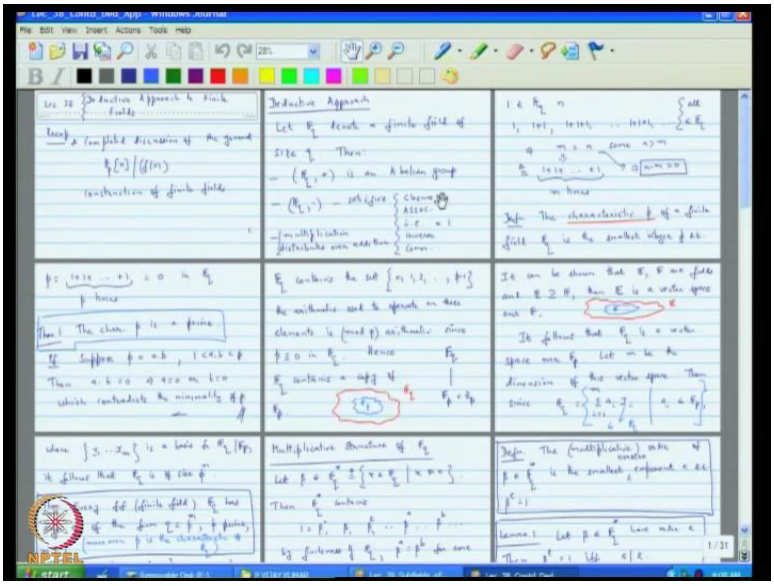
Error Correction Codes
Prof. Dr. P Vijay Kumar
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore

Lecture No. # 39
Subfields of a Finite Field

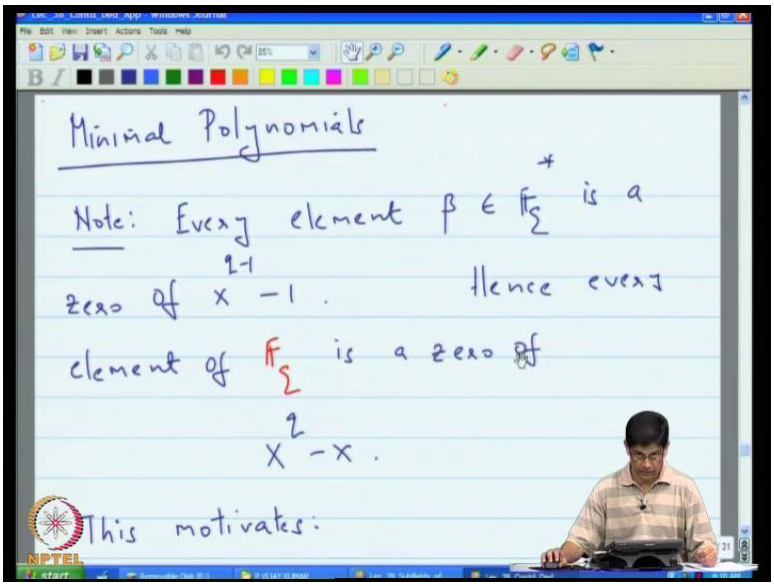
Good afternoon. Welcome back. This will be our thirty ninth lecture, we just have a few more lectures to go. So, as always let me just run through an overview of what we did last time.

(Refer Slide Time: 00:33)



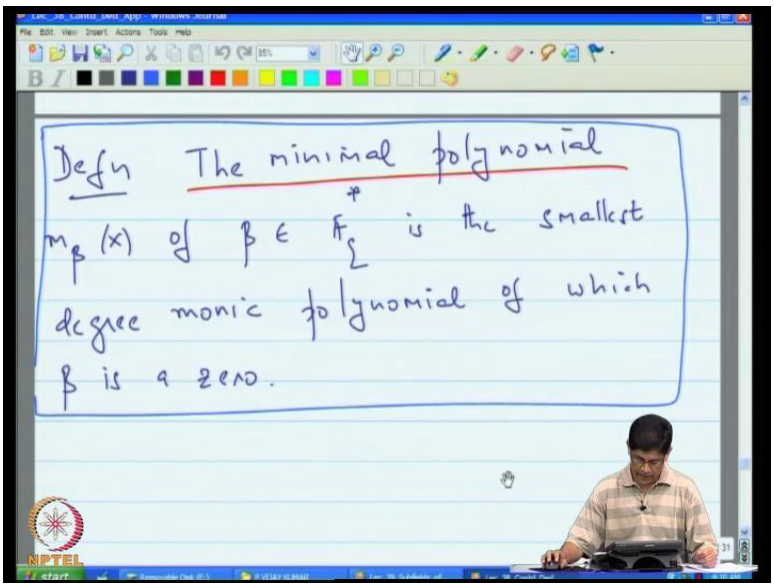
So, last time we were on the topic of taking a deductive approach to finite fields. And then we started by talking about the characteristic of a finite field, we show that it is a prime use that to show that the size of a finite field is must be a part of prime, because it is a vector space over the ground field. After that, we moved on to multiplicative structure of a finite field, and what we were able to show is that multiplicatively, it has a simple structure, all the non-zero element are passed for single element. And there after we showed that we moved on to talking about polynomials. We said we defined the minimal polynomial of an element as the smallest degree polynomial of which element is true. So, let me just begin over there.

(Refer Slide Time: 01:52)



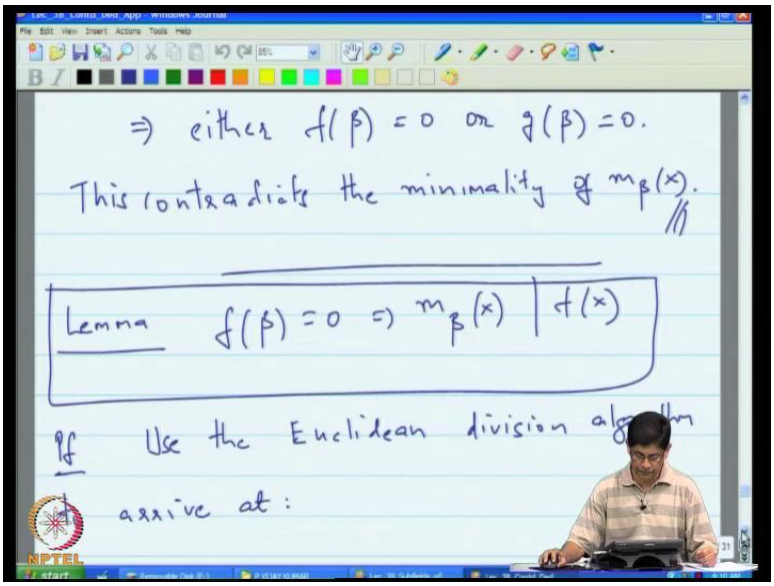
So yes that definition of minimal polynomial, the smallest degree polynomial of which the element is 0.

(Refer Slide Time: 01:58)



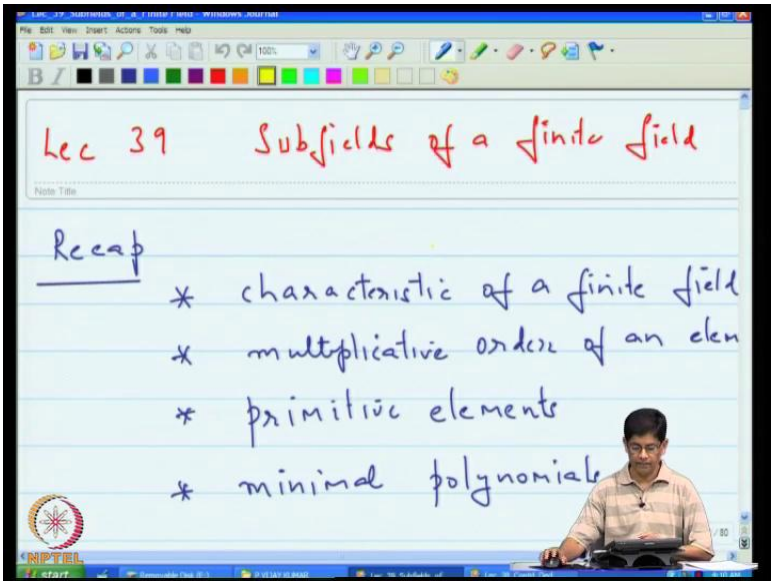
And so we were actually going through the theories of the minimal polynomials, what we actually proved is the minimal polynomial of any element is irreducible.

(Refer Slide Time: 02:08)



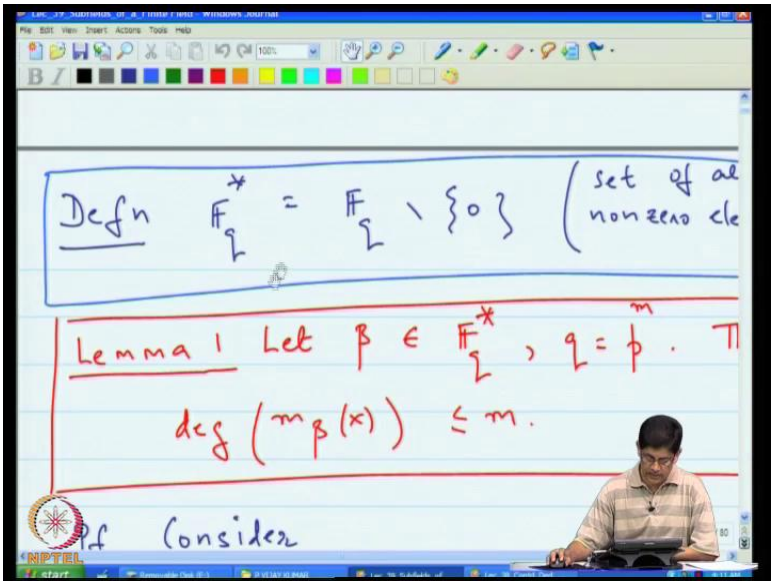
There is f, f beta is 0 then the minimal polynomial must divided and as corollary that n beta of x divides x to the q minus x, it is not about everywhere. So, we will continue on that today, I have called the subfields of the finite field, but actually this lecture designed to take you to subfields and beyond.

(Refer Slide Time: 02:28)



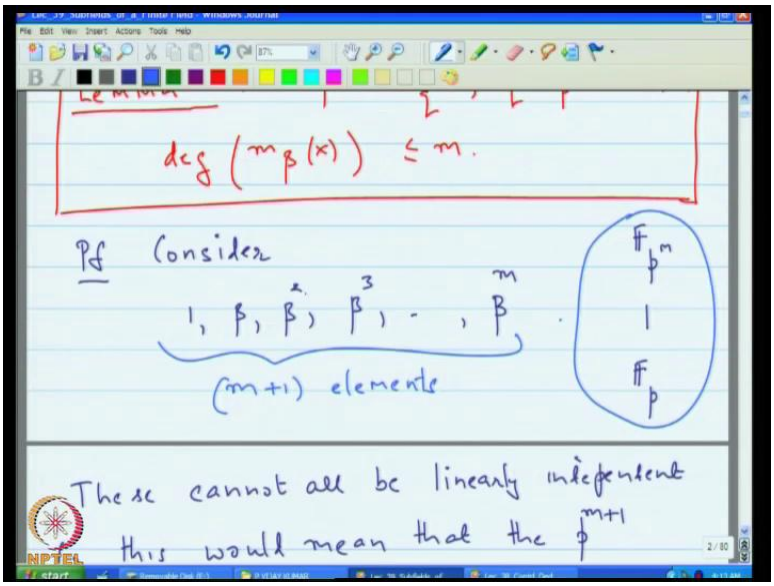
So, let us see how far we can get today. The recap is we talk last time about the characteristic of a finite field, the multiplicative order primitive element; that is the element having maximal possible multiplicative order, and minimum polynomials. Now, we want to we would like to begin by saying the little bit more about minimal polynomials.

(Refer Slide Time: 03:05)



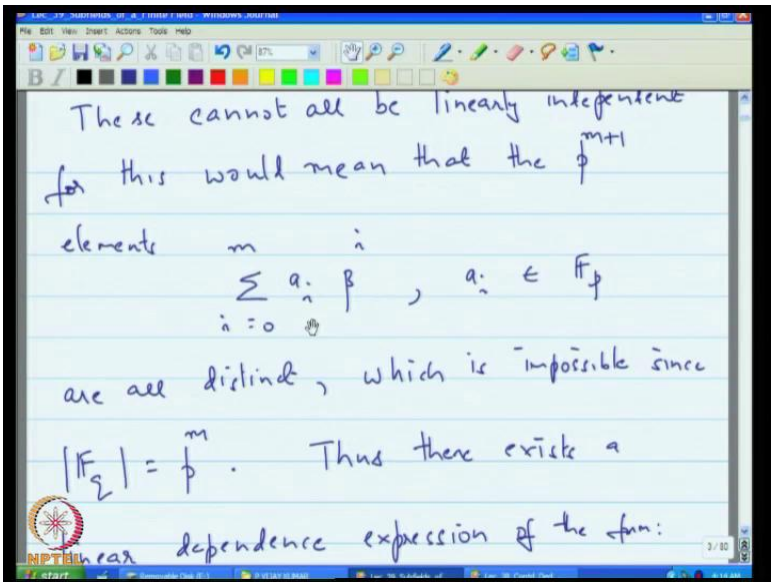
So, first of all let us defined and as I think in the past lecture, what I have done is in the interest of making sure that I get through with the felly complete discussion on cyclic codes, I have pre returned the slides. There is a small danger that I will go to fast, I try to guard against that try to slow down little bit. But many case you have this slides in front of you, so that should make it is a… So. let us get started. Now just quickly introduce some notation, we will use F q star to denote the non-zero element of the finite field.

(Refer Slide Time: 03:46)



And the first lemma states that look if beta is a non-zero element of finite field, where q is power of prime p, then the degree of the minimal polynomial beta is less than or equal to m. So, this m is same m that appears in exponential m. How do you prove that? Now, what do you do is, you consider successive powers of beta, so one beta, beta square beta to the m. Now this is total of m plus 1 elements in here, starting from beta to the 0, beta to the m. These cannot all be linearly independent, because supposing they were all linearly independent; linearly dependent over what excuse me, so what I mean here is linearly dependent. So, we are actually thinking about the following picture, we have F p, and then we have F p to the m. So, we have a smaller field sitting inside a big field. So when I talk about linear independence, what I mean is that I am going to regard this as the vector space over smaller field. I mentioned earlier that as possible.

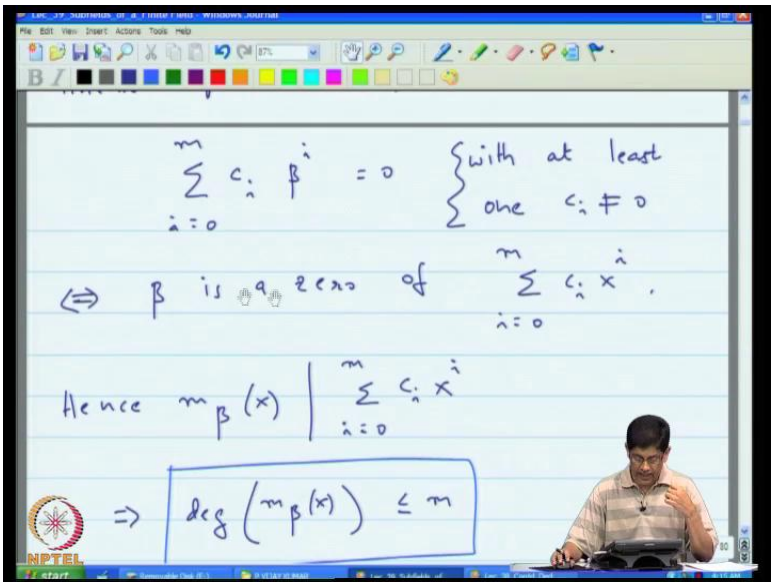
(Refer Slide Time: 05:14)



So, from that point of view there are m plus one element here they cannot all be linearly independent, because if they were then the set of all linear combination of these elements. That is where the a i so let us emphasize that the a i, the a i comes from F p set of all linear combinations are all distinct, that is property of linear independent elements. If any two are the same, that would imply linear dependence relationship among (( )) beta, and assuming they independence.

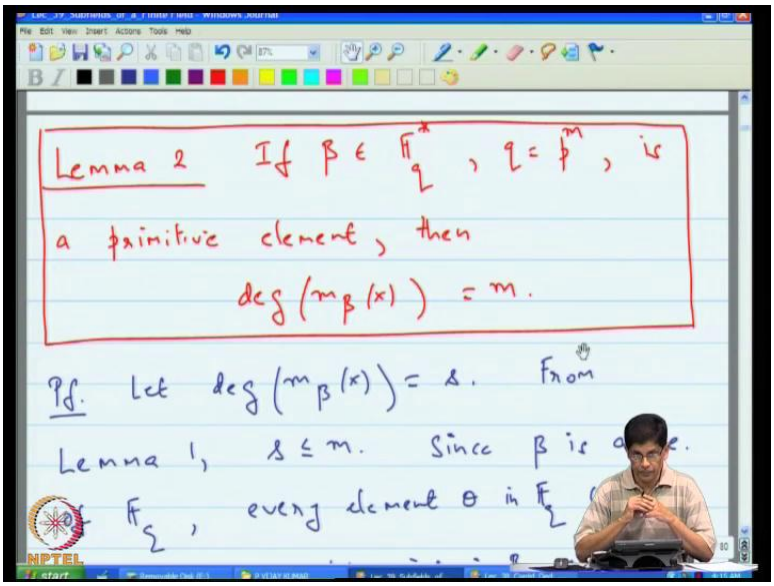
But the total number of term this form just you count the number of coefficients, there are n plus 1, and each coefficient you have 3 choices, so that makes the total of p raise to the m plus 1. But that is impossible because after all the finite field only of size p to the m, so the number of elements cannot be larger than that so only conclusion we can draw from that is that these particular set of m plus 1 elements is not a linearly independent.

(Refer Slide Time: 06:40)



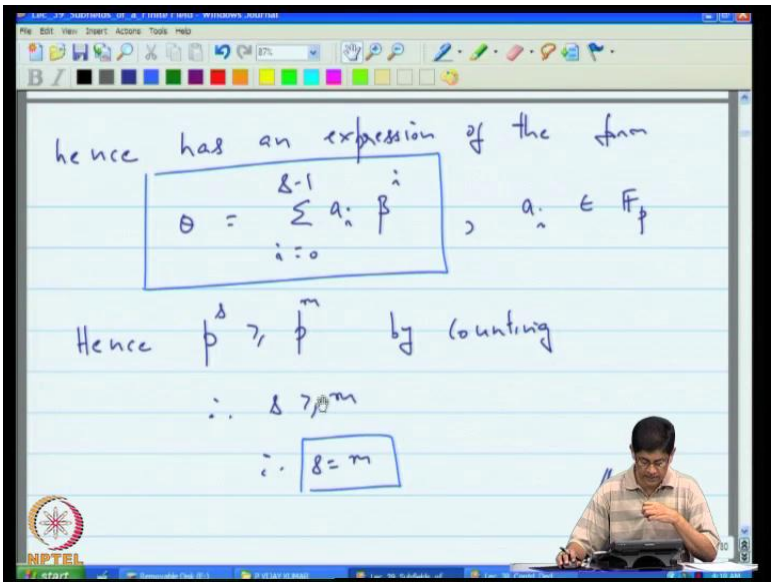
Let us assume that particular dependency expression takes on this form that is the sum c i beta to the i is 0 is at least one of these coefficient be non-zero. But that that is the same thing I am saying here that beta is a 0 of polynomial c i x to the i. So, but then if that the case minimal polynomial divides any polynomial of which beta is 0. So when particular polynomial must divides this polynomial with this polynomial has degree n, so the minimal polynomial must have the degree less than or equal to m so that is have the proof of course. Again if you got lost in little bit of technical details, it does not matter, just keep it mind that if finite field of size p to the m and you take non zero element its minimal polynomial is gone to less than or equal to m.

(Refer Slide Time: 07:31)



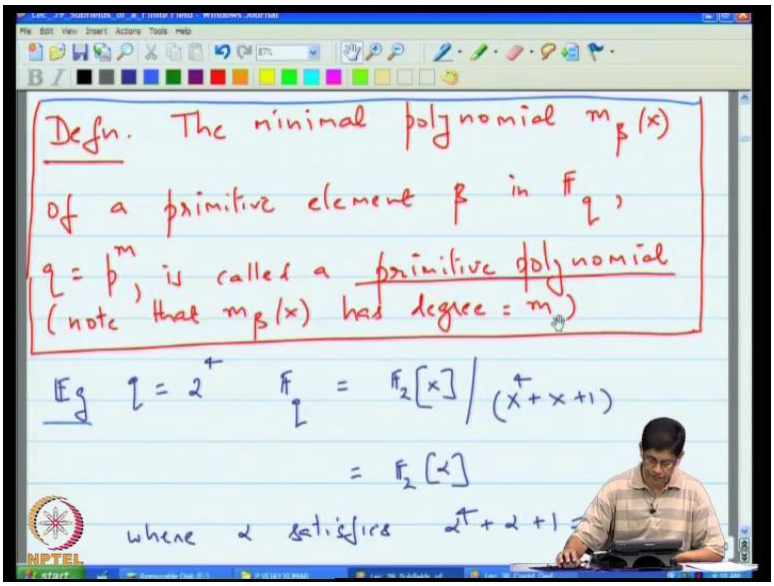
On the other hand, here is other lambda but that is true, but if this particular element beta is the primitive element, it is not just the non-zero element, it is a particular kind of non-zero element it is primitive that means every non-zero element in finite field is the power of this beta. In this particular case, we can actually, said that the degree must be exactly equal to m. What is it makes that the difference? Let us say that the degree of minimal polynomial of beta is s. Now we already know from that earlier lemma that s less than or equal to m, because you are dealing with the same finite field. Since, the degree is less than the exponent from the size of the field. But since beta is a primitive element in the finite field every element theta in the finite field can be expressed as a polynomial in beta.

(Refer Slide Time: 08:31)



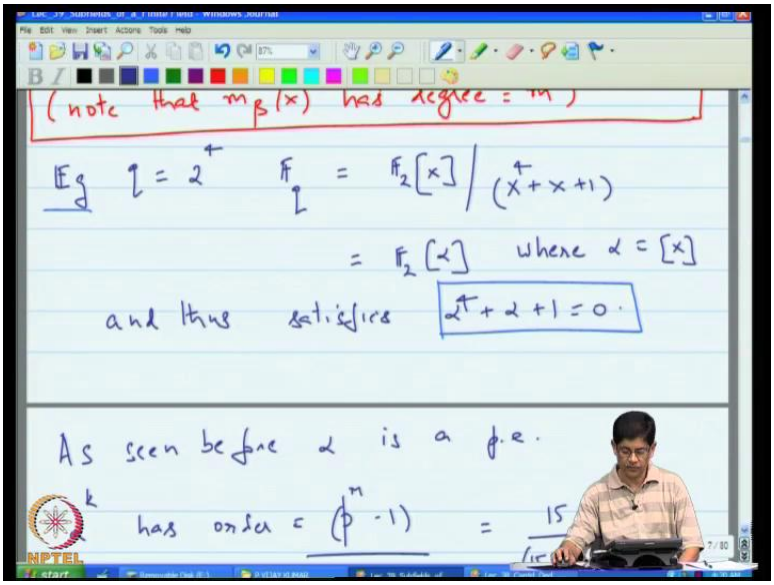
And therefore, has an expression of the form theta equal to sum i is 0 to s minus 1 a i beta to the i. Why is that? While the minimal degree has s, so that means beta to the s is dependent on lower power of beta. So, we never have to cross an exponent of beta larger than s minus 1, because we run into the s beta always re expressive in terms of lower lesser power of beta. Reason theta can always be express like this, but then the total number of elements here is only p to the s, because there are total of s coefficients a i so again emphasize that lets remind as the a i come from F p so the total number of elements of this form p to the s. But since the every element in theta in the field is to the s p to the s is greater that p to the m this by counting from that s is greater than m and, but we just went through proving that s is less than m combining the 2 we defined s is equal to m.

(Refer Slide Time: 10:17)



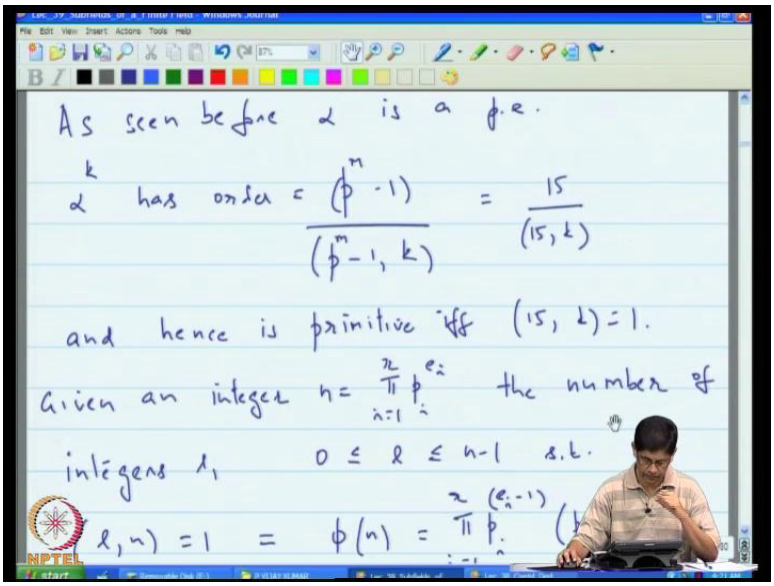
So, again the result is easy to remember if you deal with primitive element minimal polynomial degree is m, m is so called exponent to the size of finite field. Just definition that we will need to call upon later at the minimal polynomial beta of x so the notation for the state the same, when beta is a primitive element in the finite field then m beta x is called primitive polynomial. And we already seen that primitive polynomials had degree m we just saw that in the previous lemma.

(Refer Slide Time: 10:50)



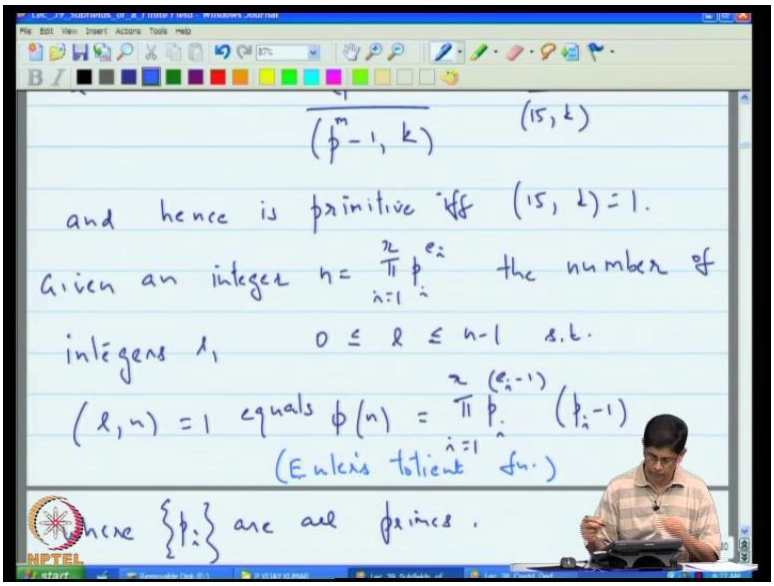
Let us take an example, supposing q is 2 to the power of 4, then the finite field of 16 element in example construction of that you seen this. You take the polynomials of binary coefficients, and you reduce modulo to the polynomial x 4 plus x plus 1. And this also be express in the form F 2 polynomials in alpha, where what we have actually done here is where alpha really denotes the equivalence class of x in this field. And thus, so limit is modify that were say alpha equals this and thus satisfies this thus satisfies particular equation.

(Refer Slide Time: 12:11)



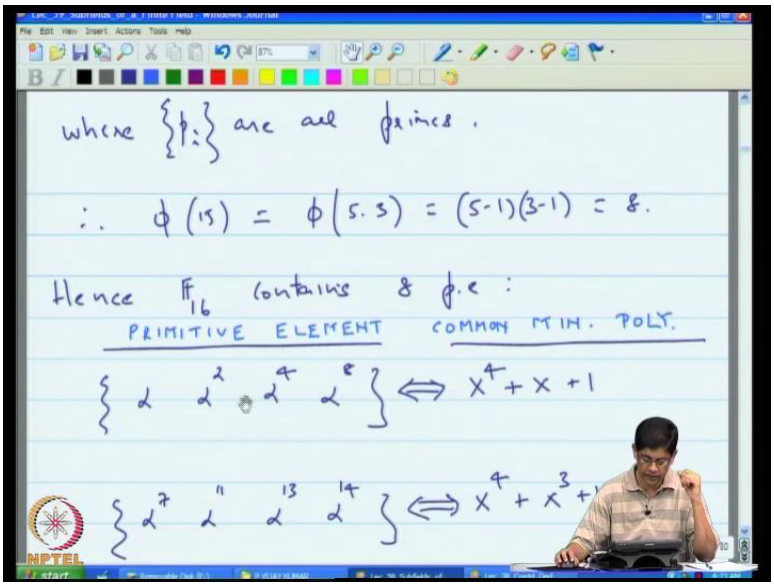
As seen before so when we examine these finite fields earlier we remarked of that particular alpha is a primitive element. So, that means if we take a power of alpha. Let say alpha to the k. And alpha to the k has the order p to the m minus 1 divided by the greatest common divisor of k, and the order of alpha, which is p to the m minus 1. So that in this case is 15 divided by the greatest common divisor of 15 and k. And from this you see that, what I am what we trying to get here is, what are some examples of primitive polynomials? The only way in which this think could equal 15 and 15 and k where relatively prime so that means alpha is the primitive element, and the powers of alpha in the form alpha to the k, where this integer are exponent k is relatively prime to 15 these are the elements which are primitive in the finite fields.

(Refer Slide Time: 13:45)



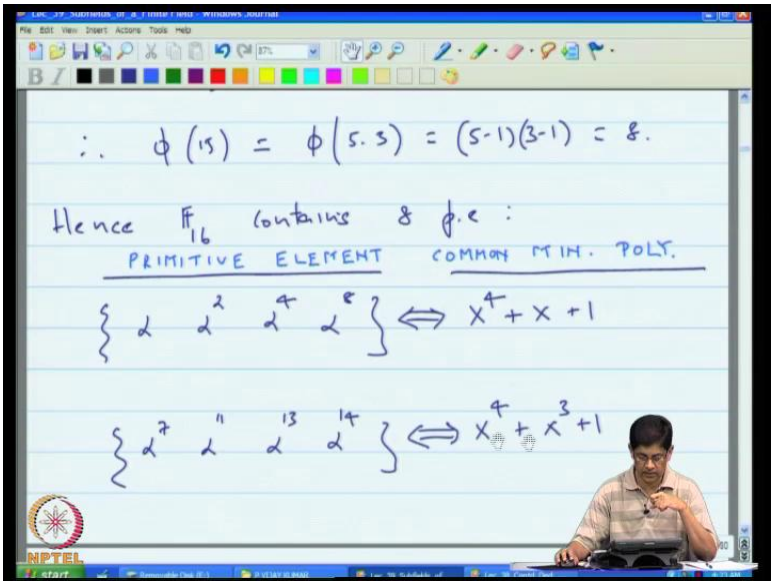
Now as an aside it turns out that if you are given an integer, which the product of primes, distinct primes, the number of integer l, where l is strictly less than n such that l and m are relatively prime is given by, so let us write this have it in words. So, that is not this little confusing, equals this function is called Euler totient function. So, this is the formula. So, its says that if you are original n is the product p i to the a i to b i and you want to find the integers that less than n and relatively prime to it. Then what you do is now look at the factorization reduce the exponent by 1 multiply by p i minus 1 and you get it.

(Refer Slide Time: 14:29)



In our particular case, phi of 15 is the same asking what is phi of 5 of 3 is 5 minus 1 and 3 minus 1 which is 4 times 2 which is 8. So, what that means is that field of 16 elements contain 8 elements that are primitive.

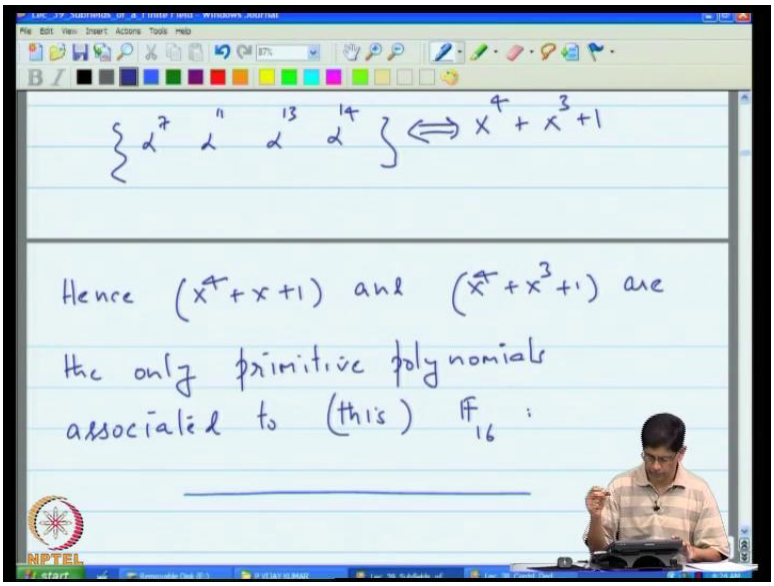
(Refer Slide Time: 14:54)



And now those 8 elements corresponds to powers of alpha, which are relatively prime to 15, so and which are less than 15. So, the integers posses the property which are 1 2 4 8 7 11 13 14

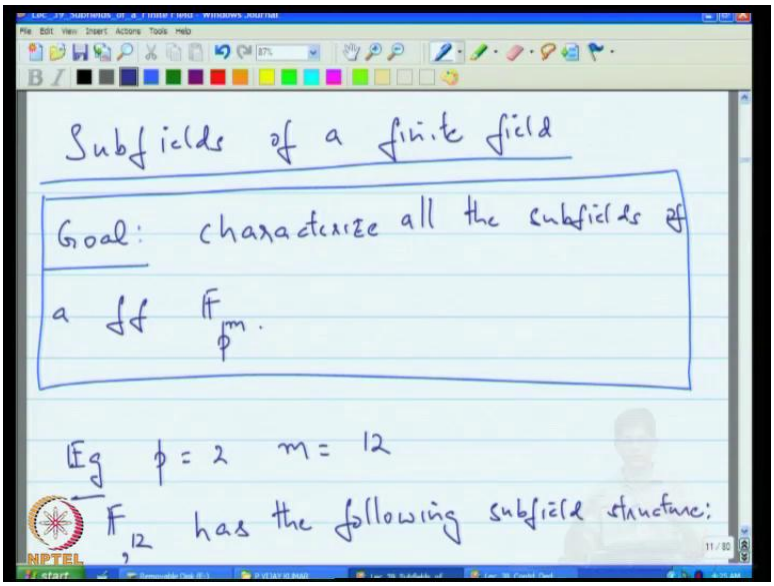
these are the 8 exponents k, which are such that are relatively prime to 15. So, these are primitive elements, and there are 8 of them and I have group of them together in this particular fashion for a reason. The reason is that these four primitive elements share these minimal polynomial and common; these 4 primitive polynomial elements share this minimal polynomial and common, these 4 primitive share this minimal polynomial and common. So that is the reason for writing it out for grouping them together like this.

(Refer Slide Time: 15:45)



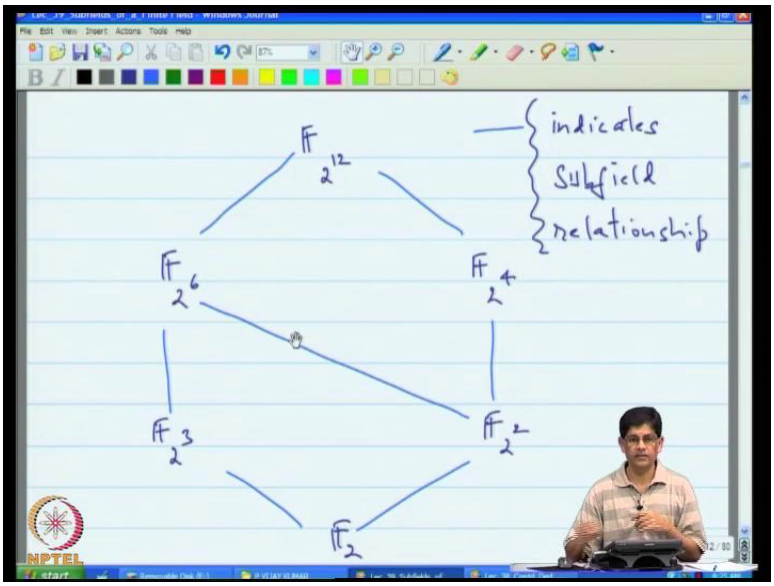
Thus so in this particular field it turns out X 4 plus X plus 1 and X 4 plus X cube plus 1 are the only primitive polynomials associated to this particular finite field. But as it turns out for all finite fields are really same, so this turns out to be true for all finite fields. So, I am just going to write this and brackets and just put down here as 16.

(Refer Slide Time: 16:28)



Now the next topic, so we are going to do little bit of jump that there is a certain theory of finite fields that we will be using in the equals or else it is something that I feel we should actually know. So, we will visits all these various aspects and sometime there will follow very nice continuously but sometime there will be little bit of jump. So, now we make a jump, we want to discuss sub fields of finite field. So this is the situation when we have the larger finite field containing a smaller finite field. So, our goal, our immediate goal is to characterize all the subfields of a given finite field F p to the m, and it turn out such a characterization possible, clearly keeping it mind this size in finite field its best illustrated with an example, when p is 2 and m is 12, when we talking about the finite field F 2 to the 12 elements it turns out has the following subfields structure.

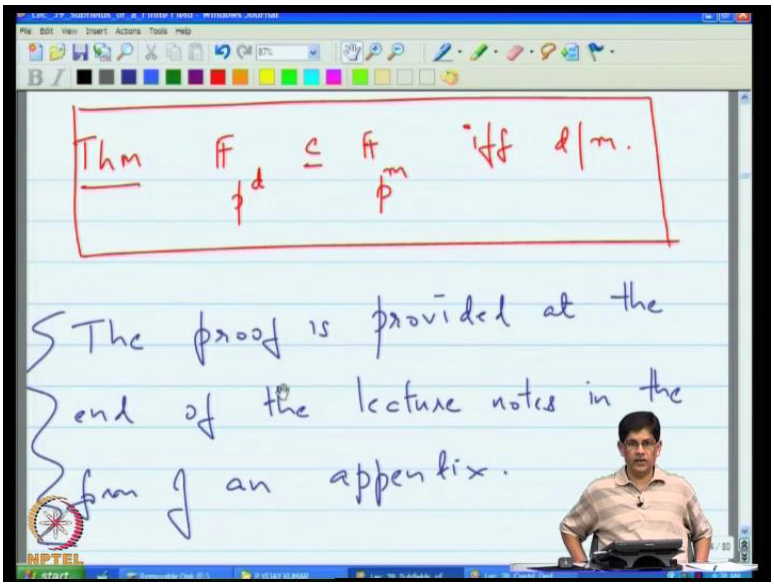
(Refer Slide Time: 17:39)



It has this, so here is the field itself, here is the ground field F 2, and we have the already know of it presence. We know that is the finite field contains corresponding fields obtained, which corresponds to the characteristic of finite field. So, we were already know aware of these two. It turns out the only other field of size 2 to the k, where k divides 12, and the divides of 12 are 6 4 3 2, there are all shown here. In this figure, whenever we draw a line like this, what we mean is that the element above contains the elements below.

So, F 2 to the 12 contains either by link by link by single or multiple lines it is also true that F 2 to the 12 contains F 2 to the 4 which contains F 2 to the 2, and therefore, it is clear that F 2 to the 12 contains F 2 to the 2. So, just by inspection we can see that containment simply requires that the exponent divides each other; for example, the reason is the F 2 to the 12 contains all these fields, because this appetites this all 12 alright we have 1, 2, 3, 4, 6 and 12. That exactly what I have actually written out here that the subfields are all of the form F 2 to the k F 2 to the k divides 12.

(Refer Slide Time: 19:19)

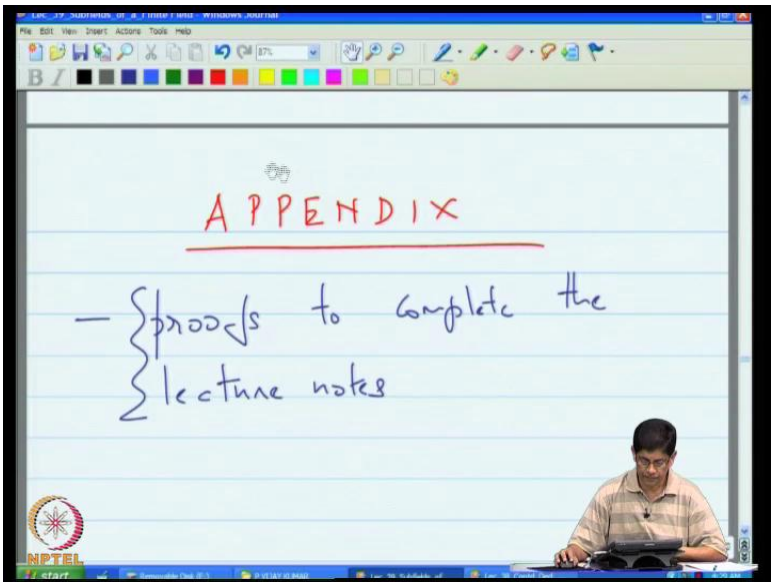


And this is not an isolated instant. It turns out that in general, in general, whenever you have the finite field whose size is part of the prime p that size p to n. Then the only finite field, we have contain in sided have size p to the d, where d divides m. Now, it is clear that any two finite fields measure the same characteristic, because they share the same multiplicative identity 8 to finite field with one contain each other, measure the same identity. And because they do they must have the same characteristic in common, because you take 1 1 plus 1 and sooner later set number 1 add to 0. And if add to 0 the bigger field, it must add to 0 in the smaller field.

Therefore, whenever you talk about one finite field contain the other it is clear that the characteristic is same. Now, we actually saying the only other condition that you really to meet is that when you consider the size, the exponent of p must have the following divisibility property that d divides m, whenever this is contained in this. This is an if and only if statement.

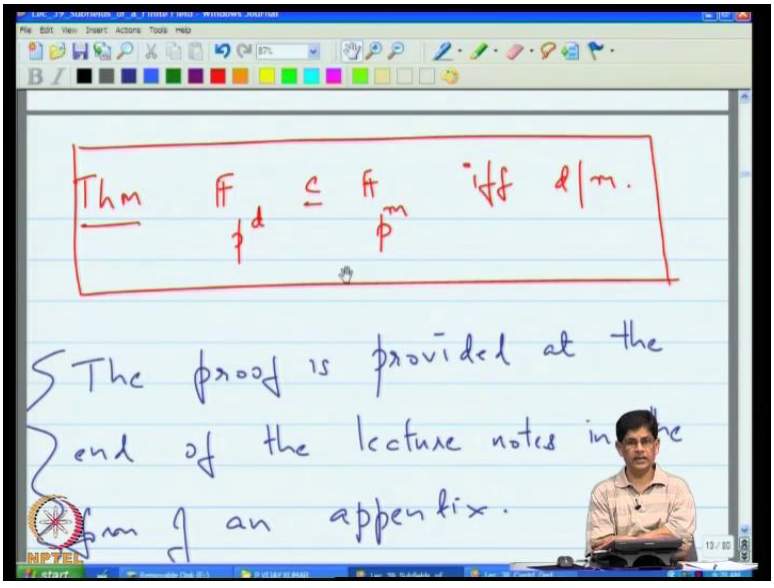
Now what have done is actually skipped the proof of this theorem in the meant x or proof incomplete form of in the appendix, what you do mean by appendix? Well, I took the liberty of putting towards the end of the lecture you know, so if you just zoom go down.

(Refer Slide Time: 21:10)



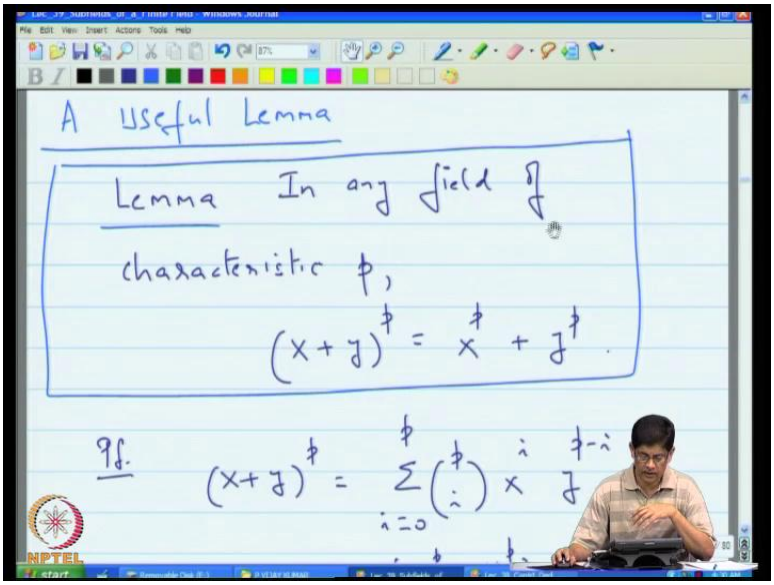
As around the middle, the little after the middle, you will see the page 48 in my particular version, which says appendix in this contains the proofs to various theorems. There appears in lecture and whose proof is perhaps too long for us go through at this stage; let us get back to everywhere.

(Refer Slide Time: 21:27)



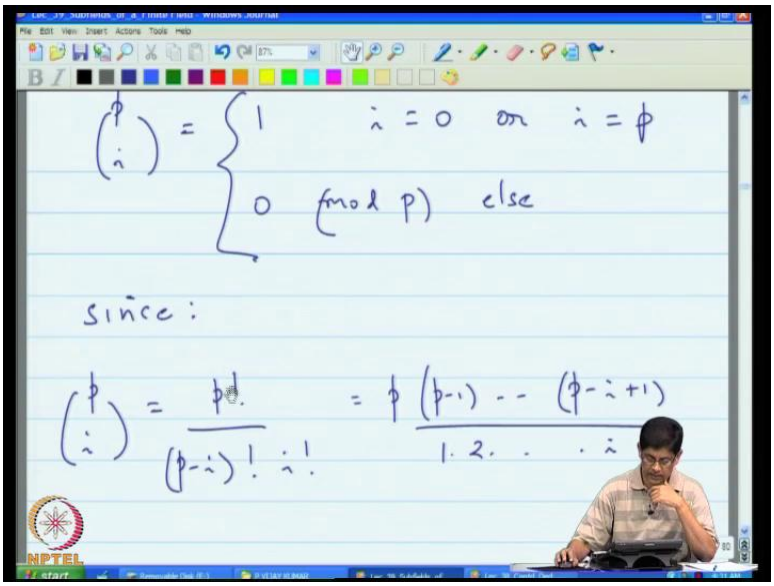
So, basically this is the relationship necessary and sufficient condition for a finite field to container sub field. This so again making a short jump now and giving a useful lemma, not really related to the previous discussion on sub fields.

(Refer Slide Time: 21:41)



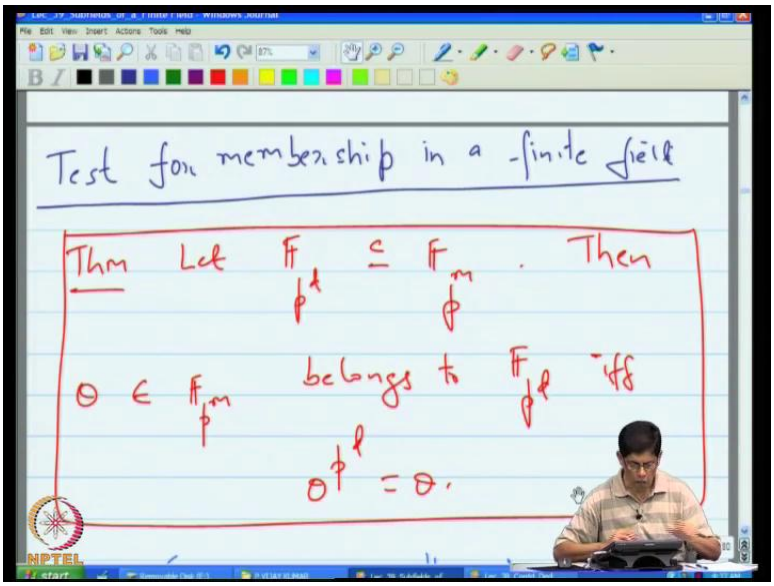
And lemma states that in any field of characteristic p x plus y to the p is x to the p plus y to the p. How do you prove that? You just carry out the binomial expansion, so x plus y to the p is sum i is equal to 0 to p p choose i x to the i y to the p minus i. Now this turns out that there are actually p plus 1 times i, but it work it out only two term two extreme terms survive, the others vanish, because if you look at this binomial coefficient p choose i it turns out that except for extreme case, when i is 0 or i is equals to p.

(Refer Slide Time: 22:41)



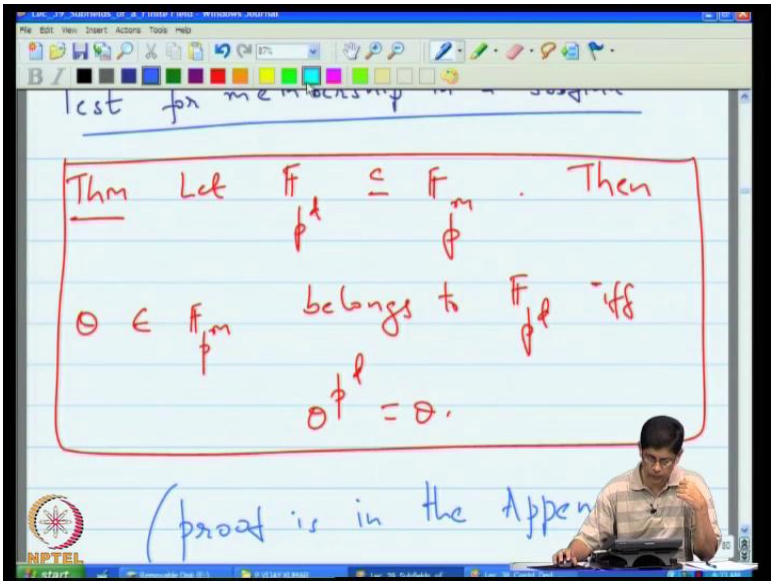
All the other values vanish modulo p, which means that because the multiple of p does not have to see, because when you write it out all p to choose its p factorial divided by p minus i factorial times factorial. So, that is p into p minus 1 and so on upto p minus i plus 1. And then you have one 2 to i, And you can see the this is the multiple of p because all these others are p does not divides any of the others and we think prime cannot have any of these factors containing the denominator. So, it follows that p divides it entire quantity, and hence and when you go modulo p this thing become 0. So, that x plus y have rather simple binomial rule in though the finite field characteristic, we just applying p well.

(Refer Slide Time: 23:52)



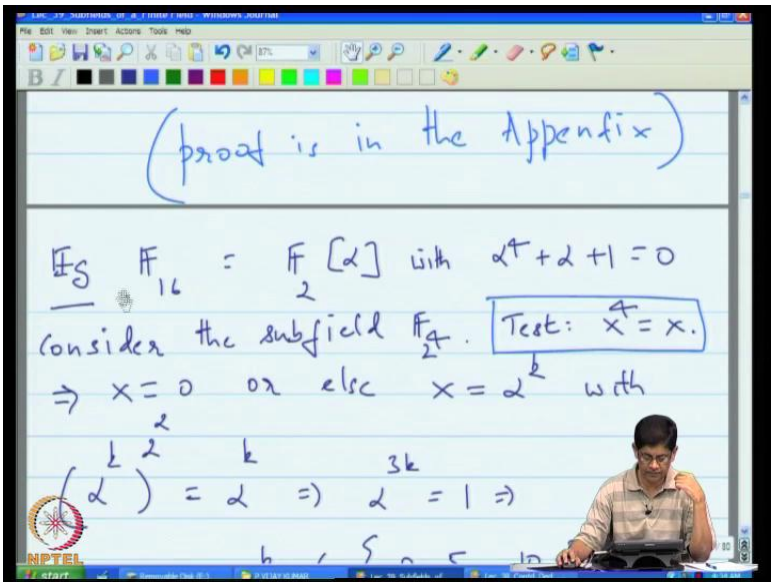
Next going back to subfields of a finite field, what I have listed here is test for membership in a finite field. So, let say that you have a finite field for size p to the m and you have F p to the d contain F p to the m. Then the theorem says that if you want to test the membership in a subfield of finite field, so I should modify this little bit.

(Refer Slide Time: 24:44)



So, I think to the following going to write test for membership in subfield. So, let us simply says that if you want to know whether or not the particular element theta belongs to the subfields of size p to the d, then you just says theta to the p to the d theta power and then you get theta. And you know that theta belongs to this fields then it must satisfies the equation of this. But this is saying that not only is this necessary it is also sufficient, the proof once second is in the appendix. The proof is again does not completely in appendix, what I think it is perhaps more is I will give an example.

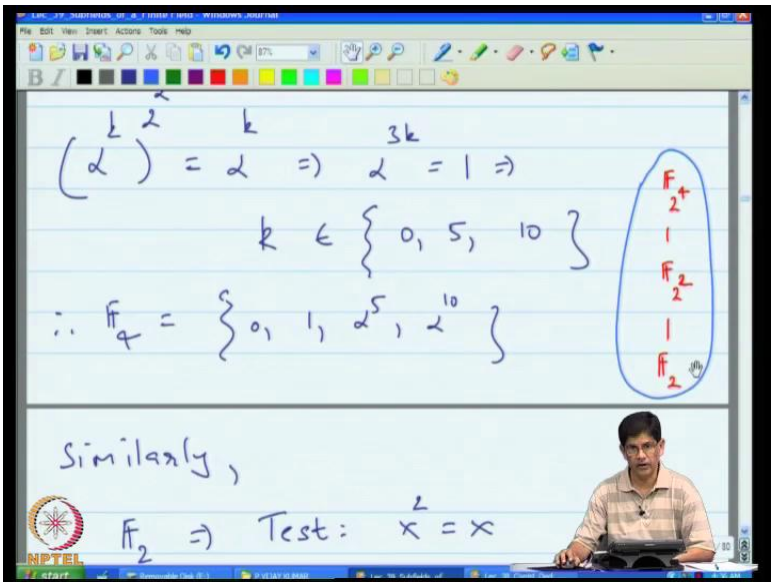
(Refer Slide Time: 25:55)



So, let say that F 16 is F 2 of alpha this notations means the set of all polynomials in alpha is coefficient line F 2, where alpha satisfies the relationship alpha 4 plus alpha plus 1 is 0. Then in this field, we know that F 2 to the 4 is subfield of this. Consider the subfield F 2 to the 2, consider sub field F 2 to the 2, and the test for this is to makes to verify whether is not true that x to the 4 takes you back to the x. But x to the 4 equals x even can happen because x is 0 or else if x is equal to alpha to the k as every element can express the power of k alpha, when it is non-zero with alpha to the k raise to the 4 power giving you back alpha to the k, but that can only happen this is now just alpha to the 4 k so this is alpha to the k. So the only this is happen is alpha to the 3 k equal to 1, but that is the same as saying that k is 0, 5 or 10.

So therefore, in this particular case, the subfield test has lead us to this particular set as being the sub field of the field of 4 elements; that is 0 1 and alpha to the 5 and alpha to the 10.

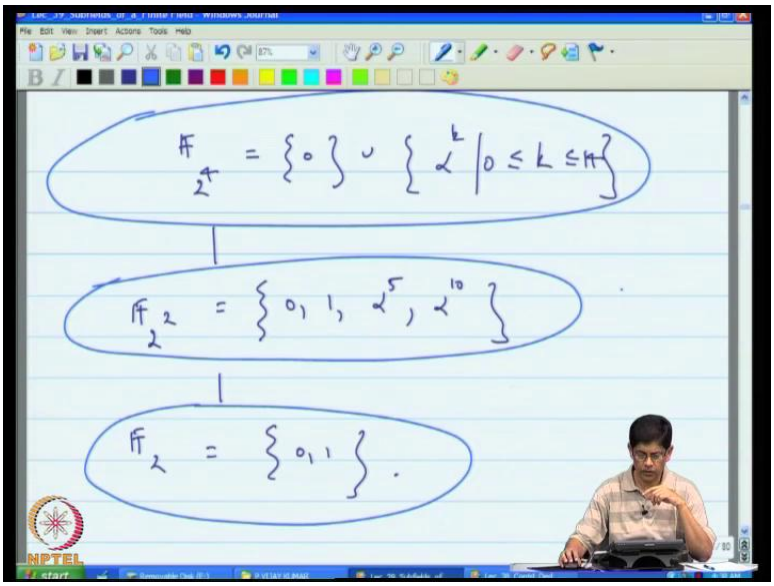
(Refer Slide Time: 27:44)



Similarly, supposing now so in this particular field that we are considering, you really have 2 subfields; you have F 2, we have F 2 to the 4. And then in the middle, we have F 2 to the 2, so these are your our subfields. So, we have already seen just now the test for membership in these particular subfields, how about membership in this subfield all the way at the bottom. Again you applying the the same rule, because this holds for all these cases, because set for all you need to check the exponent d divides exponent m. So the test is to whether or not x square is equal x, but the only way the x square is x can happen if x is equal to 0 or else x is alpha to the k with alpha to the 2 k equals alpha to the k that is when I plug in x equals alpha to the k here. But if alpha to the 2 k equal to alpha to the k that implies alpha to the k is 1, this implies the only way it happen is 0.

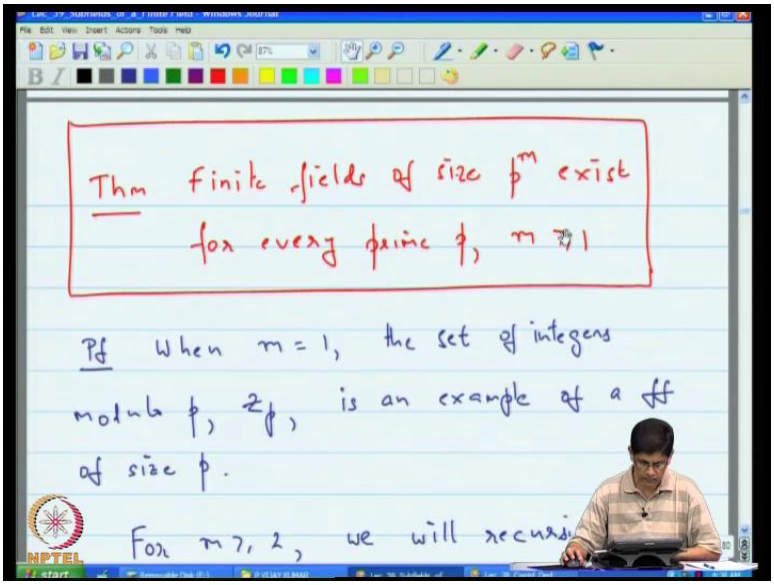
Therefore, it finite field the elements in the, but still appetizer the alpha to the k is 1 this implies the only way this can happen. If this k is 0 therefore, the finite field elements in subfield F 2 a precisely those corresponding to x is equal to 0; and the element x equal to alpha to the k so 0 and 1 element in subfield. So this is just verification, because after all we already knew that these two elements where in subfield.

(Refer Slide Time: 29:46)



So if you put together this discussion that we just had in lecture that is you have the ground field, the parent field and then we have any subfield here. And these are precisely the element in the subfields. So, we have 0 1 which belongs to the ground field, this is the particular subfield, and this is the entire field of sixteen elements. Now on to another topic, we have been proving several topic of finite field.

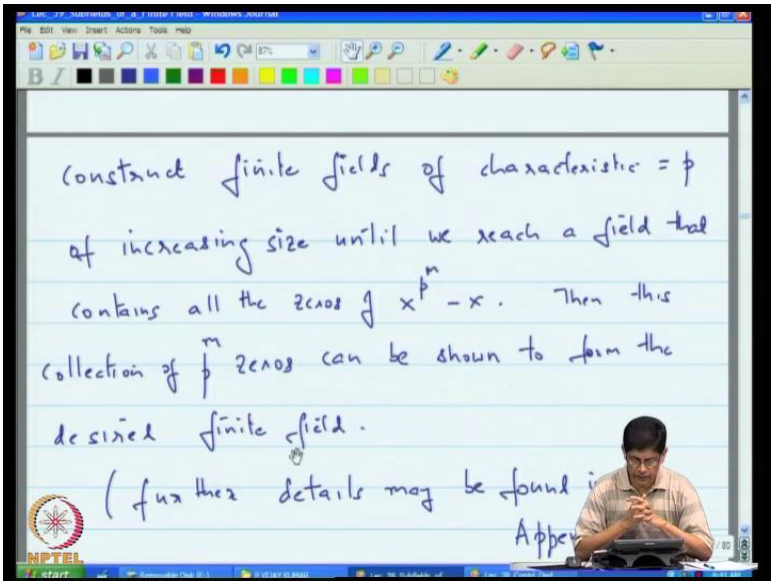
(Refer Slide Time: 30:15)



I have shown you the construction of finite field p of size p to the d provided certainly reducible polynomial degree of certain x. So, the aim of this theorem here is to tell you that is to give you another way of showing that finite fields every size of the form p to the m exists. As long as p is prime of course, and m is greater than or equal to 1 what I have done here sketched, I have just sketched the proof here of this theorem. And I have left the complete proof to the appendix, finite of back of few notes in (( )). So the theorem says that finite field exists of every size of this form.

And when m is equal to one, the set of integers modulo p z p is an example of a finite field of size p. And we are already familiar with that, if you are using that the more interesting case when m is greater than or equal to 2. So, how do you construct finite field of size p to the m equal to 2? What will you do in this case is? That we will recursively construct finite field of characteristic p of increasing size.

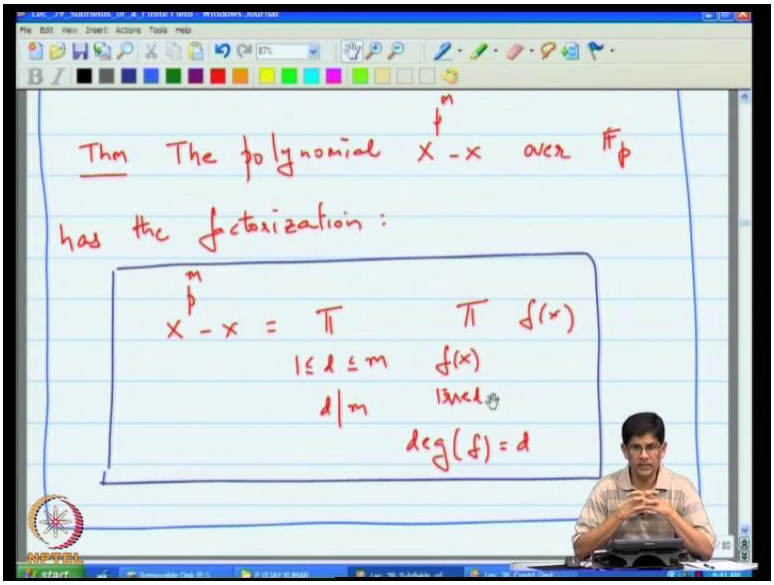
(Refer Slide Time: 31:54)



We going to keep star t with the finite field z p typically of characteristic p, you keep building to it until we reach a finite field, until we reach a finite field that contains all the zeros of this particular polynomial. Then it turns out that this collection of p to the m of this polynomial form, the desired polynomial field. And there is the little bit more to it than that, how exactly do you build the finite field of increasing size? But that cover in appendix will actually skip that for us

surprise to know that finite fields can only exists, and there of size p to the n, and if the size of if you give me a size p to the n, then I know that this is the finite field. So that is what this theorem says. So we are not very far from completing the discussion on finite fields.

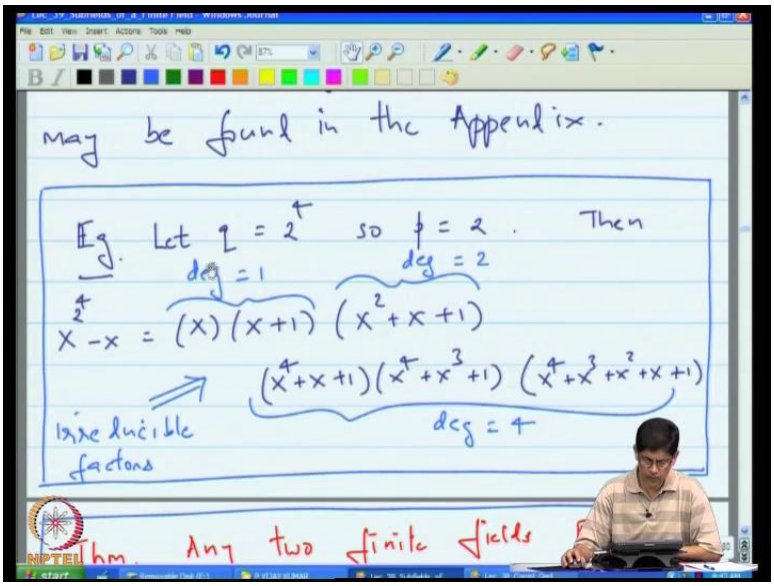
(Refer Slide Time: 33:01)



We need to wrap up the discussion on minimal polynomial and one of the topic so this theorem and gets start on that. So, it says that so we are now back to discussing about polynomials. So, the polynomial x to the p to the m minus x is over x p has the following factor that is it is the product of irreducible polynomial. So, each of this f of x here is an irreducible polynomial; so this is just saying that x to the p to the m minus x must be the product of bunch of polynomial of the irreducible polynomial.

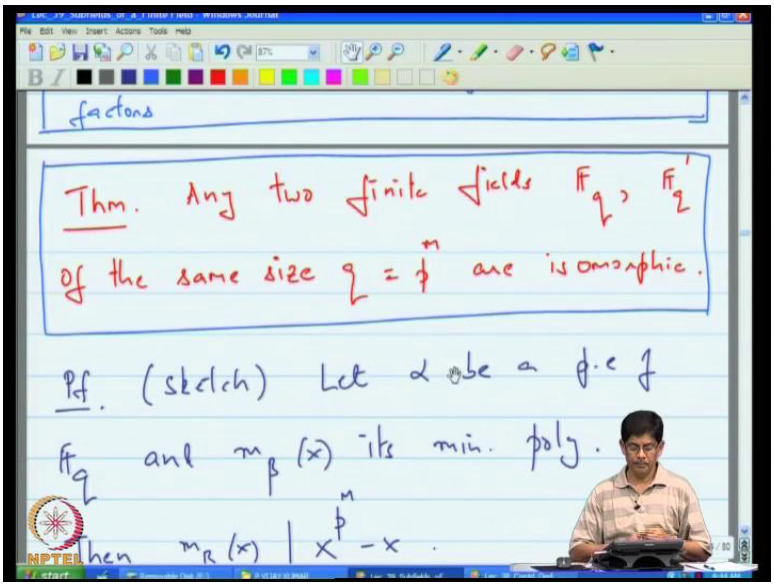
But the interesting thing is that there is lot of numerology in this, because it turns out that every irreducible polynomial whose degree is d, for any divisor d of m, the p is here. So, for example m could be 12 and you would have all the irreducible polynomials of degree 6 degree 4 degree 3 degree 2 degree 1; all of them, actually appearing in here so that interesting.

(Refer Slide Time: 34:28)



And what will do is we actually illustrate by example and the proof once again is send back to the appendix. So in the example, we have that q is 2 to the 4, so the p is prime p is 2, and then its turns out that when you fact the x to the 2 to the 4 minus x, it factors as follows. And we already know from what the theorem says that its factors into the product of reducible polynomial of degree d divide p to the m. But it turns out that there are no other polynomials irreducible polynomials of degree d dividing m; we will show that a little later. So right for now, we have factor like this, so it turns out that these are the 3 irreducible polynomial of degree 4, these are linear degree 1 and this is degree equal to 2.

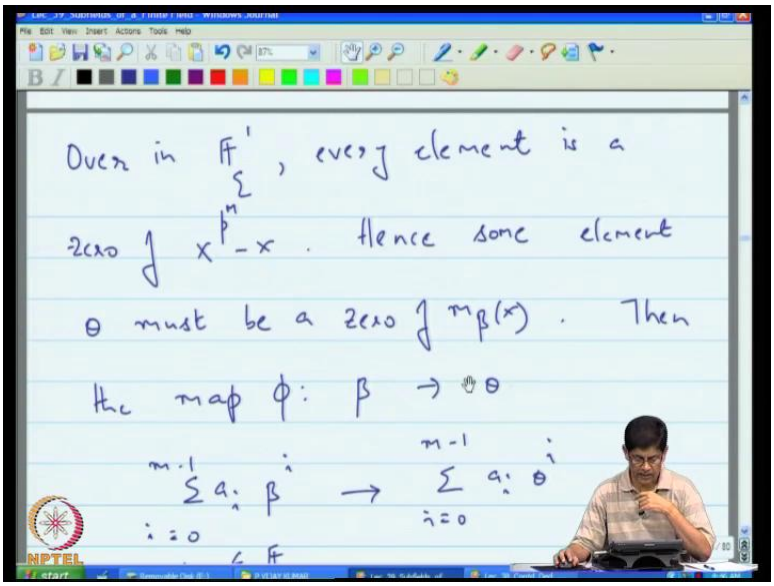
(Refer Slide Time: 35:43)



The next theorem states that I mentioned before any 2 finite field F q and F q prime are isomorphic provided they are of isomorphic. So what is isomorphic really just means that they are same except that what I call alpha, you might call beta or beta cube or whatever. So, really the same there is more formal definition of isomorphism, but in this finite case also mapping from one finite field to the other. This mapping they I have just talk about respect any algebraic relationship that preexists among the element from the field.

Here is the sketch of the proof. Let see alpha is the primitive element of f p m beta of x its minimal polynomial. Then we know that m beta of x divides x to the p to the m minus x, because all the elements of the finite fields of size p to the m or 0 of this polynomial. And that also implies beta so therefore it must be minimal polynomial divides this so there are two finite fields here F q and F q prime. What we actually did here is? Started with F q and we pick primitive element identify its polynomial element noted that it divides x to the p to the m minus x.

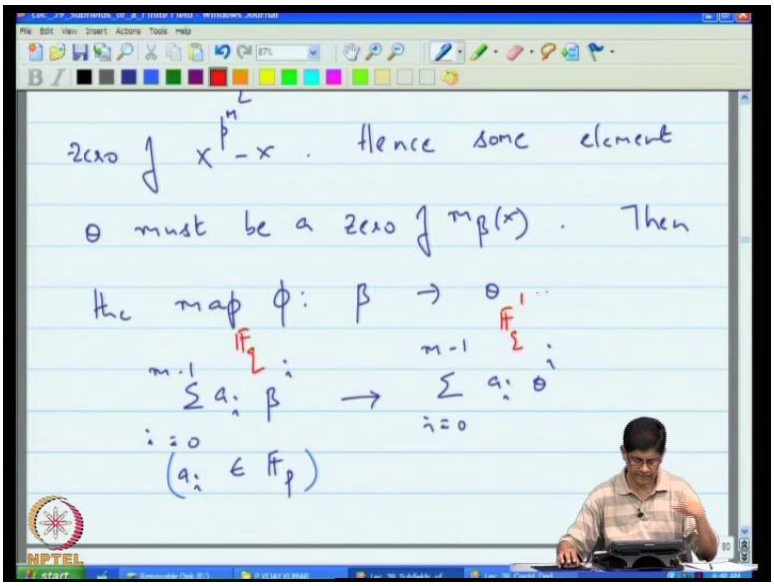
(Refer Slide Time: 37:30)



Now we moved to the other finite field, which is F q dash. In this field every element is a 0 of x to the p to the m minus x. That is was too even in the case of other field of course, and also it is true here. Therefore, some element theta must be a 0 of this polynomial m beta of x. Then the map which seems beta to theta, towards beta, beta is… This is not about that that of course, beta. Now you want to actually show that the two fields are isomorphic, but we know that in both fields, it is true that the elements can be expressed in terms of in terms of linear combination of powers of beta, where beta is the primitive element of finite field. So, every element must have the expression in terms of polynomial like this.

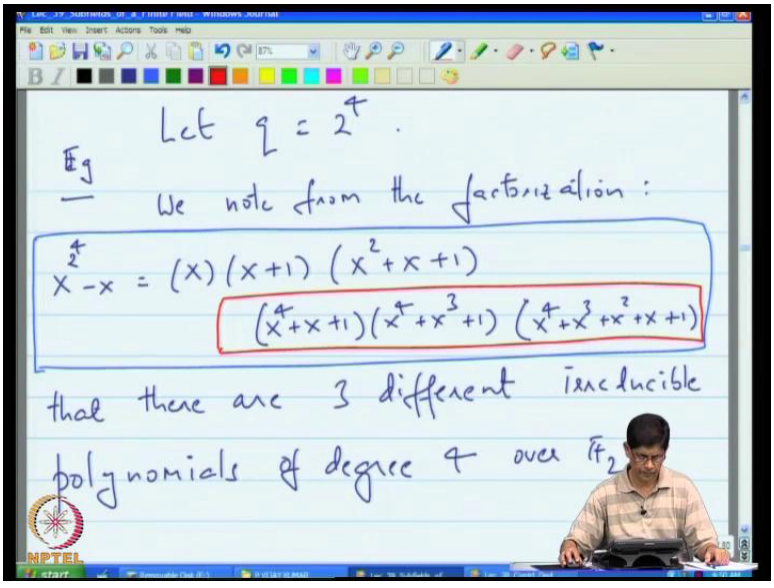
And now we consider the map between this element and the corresponding element here. The only difference being is we replace beta by theta. Remember the tie between the beta and theta is that they both share the same common minimal polynomial; of course, it goes without saying that the a i's belong to f p, so it can be shown that this is the isomorphism.

(Refer Slide Time: 39:41)



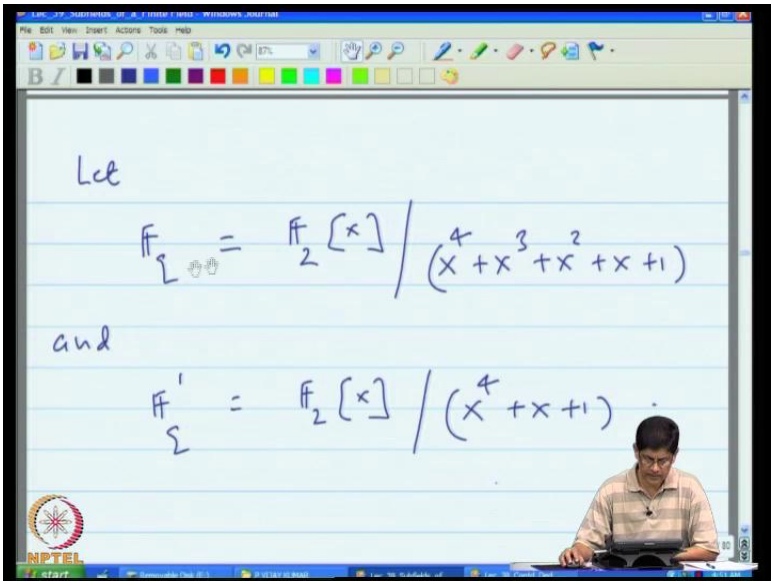
So, just to emphasize let me write here that what we have on the left is the finite field of F q, what we have on the right is the finite field F q dash. So, we will start with the map that goes from one finite field to the other, and the way it is works that takes every polynomial beta here in beta, and maps it to corresponding polynomial in theta.

(Refer Slide Time: 40:41)



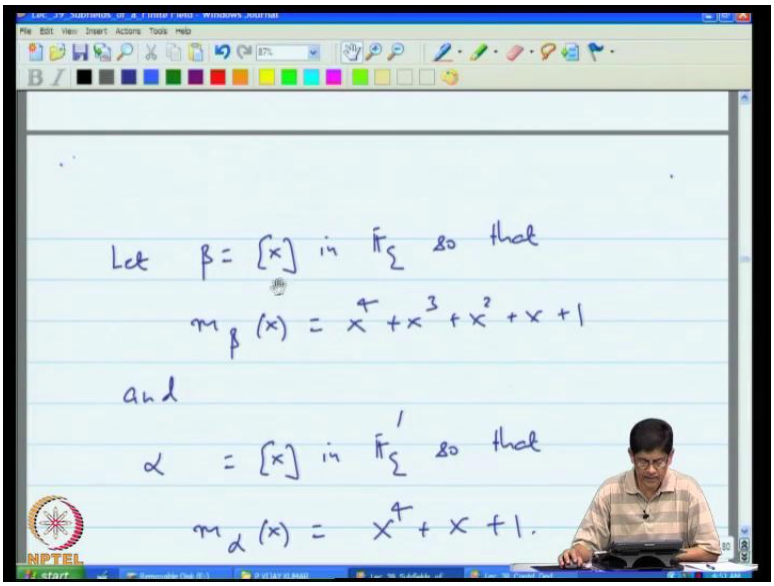
So, this always be general always be shown to be an isomorphism, what we do here is we illustrate with an example. Let q be 2 to the 4, and then we note from this factorization, I have shown you this factorization earlier that there are 3, at least 3 different work, we showed short while ago that 2 to the 4 minus x is really the product of all the irreducible polynomials, whose degree divides 4. So, that means all the irreducible polynomials of degree 1 2 and 4, because 1 2 and 4 are only divisor of 4 all appear here, there are no other irreducible polynomial. So, by factoring the single polynomial you can with finite field, because all irreducible polynomials, whose degree divides your original, whose degree divides this particular polynomials the exponent here that is 4. Thus in particular, there are three different irreducible polynomial of degree 4 and those are these 3.

(Refer Slide Time: 42:06)



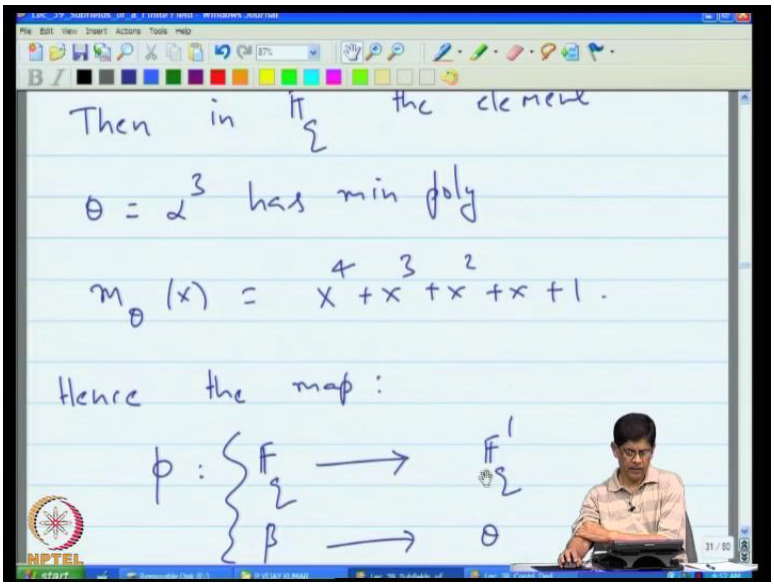
Now, we want to show this the 2 fields are isomorphic, and it will help us actually regard these fields in the following way. There is F q is F 2 of x modulo polynomial; and F q prime for example could be F 2 to the x modulo x 4 plus x plus 1, anyway there are these 2 finite fields let see.

(Refer Slide Time: 42:46)



Let beta be the equivalence class F q; let beta m minimal polynomial of beta is x 4 plus x cube plus x square plus x plus 1, because the reason being that we already that this is irreducible polynomial. So, if any element in the finite field is 0 of this polynomial, then that element must necessarily be, then this polynomial must be its minimal polynomial. so that is what I have written here. Similarly in here, let alpha represents the equivalence class of x in this field, then the minimal polynomial if alpha x to the 4 plus x plus 1. So you can see the apparently these 2 fields are different, but it not really so, because in F q we already identified the element whose minimal polynomial is like this. So let us first try to in second finite field, let us try to find in element whose minimal polynomial like this.

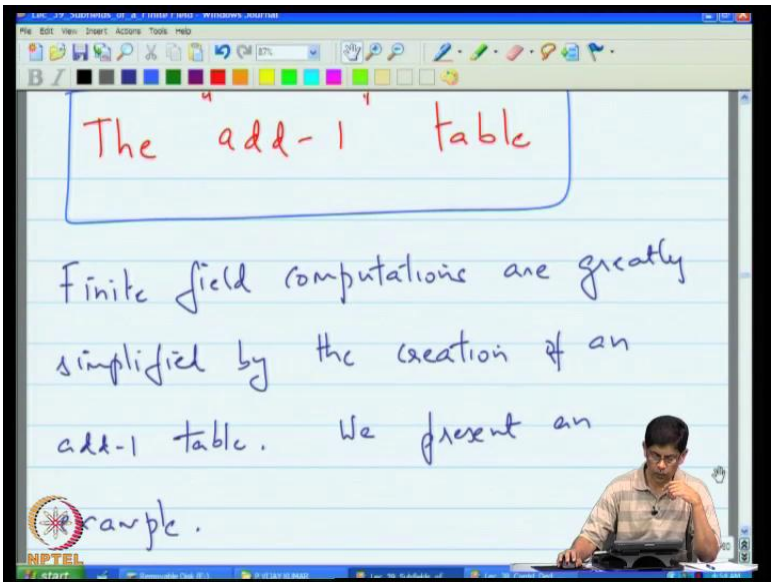
(Refer Slide Time: 43:55)



So for that, what we do is we have to identify an element in this second field, which has this particular minimal polynomial. And it turns out that they are waste to do it; for example, you can show that if theta is alpha cubed, then this element theta has minimal polynomial which is exactly this minimal polynomial of beta, in first field, so you will have that. Now how do you, now what do you next? Well, what you do is you have just say we will look this, what you call beta may be what you call beta? What I call theta is the same.

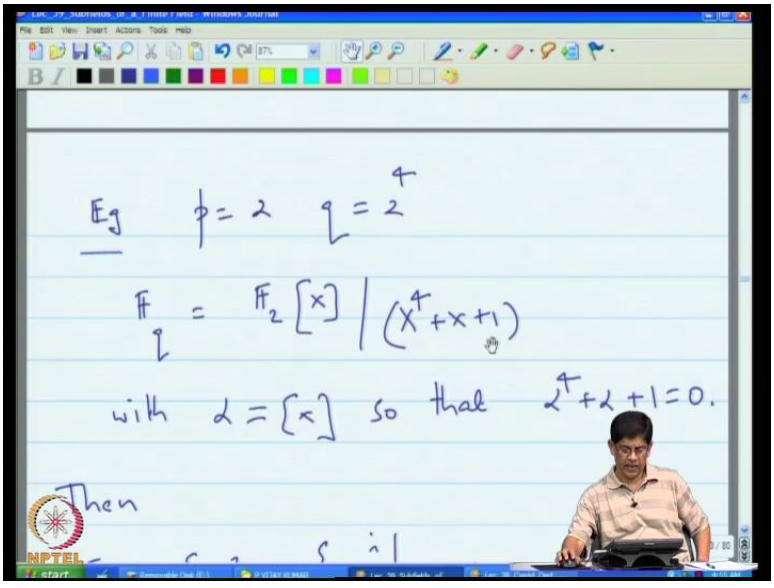
Already we know that they minimal polynomial because the map F q to F q 1 and which we send beta to theta; and it turns out that is the isomorphism. So the elements are really one to one corresponding, and so what that means above that above that it respects field operations. So, really the two fields are the same except as we have just noticed alpha 1 alpha beta in one field is the theta in the other field; apart from that really the no difference.

(Refer Slide Time: 45:28)



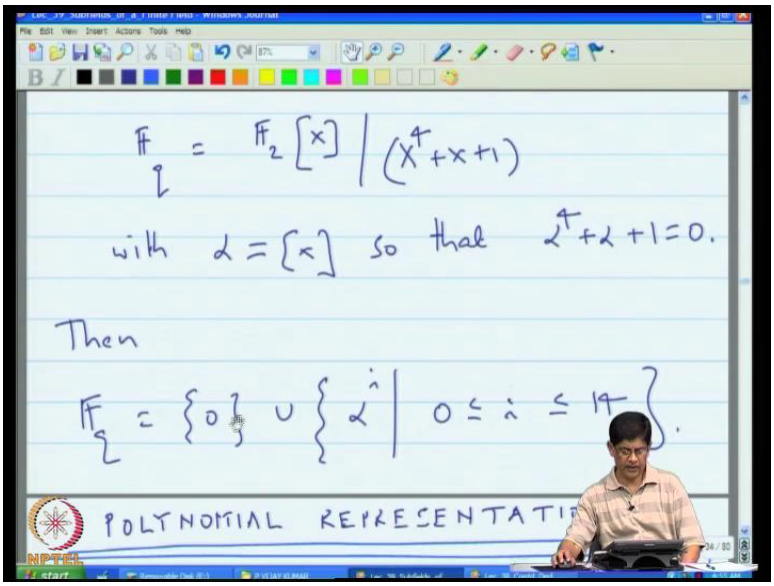
Now a more computational topic and I am going to introduce something that is called the add-1 table. It is also sometime called exact logarithm, but that sound too complicated name what it else; and as its turns out the origins of the terms z log are not really clear. So we will just take to the simpler terminology add 1 table.

(Refer Slide Time: 46:09)



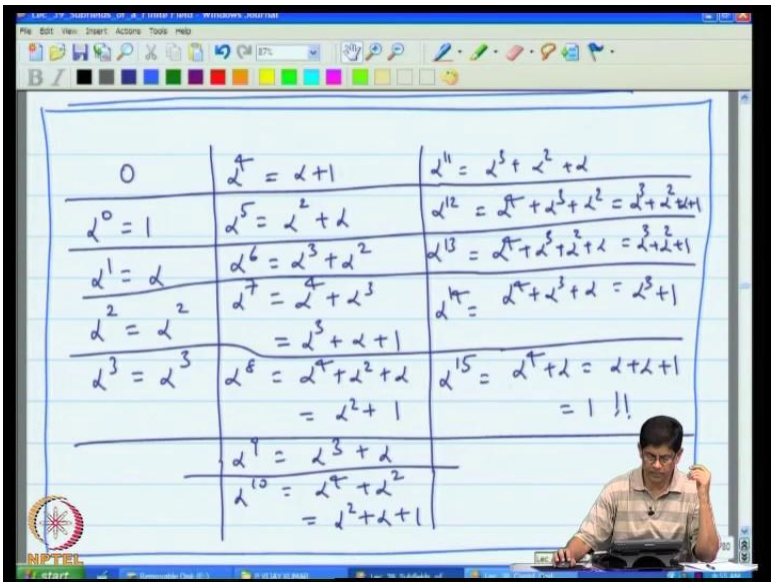
So, what this is all about is that is the following. It turns out that finite field computation are greatly simplified by the creation of the add-1 table, so we present an example here let say p is 2 q is 2 to 4 and F q is F 2 of x modulo x 4 plus x plus 1 with alpha is equal x so that alpha plus 4 alpha plus 1 is equal to 0. So, this scenario is familiar to us as we have used this several times already.

(Refer Slide Time: 46:35)



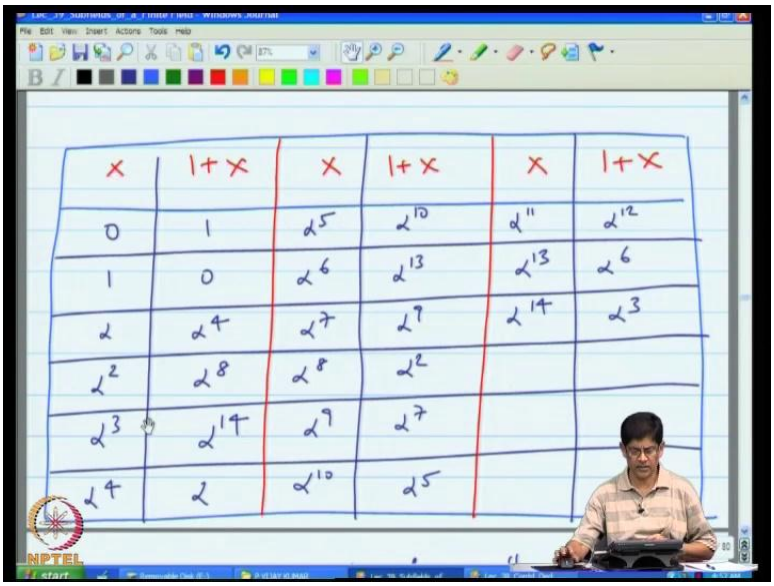
We also know that this particular finite field, that the alpha in primitive in this field. So, that means all the elements in finite field is either corresponds to 0 or else some power of alpha but lie in 0 and 14.

(Refer Slide Time: 46:53)



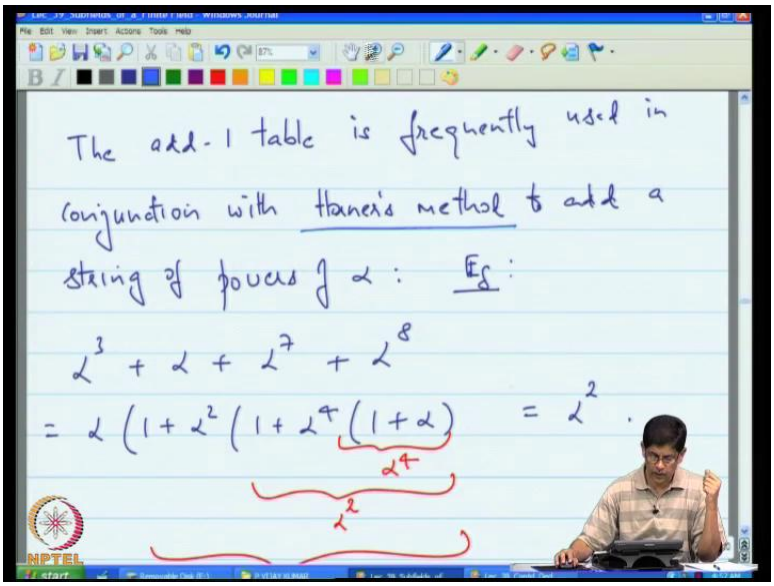
And some lecture ago, we look into the polynomial representation in the finite field in which every element in the finite field expressed as polynomial in alpha. And you can see that, because you know that every element is the power of alpha; and this time, the requirement is that this time we just representing as polynomial alpha. And with the aid of these polynomial representations, so the way in which we are going to add use this table as follows. So I am interested in things like here is the alpha to the 4, its alpha plus 1; what will I get, if I add 1 to the alpha 4? 1 plus alpha 4 is alpha plus 1 plus 1; 1 is cancel leaving you alpha; so that means 1 plus alpha to the 4 is alpha. Similarly, if you add 1 to alpha 14 and alpha 14 is itself alpha cube plus 1, so alpha cube plus 1 if you want to add 1 to it then it get you back to alpha cubed.

(Refer Slide Time: 48:14)



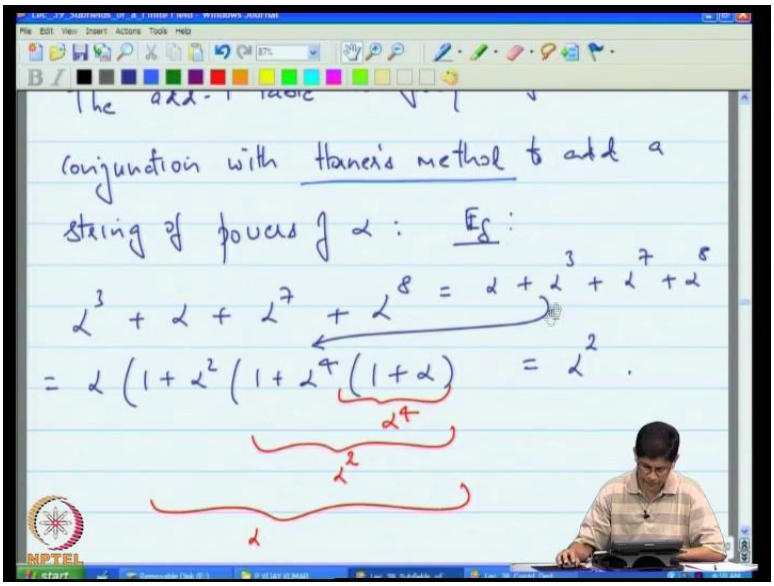
So, in this way, with the aid of that other table, you can said that this table already; this is called add-1 table of the finite field, and it tells you that for instance that if you take add alpha squared and add 1 to it. You will get alpha to the 8; of course, the converse is also true if you take alpha to the 8, and is multiplied by power of alpha. Then the reverse also true in the sense if you take alpha to the 8, and add 1 to it, you will get alpha square. So similarly, alpha 3 plus 1 is alpha 14 and alpha 14 plus 1 is alpha 3; so thus that symmetry.

(Refer Slide Time: 48:52)



And how do you actually go about using this add 1 table; well you use this conjunction with the method that is called horner's method. So, horner's method is used, when you want to add strings of power of alpha; in other words, you want to add several elements in the finite field, and you represent them in powers of alpha; of course, you ignores 0. And next what you do is you order them according to increasing powers of alpha; so in this particular place although it is not shown here, this was reordered, according to alpha plus alpha cubed plus alpha to the 7 plus alpha to the 8.

(Refer Slide Time: 49:31)



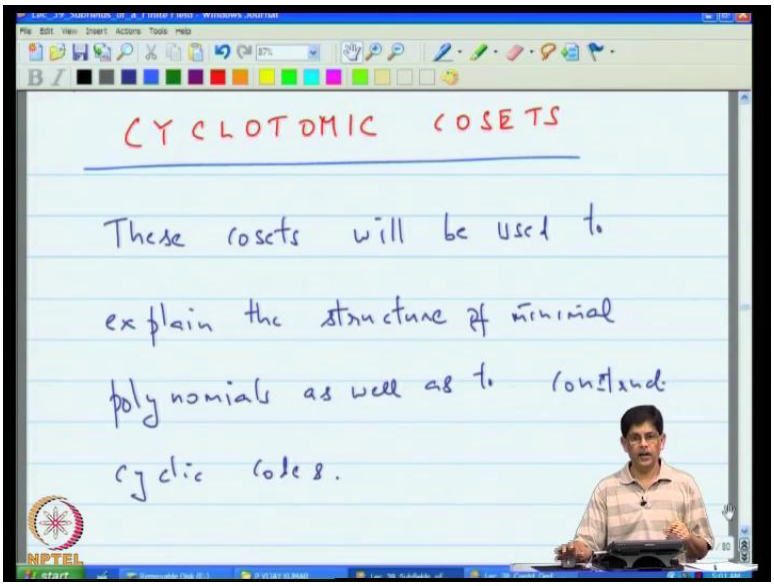
So, after this reordering, so we go there and then we come here. Now in horner's method, what you do is you take the alpha common, then you get 1 plus alpha square, so that cover this. Then you take the whole as alpha cube common get 1 plus alpha 4 and then you take alpha to the 7 to the common you get 1 plus alpha.

So it is just difference way of representing this, if you multiply this all out you will get exactly this; and I think if you not convinced you should tried it out on your own. Now once you written it out, this is setup you can recursively use the advantage. So, for example, here 1 plus alpha is alpha to the 4 alpha to the 4 times alpha to the 4 is alpha to the 8 alpha to the 8 is alpha to the 8 alpha square times alpha square is alpha to the 4 1 plus alpha to the 4 is alpha and alpha times alpha is alpha square. So that is your final answer here. So, in the way what you are really saying it look if I want to think about finite field I can either think of elements as the polynomials in primitive element in alpha or the other way in which really, I can think about finite field is the powers of primitive element alpha.

And clearly the representation is powers of primitive element alpha so much easier and more convenient. Only problem is how do you add, because in the polynomial notation is easy to add in the power of alpha notation it is easy to multiply is alpha cube times alpha 4 is alpha to the 7 and that is obvious. So, you get in some sense the best of both world, because you get to work

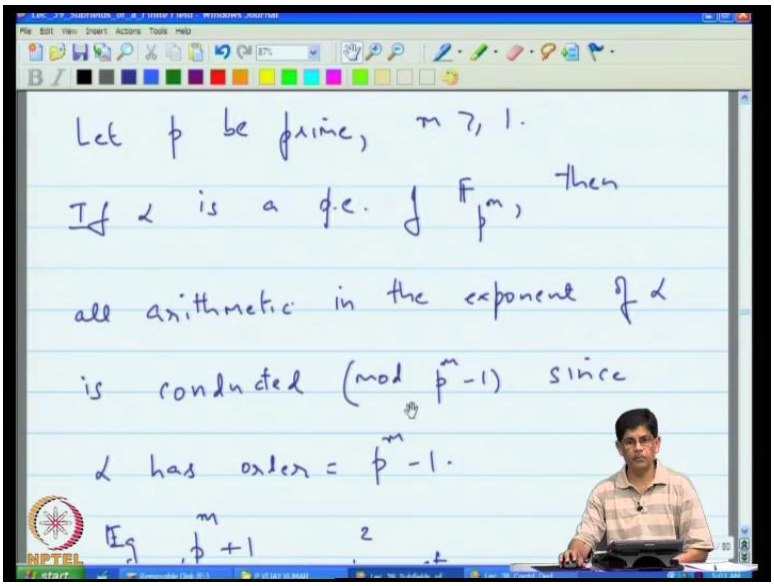
with the powers of alpha; and all that you need to do, it only there is only one cost involved is that you need to keep this add-1 table in your mind, either memorize it or have it on a sheet in front of table as in competitions. And then the finite field representation is, and then the finite field competitions become rather straight forward. We are edging towards the closure for lecture here and our next topic.

(Refer Slide Time: 52:16)



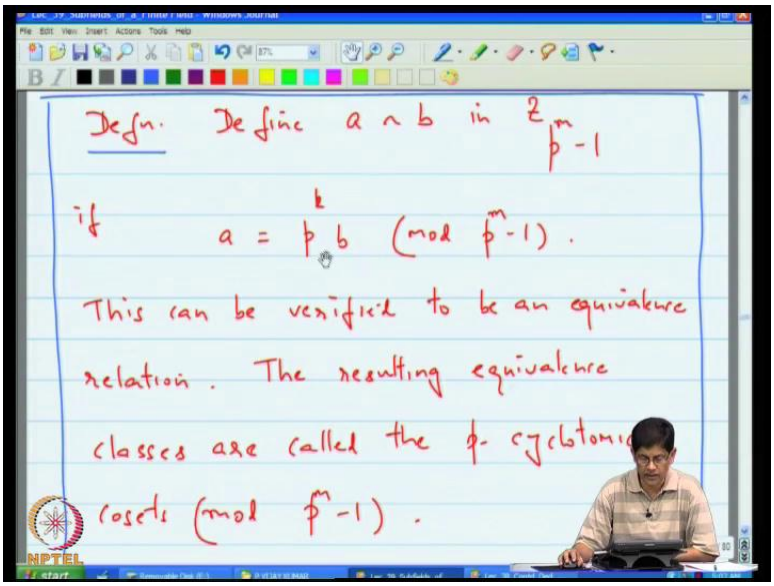
So, again there is a little bit of jam is called cyclotomic cosets, what is that means the moment you heard the word cosets? You start thinking well may be this is talking about groups and sub groups and your answers yes or no here. But where we interested in this cosets, because these cosets will be use to explain the structure of the minimal polynomial. And it is also your turns out interestingly will be helpful in constructing cyclic codes that is error correcting codes for particular type known as cyclic codes that these cyclotomic codes so the definition goes us follows.

(Refer Slide Time: 52:52)



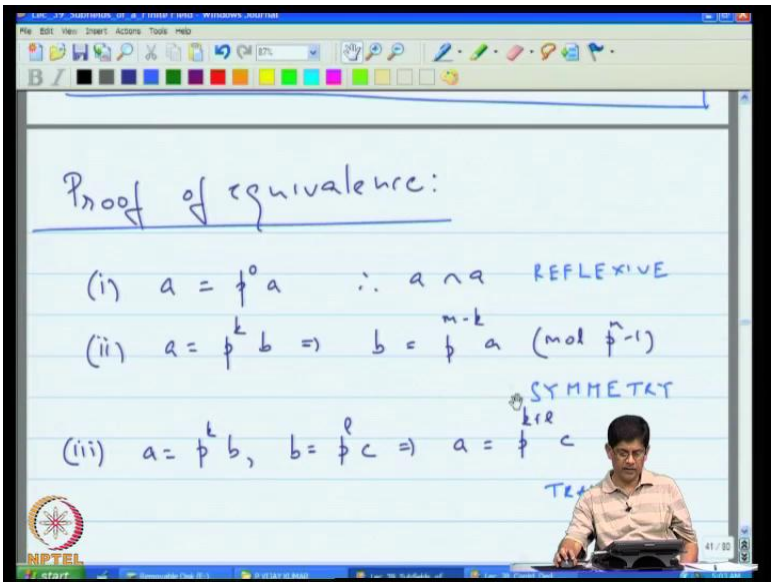
So, let p be prime and greater than equal to 1 always, and then alpha is a primitive element of f p to the m. Then all arithmetic in the exponent of alpha is conducted mod p to the m minus 1, because supposing alpha has order 15 and you want to talk alpha raise to the power k times l, then that k times l multiplication you can regard that this modulo p to the m minus 1, because simply because alpha to the p to the m minus 1 is 1. So, for example, if I look at alpha to the p to the m plus 2, then I know that just alpha square I can see that by doing arithmetic modulo p to the m minus 1 in the x y.

(Refer Slide Time: 53:48)



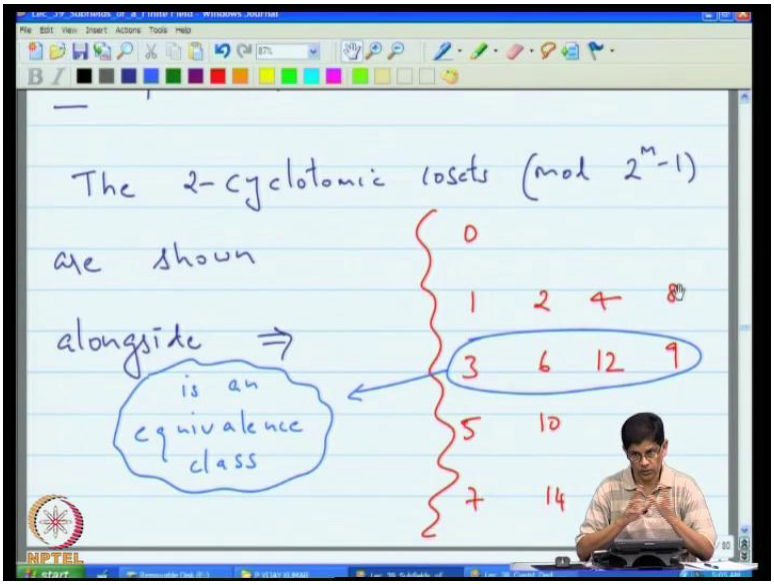
So, with that is motivation what we do is, we now focus on the set of integers modulo p to the m minus 1. And here we define two elements a and b to be equivalent, if a is some power of p times b. And of course, this is in this arithmetic is here in this algebraic structure, so it is modulo p to the m minus 1. Now you can verify this to be an equivalence relationship, and the resulting equivalence classes are called the p cyclotomic cosets mod p to the m minus 1. So, the reason why it called p cyclotomic cosets, because p appears here, and modulo p to the m minus 1 is of course, I already explained. Now I have called this in equivalence relation, why is that the case?

(Refer Slide Time: 54:51)



That is because you can actually verify that the reflexive the symmetry and the transitive properties actually hold. And I would not actually although I have written (( )) on this slide, I am not bother to going through them, because they are elementary. So it is clear that the reflexive symmetry and transitive property is hold. So this property that we define here is in equivalence relationship.

(Refer Slide Time: 55:20)



Let us illustrate with an example; when p is 2 and q is 2 to the 4, then the 2 cyclotomic cosets mod 2 to the m minus 1 are showed here. So the cyclotomic cosets themselves are the resulting equivalence classes. And you notice that the equivalence classes are of different sizes. So each row here, therefore, in this diagram each row here corresponds to them so for example, this thing here is the equivalence class containing 3. So, similarly there is another equivalence class which only contains 0; and it turns out these are really not cosets, because if you were taking a groups and sub groups, and then looking out the cosets of the sub groups you know that all cosets are same size. So these are not really cosets, although there is a link its sub group, but again for lack of time, I will not pursue that. So just accept that terminology cyclotomic cosets.

Now I think, I think this is the good place to stop this covered lot of ground, and but I think I given that the notes are written out and you have them accessible. You might go through on them once on your own, just make sure you understand everything. We almost complete discussion on finite field; and in the next lecture we will start discussing cyclic codes. So with that I will close. Thank you.