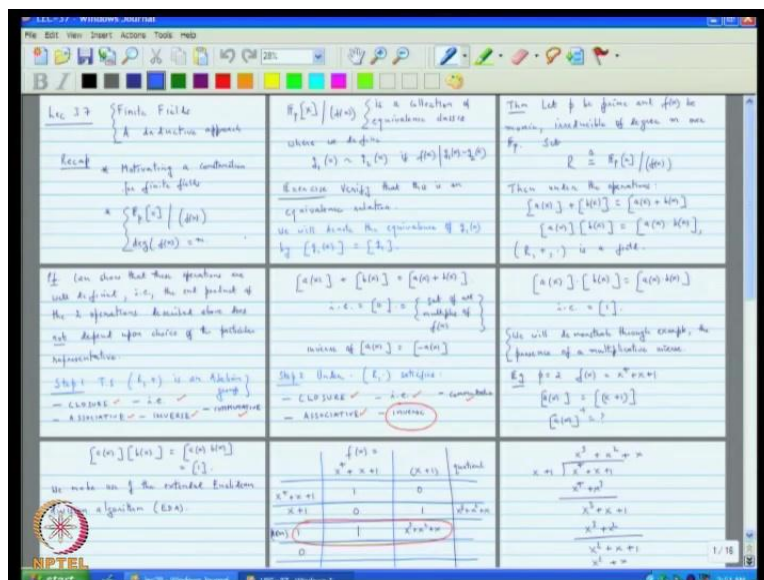


Lecture No. # 38

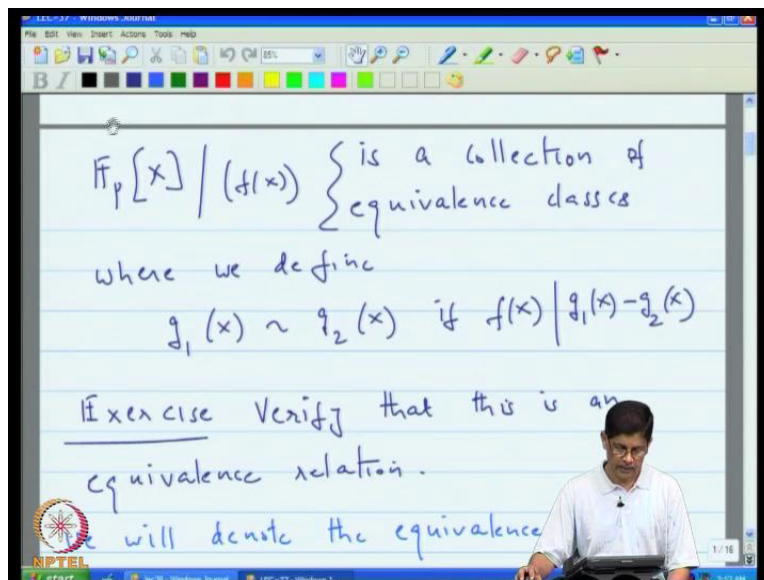
Deductive Approach to Finite Fields

(Refer Side Time: 01:07)



Last time we were talking about finite fields, and although I label the lecture finite fields deductive approach. We really did not get excuse me we really did get the chance to go into the deductive approach, we spend most of the time recapping our earlier discussion on construction of the finite field, but we completed that. And so the end of the last lecture, we were just ready to begin discussing the deductive approach, so where we left off, but actually provide you the

construction of the finite fields, and the way we deduct was same that you can always take you can the generic construction is like this. (Refer Side Time: 02:02)



$\mathbb{F}_p[x] / (f(x))$ is a collection of equivalence classes
 where we define
 $g_1(x) \sim g_2(x)$ if $f(x) \mid g_1(x) - g_2(x)$
Exercise Verify that this is an equivalence relation.
 We will denote the equivalence

You actually look at the set of all polynomials over certain finite field \mathbb{F}_p , and then you go modular and reducible polynomial and this really should be integrated as the collection of equivalence classes, where you define two to be equalling, if x divides the difference define this is a field and towards the end of the last lecture. What we did was we took an example and in the example the characteristics was two the reducible polynomial was $x^4 + x + 1$ and then we carried out an should you explicitly, the finite field. In this form where actually should you how the elements of the finite field look like.

(Refer Side Time: 02:55)

Lec 38 { Deductive Approach to Finite Fields

Recap

A completed discussion of the quotient ring $\mathbb{F}_p[x]/(f(x))$

construction of finite fields

So, today we will actually go towards deductive approach. I just written out what I just told you here. (Refer Side Time: 03:03)

Deductive Approach

Let \mathbb{F}_q denote a finite field of size q . Then:

- $(\mathbb{F}_q, +)$ is an Abelian group
- (\mathbb{F}_q, \cdot) satisfies { closure, Assoc., i.e. = inverse, comm }

Let us begin with the deductive approach; the deductive approach is very little it says look all the time you know is there have a finite field that the finite fields contain q elements. This is the set, it is a kind of like a black box, and entire to investigate what is internal structure is like? What are do know is that the element form of field that is there are two operations, which we called the

additions and multiplications. And these operations, these set together these two operations from what is called the field, and the other important thing what we know is the number of elements is q from those we want to actually deduce the internal structure of the group. What do you mean by the fact by using the structure of the field. Why we know that the F_q plus must be Abelian group, and that if you take this F_q along under multiplication. It must satisfy the axioms of closure associatively the identity element the inverse commutative.

(Refer Side Time: 04:10)

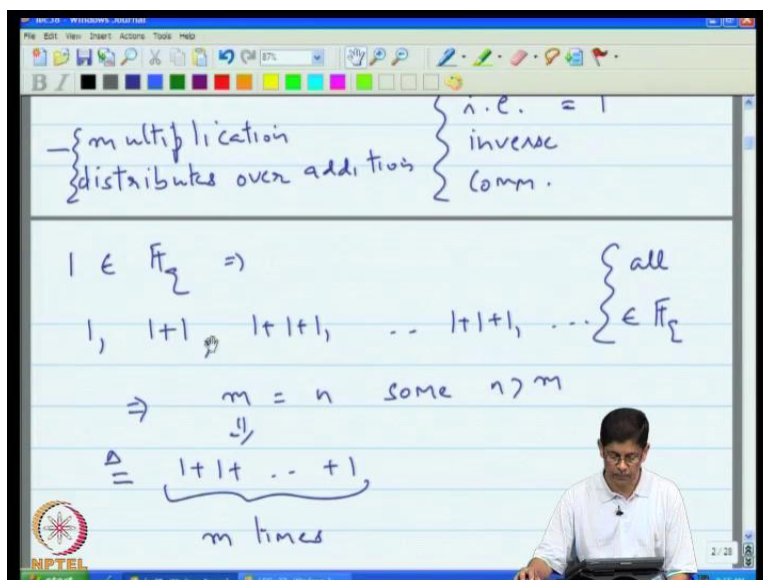
The whiteboard contains the following handwritten text:

- $(F_q, +)$ is an Abelian group
- (F_q, \cdot) satisfies
 - Closure
 - Assoc.
 - i.e. $= 1$
 - inverse
 - Comm.
- $\left\{ \begin{array}{l} \text{multiplication} \\ \text{distributes over addition} \end{array} \right\}$
- $1 \in F_q \Rightarrow$
- $1, 1+1, 1+1+1, \dots, 1+1+1$

The lecturer, a man with glasses, is visible in the bottom right corner of the frame.

And there is also a matter of distributor, and in addition we have that multiplication distributes over addition. So, we want to make use of this interact to reduce the structure. We will actually start this by looking at the identity element and multiplication.

(Refer Side Time: 04:48)



Let us called at one, now the finite field since it require satisfying all this axioms must contain a one, which is a multiplicative identity. But it contains one must it contains one plus one, one plus one plus one and so on. There contain 1, 2, 3, and so on, but since this field is finite this list cannot continue in definitely at some point there must be a repetition. Because after all infinite number of elements cannot be contain in a finite field. Let us say that m is equal to n and without loss of variety. We can resume that n is greater than m . Now just keep in mind that when I write n , but what I really mean is one plus one plus one in n times. Now, this now let me just say that from this it is follows.

So, from this it follows that n minus m is equal to 0, in the way you should interpret that, because when you write n you really mean one added to itself n times. You mean that one added to itself n minus m times the collection of n minus m ones when added together most give you 0. This motivates the definition for something that is called the characteristic of a finite field.

(Refer Side Time: 06:29)

Defn. The characteristic p of a finite field \mathbb{F}_q is the smallest integer p s.t.

$$p = \underbrace{1+1+\dots+1}_{p \text{ times}} = 0 \text{ in } \mathbb{F}_q$$

Thm 1 The char. p is a prime.

The image shows a man in a white shirt sitting at a desk, looking at a laptop. The background is a digital whiteboard with the handwritten text and equations.

The characteristic of a finite field is smallest integer p , such that when you take p copies of the identity element and multiplication, you will actually get 0. Why did you see there must be some integers as that is equal to 0, now I assign let p be the smallest set integer, such that p copies of one, when added together will end of being 0, this is called the characteristics.

(Refer Side Time: 06:56)

$p = \underbrace{1+1+\dots+1}_{p \text{ times}} = 0 \text{ in } \mathbb{F}_q$

Thm 1 The char. p is a prime.

If. Suppose $p = a \cdot b$, $1 < a, b < p$

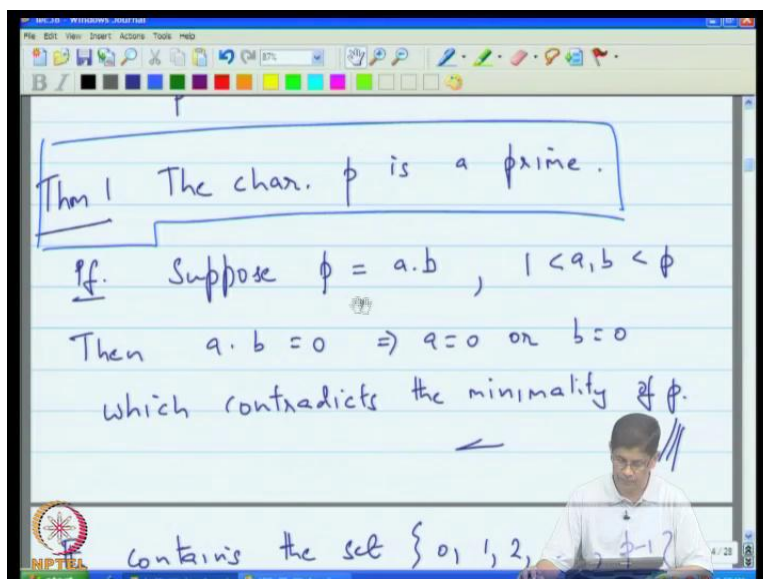
Then $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

which contradicts the minimality of p .

The image shows the same man from the previous image, now looking at a different part of the digital whiteboard. The background is the same digital whiteboard with the handwritten text and equations.

The first theorem that we want to actually prove is that the characteristic of a finite field is a prime, in other words the smallest number of integers copies of one in order together to give 0 must be a prime.

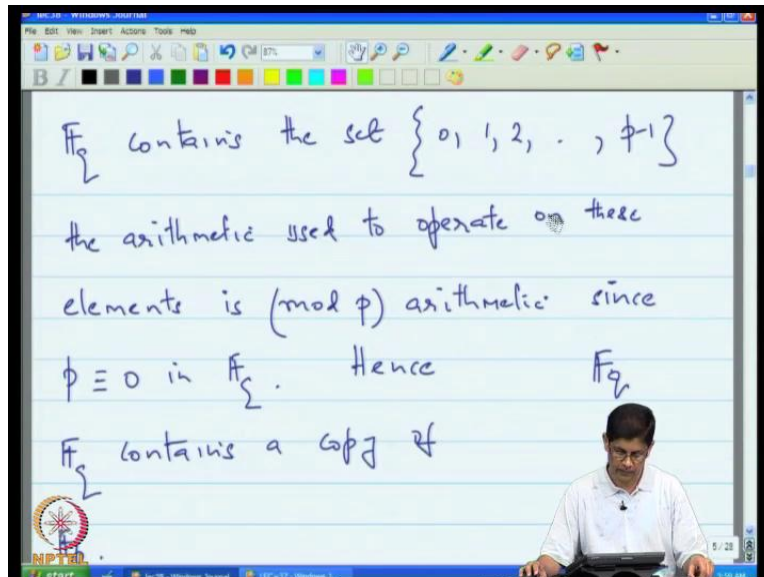
(Refer Side Time: 07:18)



How do you prove that well it is a straight forward, supposing in this characteristic was actually a times b ; that means you took a times b copies of one, and added them together and you obtain 0. That is equalling to same, but a times b is 0, that if a, b is 0 then it must be that either a is 0 or b is equal to 0. But then remember that since you factor p into the form a and b into the product of a and b . It must be the both a and b lie between one and p , but then if a is 0 then that contradicts the minimality of p , because we said p is the smallest integers such that if you take p identity element copies of the multiplicative identity, then we actually get 0. But here you getting that a is 0 or b is 0. So, that contradicts the minimality. So that, only we could happen is in fact such a factorisation is not possible which tells you the p is a prime number. So, p could be 2, 3, 5, 7, 11 and so on, but it cannot not be 6, 9 or 12.

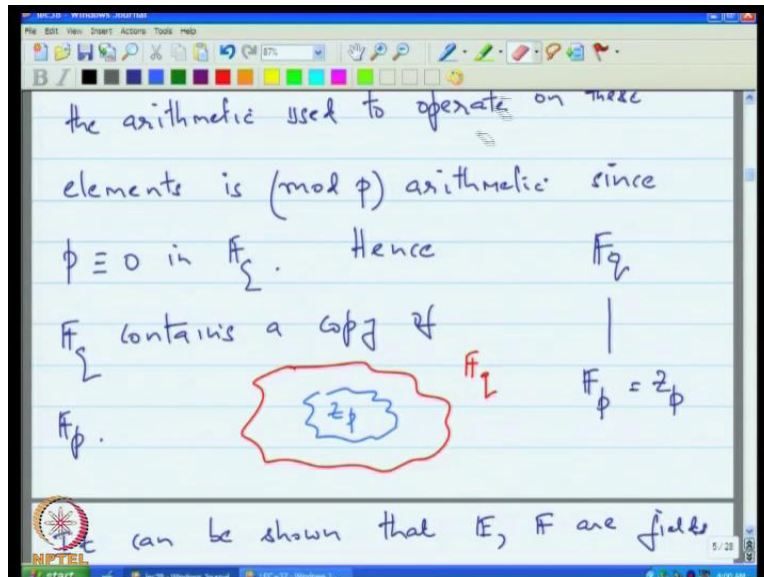
Now so that was the first observation, so what to summarise and what we will actually seen is that there is unique prime that is associated to a finite field of q element, and that prime is called it is characteristics.

(Refer Side Time: 08:45)



Now we are going to explore that little bit further, so well we say \mathbb{F}_q therefore contain 0, 1, 2 all there up to p minus 1. And we know that p is 0, which means that if you just, so here is the \mathbb{F}_q and here is the these elements, which is actually a subset of \mathbb{Z} ? Now the arithmetic that we used to operate on this element is not the arithmetic, because for example if you had 1 to p minus 1 you will get 0, because we know that p is 0 in the finite field. What means that the new work with these elements, and you under the two operations addition and multiplication, what you will be doing is virtually (\mathbb{Z}) the operation that you would carry out in a field of p elements, there is \mathbb{Z}_p . So, \mathbb{Z}_p is something that you are familiar with, so these are subset of finite field really behaves like \mathbb{Z}_p .

(Refer Side Time: 09:51)



That means the picture that now that is that inside your finite field F_p , you have this sub set which is \mathbb{Z}_p . Only thing is that instead of calling of \mathbb{Z}_p we will narrate F_p , because preferred notation. Now is to use f to denote the finite field, and let the subscript denote the size. So, that means that sitting inside larger finite field, we have a smaller finite field. Let me just make that just write here and write the F instead of \mathbb{Z} .

(Refer Side Time: 10:32)

F_p .

It can be shown that E, F are fields and $E \supseteq F$, then E is a vector space over F .

It follows that F_Σ is a vector space over F_p . Let n be the dimension of this vector space. Then

and $E \supseteq F$, then E is a vector space over F .

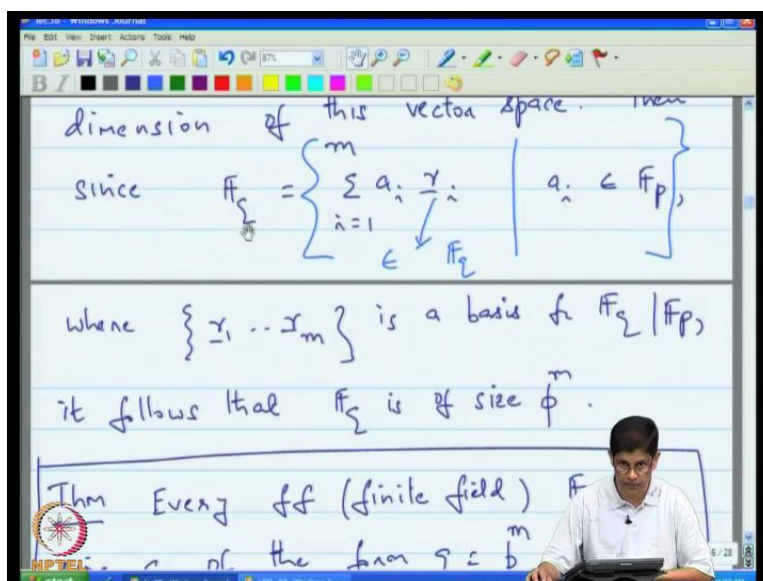
It follows that F_Σ is a vector space over F_p . Let n be the dimension of this vector space. Then since $F_\Sigma = \sum_{i=1}^n a_i \gamma_i$, $a_i \in F_p$,

So, now we have larger field containing smaller field. Now in general, it can be shown that whenever you have a situation in which, you have two fields E and F in with E containing F . Then it can be shown that capitalise E is a vector space over F , this is true in general, so it is not for this particular situation.

So, whenever you have the situation let you have the finite field, E containing the second finite field F , it can be shown and it is not difficult to show you just go through the axioms that going

to defining vector space. So, this is the larger field will be a vector space over the smaller field, which means you can think of the elements in the bigger field as if there are vectors of the smaller field. Now, in particular that means that in our situation here, that means that the finite field of q elements is a vector space over the finite field of p elements, but there is a nutrition property that we can call upon here with respect to the vector spaces.

(Refer Side Time: 11:52)

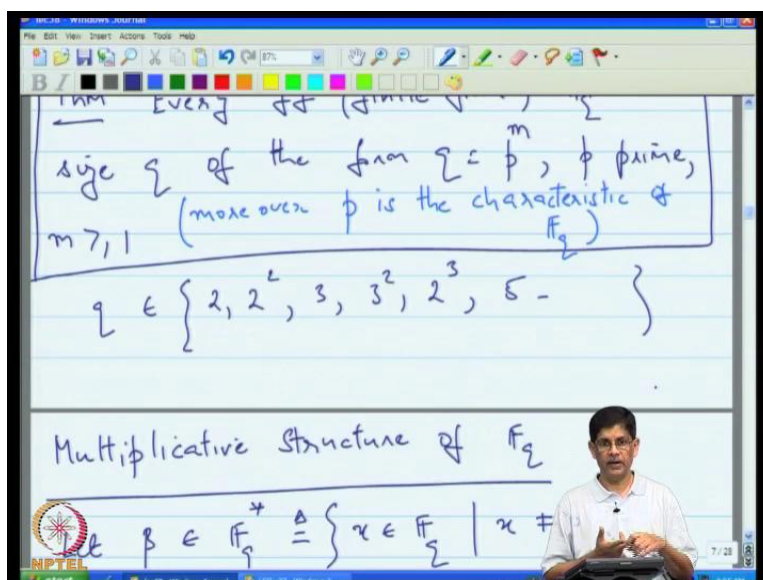


Namely, that since that you can describe all the elements in the finite field like this; that is you can say that you can take a basics for the vector space over the field, so you can take a vector space for this vector space over this field, let the basics gamma 1 to gamma m.

So, I am actually getting n denote the dimension of the vector space, that is why the basics is n elements, but that the properties of the basics tells is that every element in the vector space is unique expression as a linear combination of the basic elements. That means the element in the F_q can be written in the form $\sum_{i=1}^n a_i \gamma_i$, i is equal to 1 to n and put an underline here, just to emphasis the fact that we are thinking of these elements γ_i . So, these really belong to F_q . these elements are elements of F_q except that just emphasis the vector nature of these elements.

I am actually putting a bar under near this. Now, but then the moment you like this and you realize that look there are p choices each of this co-efficient, and I can actually count I can say look this finite field on left has q elements. On the other hand you look of the size of this set and I know that the every search linear combinations is distinct, how many possible linear combinations are there? Well p choices for a_1 , p choices for a_2 , and p choice for a_m . The total number of them is p to the m , it follows that the size of this finite field is p to the m , but the size of the finite field is q , so it must be that q is p to the m . So, it is summarise, but that tells is that every finite field F_q must have size, which is the form q is equals p to the m some prime p m greater than or equal to 1.

(Refer Side Time: 14:07)

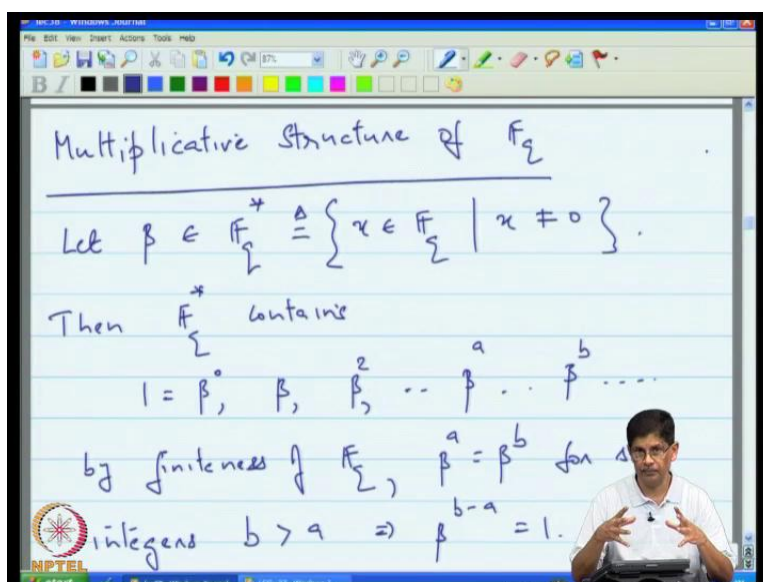


Moreover we can actually say what this primes, moreover p is the characteristic of F_q . So, in summary every finite field F_q must be a size, must be a half size p to the m , where p is a characteristics.

So, it means that you cannot have finite fields for example of size 12, because the 12 is not the power of a prime. So, what are the possibilities one of the possibilities, the possibilities include. So, q for example could belong to 2 it could belong to 2 square, it could be 3 it could be 3 square, it could be 2 cube and so on. It could be 5, so always it could be a pair of prime. Now after now it deduce the two things first of all that there is a unique prime, that is associated with

every finite field. And that prime is the characteristics of the finite field, and in terms of the finite field, it means that if you take p copies of the multiplicative identity and add them together you will get 0. So, that is have you pull of p from the structure of the finite field F_q , then the second property is that the finite field F_q is a vector space over the set 0 to p minus 1, that is said actually forms the smaller field F_p and since F_q is the vector space over F_p it must be that q must be the pair of prime p .

(Refer Side Time: 16:05)



Now, what we want to do is we want (()) into them multiplicative structure of F_q , what is that mean? We want to focus on multiplication, we are going to talk some much about addition and we want to see what we can actually say and the beauty about of this that we are going to build up to very simple picture, and you know that is the best of all things. You work very hard, but at the end very simple picture of the finite field. And that is the kind of thing would you like to have happen, you know want to work very hard and come up to the very complicated picture. We will go to work and extracted very simple picture of the finite field. So here, let beta belong to F_q^* .

Now this star notation here, simply means that we are going to look at F_q , but we are going to exclude the element 0. In other words F_q^* is the notation for all the non-zero elements in F_q , then F_q^* contains it must contain one which you can regard as beta to the 0. That is beta to

the 0 here it contains beta, beta square, beta cube, beta to the a, beta to the b and so on, but this is an infinite sequence. But the finite field after all is finite. Therefore it is some point you must have repetition, that is for some pair of integers a and b with b greater than a, beta to the a must equal to the beta to the b, beta to the a is equal beta to the b, but that is equal to saying that beta to the b minus a is equal to the 1. Now, what that is telling us is that if you take a non-zero element in F_q . You can for every search elements there exists some integers such that, if you raise beta to the power you will get 1.

(Refer Side Time: 17:58)

This motivates :

Defn. The (multiplicative) order of $\beta \in F_q$ is the smallest exponent e s.t. $\beta^e = 1$

Lemma 1 Let $\beta \in F_q$ have order e . Then $\beta^a = 1$ iff $e \mid a$.

Now, let to the following definition, the multiplicative order of beta is the smallest exponent e , such that beta to the e is 1, because we already know that there is some integers says that beta to that integer is 1. So, now we asking what are the smallest integer with that property? And that is called the order of beta in F_q . Now lemma 1, let beta let F_q star have order e let assume that the order is an integer e and supposing someone tells you. By the way I just discover beta to the 1 is equal to 1 and this lemma is telling you well the only way that can happen. If when a is the order and beta to the 1 is equal to 1, the only way this can happen a is if e divides 1 and if e divides 1 this is going to happen. How do we prove that?

(Refer Side Time: 19:13)

Then $\beta^e = 1$ iff $e \mid l$.

pf Let $l = ue + v$, $0 \leq v \leq e-1$
 \uparrow \uparrow
quotient remainder

Then, $\beta^l = \beta^{ue} \cdot \beta^v = (\beta^e)^u$

Then, $\beta^l = \beta^{ue} \cdot \beta^v = (\beta^e)^u \cdot \beta^v$
 $= (1)^u \cdot \beta^v = \beta^v$

but this contradicts the minimality of e unless $v = 0$. Hence $e \mid l$

We do is we take l we know that the beta is order e , so the smallest integer to which the beta is 1 so the l must therefore be greater than or equal to e . So it makes sense to actually divide l by e and let us say that v is the remainder and we know that from Euclidean division or from, which is the everyday integer division algorithm. We know that you can actually divide to get the quotient and the remainder and that the remainder is strictly less than e , can only be the larger e minus 1. So, now from this we can say that therefore beta to the l is beta to the $ue + v$ which is beta to the ue times beta to the v , but this can be rewritten as beta to the e to the u times

beta to the v , but beta to the e is 1 reason being that we defined e is the order of beta by definition beta to the e is 1.

So, that is one time beta to the v which is 1 why is that, because by the hypothesis of the theorem beta to the 1 is equal to 1. So, beta to the 1 is equal to 1, which implies that the beta to v is equal to 1, but wait a minute. When we wrote the expression down when we note it that the v was strictly less than e , but I can't do that. Because after all we said that the beta is the order e so the only way all these facts can be consistent simultaneously consistent if in fact v is actually 0. v is 0 then this no contradiction, because beta to the 0 is one and when you define the order you excludes 0. The multiplicative is smallest so may be is the clarified that there, let us put that in is that the smallest non-zero exponent e such that beta to the e is one.

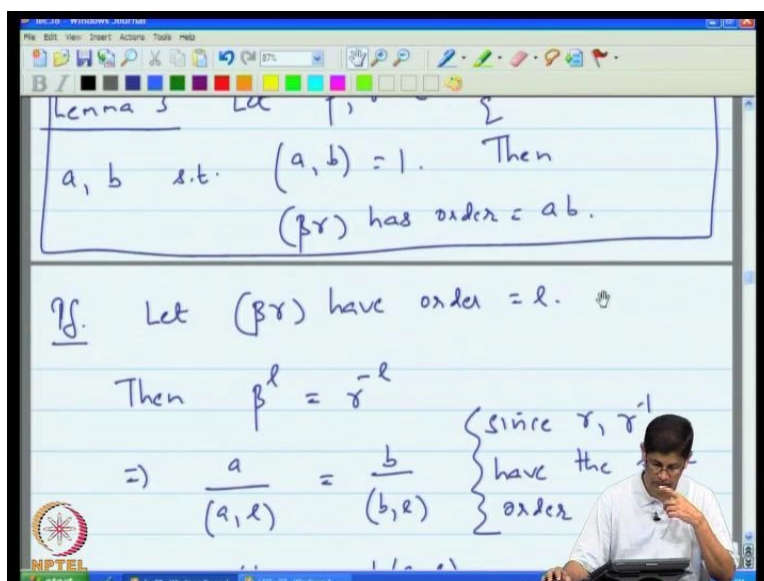
(Refer Side Time: 21:21)

Lemma 2 Let $\beta \in \mathbb{F}_\Sigma^*$ have order e .
 Then β^l has order $= \frac{e}{(l, e)}$.
 eg. $e = 15$ $l = 10$
 order $=$:
 pf. (Exercise, straightforward).
 Lemma 3 Let $\beta, \gamma \in \mathbb{F}_\Sigma^*$ have

So, that tells that e divide l again to summarise if beta is order e and beta to the l is equal to the 1. The only way that can happen is if e divides l , and (()) if e divides l this will take place. Now there are couple more numbers which are somewhat technical in nature, again I just want to you keep you motivated by telling you, that if you are patient in this phase then eventually you will come to very simple picture of the finite field. So, number two says that if beta is the order e and you raise beta to the power l , then beta to the l has an order e divided by the greatest common divisor of l and e .

Just to illustrate as I just to the site calculation here, so we will actually say that supposing let say that e is 15 and l is equal to 10, and what it is saying is that the order of beta to the 10 is 15 divided by the greatest common divisor of 15 and 10, which is the greatest common divisor of 15 and 10 is 5. So, this is will end of being 3.

(Refer Side Time: 23:03)

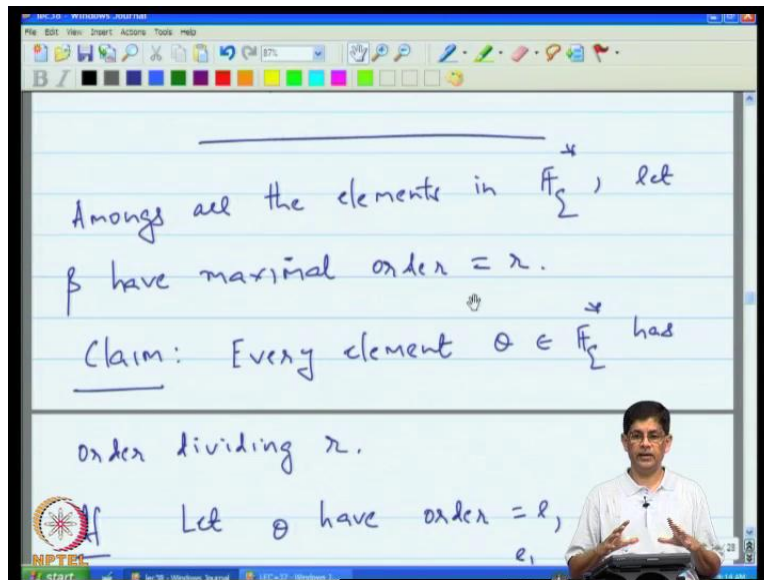


So, I this was just give you an example, I will not prove this, but I left this exercises for you, and the exercises is trade for... Then we come to an interesting element which says that look if beta and gamma are two non-zero elements in the finite fields, and let say that a is the order of beta and little b is the order of gamma. Then if a and b are relatively prime, that is what this is prime, where greatest common divisor is 1. Then beta times gamma has an order is equal to a, b the product of the orders, and how do you prove that I think that the proof is actually written down here, it is a little bit technical. So, I want actually go through it you can read it on your own, it provide it to make a notes more complete, but rather than rush you through the lot of technical details. I will try to give you the overall picture and the details are there in the writing.

Let us try to focus on understanding what the lemma says, it says take two non-zero elements and let us says that the orders are a , and b , such that the a and b are relatively prime. Then it is saying that the product of the two elements as order equal to the product of the two orders, but the key point is that there the two orders are relatively prime. How do you use that? Now where,

it turns out that you can actually use this to show that amongst all the elements in the F_q star. Let us say that there is an element β whose order is the maximum, what is that mean?

(Refer Side Time: 24:50)



Amongst all the elements in F_q^* , let β have maximal order $= r$.

Claim: Every element $\alpha \in F_q^*$ has order dividing r .

If α have order $= r$, e_1

It means that you are looking at all the elements in the finite field and you looking at all their orders, and you want to pick the elements that has the largest possible orders. And let say that there is an element β whose order is the maximum. What is that mean? It means that you are looking at all the elements in the finite field, you looking at all the orders and you want to pick the element perhaps the largest possible order, and let say the order is β , and let say the order is r . Then the interesting claim that the order of all the other elements in the finite field must divide r .

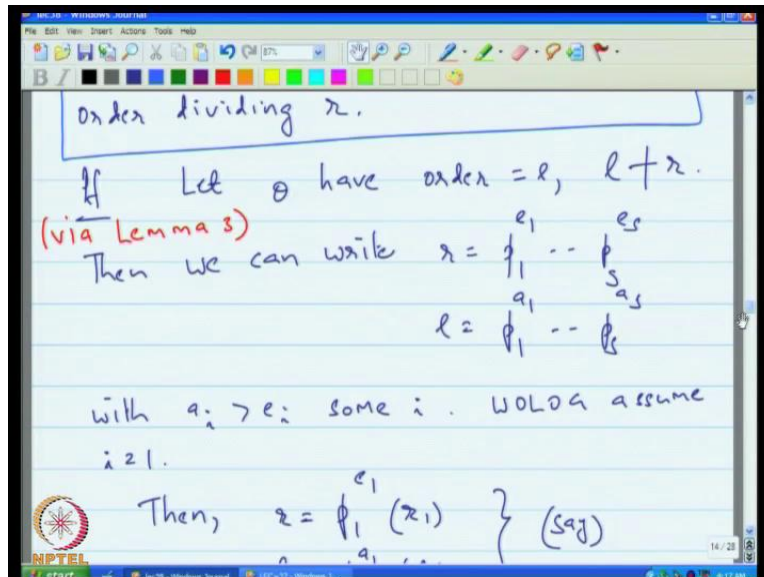
(Refer Side Time: 25:34)

0	$\alpha^4 = \alpha + 1$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^0 = 1$	$\alpha^5 = \alpha^2 + \alpha$	$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^1 = \alpha$	$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1$
$\alpha^2 = \alpha^2$	$\alpha^7 = \alpha^4 + \alpha^3$	$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + 1$
$\alpha^3 = \alpha^3$	$\alpha^8 = \alpha^4 + \alpha^2 + \alpha$	$\alpha^{15} = \alpha^4 + \alpha = \alpha + \alpha + 1 = 1$
	$= \alpha^2 + 1$	
	$\alpha^9 = \alpha^3 + \alpha$	
	$\alpha^{10} = \alpha^4 + \alpha^2$	
	$= \alpha^2 + \alpha + 1$	

For example, if we go back to our lecture of last time, here are the 16 elements in the finite field of size 16, we notice here that $\alpha^{15} = 1$ as the order 15 is the largest possible order in the finite field. And interestingly what that the claim saying is that every non-zero element, so you exclude this 0, every non-zero element in the field must have order that divides 15.

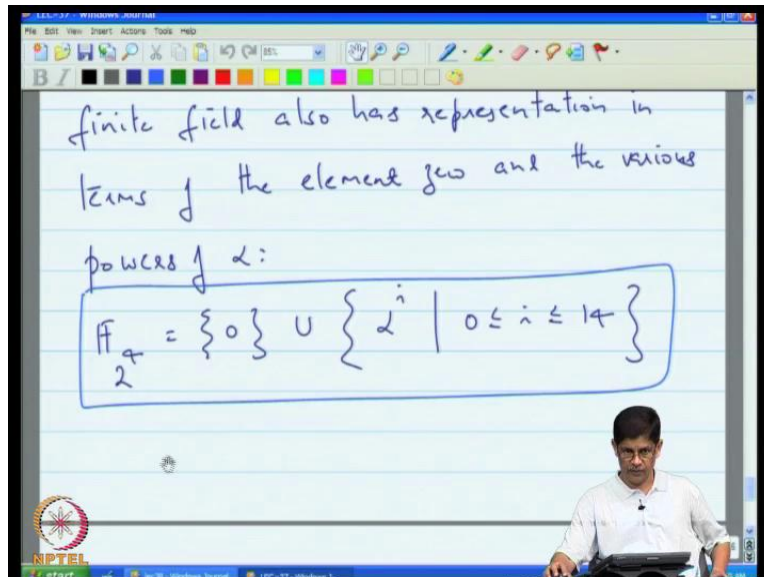
So, we can actually verify for example that α^5 is order 3, α^7 is order 15, α^3 is order 5. So, all these orders actually divide 15 and that is the content of this claim. Every element of the order that divides r and the distinguishing feature of r is just keep in mind and the distinguishing feature of r is that is the maximum order of non-zero element. And again this proof did not work here, the proof is again technical. So, actually skip it, but it did not in case what you want to follow through with the details, so then what I have been shown tomorrow.

(Refer Side Time: 27:22)



Now, what we actually shown is this lemma here lemma 3 is used to proof lemma 4, but we used to proof the claim. Let me just make a remark here, we will just say that the proof here is via lemma 3. So, lemma 3 comes into play in actually proving this claim. Now, we come to other lemma and what the lemma says is that well you know earlier you are talking about the maximum order of an element, and you called it r will the truth is that if the finite field contains q elements, then I can tell you what that the maximum order is.

(Refer Side Time: 28:15)



That maximum order is precisely one less than the size of the field. So, another word the maximum order here is the q minus 1, which is p to the m minus 1, and that is an agreement for an example here in our last lecture, we have a finite field of 16 elements. The finite field look like this, contains 0 and all the other elements were power of some element α , this is the very simple picture of the finite field that we like to deduce. And what the lemma that we just looking out is that in a finite field of 16 elements, the maximum possible order that any element can have is 15. And that what this and what this table is saying is that well α here is order 15, say it has maximum possible order. We are just we are identify the element of maximal possible order.

(Refer Side Time: 29:18)

The screenshot shows a digital whiteboard interface with a toolbar at the top. The handwritten text on the whiteboard is as follows:

$\Rightarrow \theta$ has order r

$$\theta^r = 1 \Rightarrow x^r - 1 \Big|_{x=\theta} = 0.$$

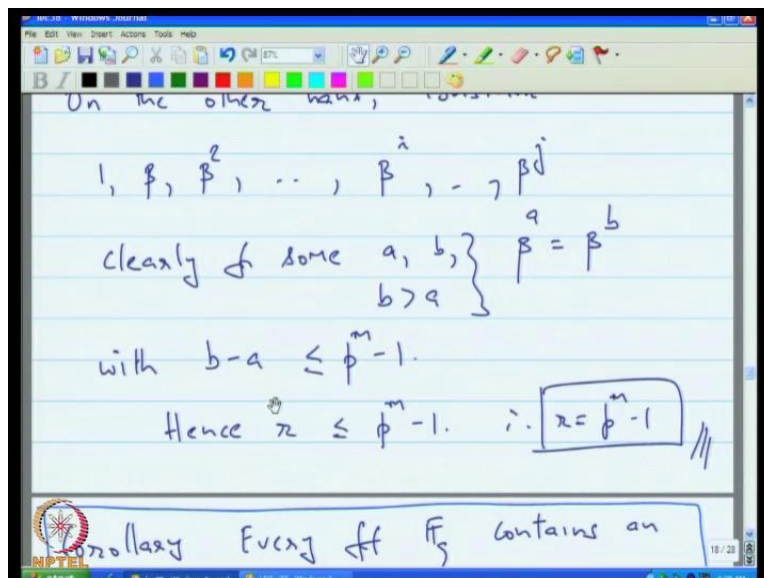
It follows that every nonzero element in \mathbb{F}_q is a zero of $(x^r - 1)$.

$\therefore r \geq \phi - 1.$

Below the whiteboard, a lecturer is visible, and the text "concludes" is partially written.

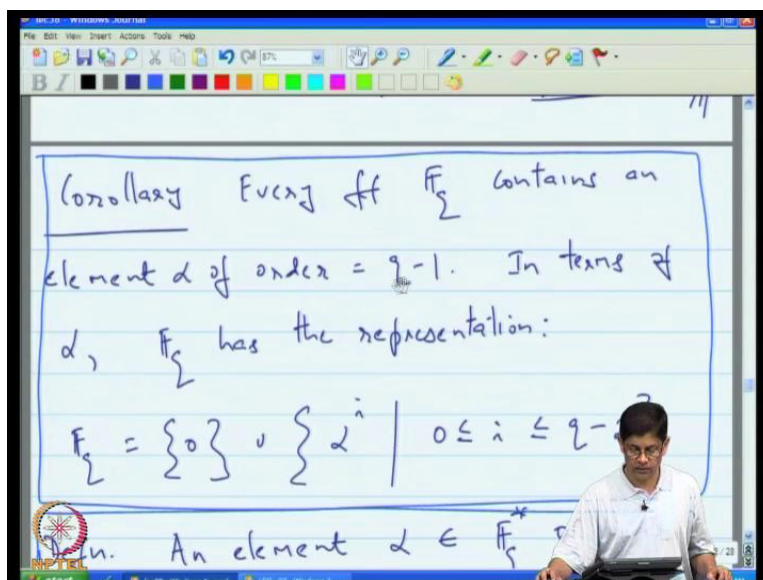
How do you prove that? So, the proof is straight forward let β have maximum order r , and we want to show that this r is q minus 1 or p to the m minus 1. Now, since θ and \mathbb{F}_q star, if θ belongs to \mathbb{F}_q star then θ must be order dividing r , which means that the θ to the r is equal to 1, which means that the θ is 0 of the polynomial x to the r minus one. But θ is just any arbitrary element in \mathbb{F}_q star that means for every non-zero element in \mathbb{F}_q is a 0 of x to the r minus 1. But the fundamental theorem of algebra tells that if you take a polynomial of degrees r it can have no more than r 0s in the field.

(Refer Side Time: 30:05)



Therefore, it must be that the r is greater than or equal to p to the m minus 1, other than if you consider 1, β , β^2 increasing powers of β . Again for some pair a, b β^a must equal β^b with $b - a \leq p^m - 1$, because the finite field contains only $p^m - 1$ non-zero elements. So, by the time we reach $p^m - 2$, you achieve the maximal possible counts thereafter any elements that you get must be repeat of some earlier element and therefore it must be true. That the difference between b and a must be less than or equal to $p^m - 1$.

(Refer Side Time: 30:48)



Therefore, the maximal order must be less than or equal to $p^n - 1$, because this here is equivalent to saying that the beta that beta with the $b - a$ is equal to 1, beta to the p , $b - a$ is equal to 1, but r is the order. So this must be greater than or equal to r so $b - a$. We know that from this sequence here that $b - a$ is less than or equal to $r p^n - 1$ and r must be less than or equal to this.

Therefore r is less than or equal to the $p^n - 1$, but we just show that r is greater than or equal to it so the conclusion is r is equal to $p^n - 1$. Now it is possible that went little faster than you might have light, but the result is easy to keep in mind is just say that look. If you are looking at all the elements non-zero elements in the finite field, you look at all their orders and you pick the largest order of a non-zero element that number is precisely 1 less than the size of a of the field.

(Refer Side Time: 32:34)

$$F_q = \{0\} \cup \{ \alpha^i \mid 0 \leq i \leq q-2 \}$$

Defn. An element $\alpha \in F_q^*$ of order $= (q-1)$ is called a primitive element of F_q .

Ex Consider $F_4 = F_2[x] / (x^2 + x + 1)$
 $(x^2 + x + 1)$ is irreducible over F_2

So, the corollary at with this, now we have a very simple picture of the finite field. The picture is that first of all every finite field contains an element whose order is q minus 1. Let us call that element α , in terms of α F_q has very simple representation as being the union of 0 together with all the non-zero elements in the field and every one of them can be represented uniquely has some power of α , where the power i ranges between 0 and q minus 2, because there are q minus 1 there must be q minus 1 elements in here. That is our beautiful representation of the finite field and important definition here.

We will frequently speak about make reference to a primitive element of a finite field. So, an element α whose order is equal to q minus 1, in other words whose order is the maximum possible is called primitive element of the finite field. So, the word primitive is used in the sense that it can be used to generate all the other elements in the field. It is primitive in the sense there is a basic element from which you can build all other elements.

(Refer Side Time: 34:12)

$$\mathbb{F}_q = \{0\} \cup \{\alpha^i \mid 0 \leq i \leq q-2\}$$

Defn. An element $\alpha \in \mathbb{F}_q^*$ of order $= (q-1)$ is called a primitive element of \mathbb{F}_q .

Ex Consider $\mathbb{F}_{2^4} = \mathbb{F}_2[x] / (x^4 + x + 1)$

$x^4 + x + 1$ is irreducible over \mathbb{F}_2

You can see that here except apart from 0, all the non-zero elements in the field can be obtained simply by taking the various powers of alpha. Now let us look at an example, so supposing this was the example that we looked at the last time. So, the p was two the reducible polynomial is $x^4 + x + 1$ and we can regard this as a collection of equivalence classes, and use alpha to denote the equivalence class of x or alternately one can actually regard alpha as an imaginary element, that is satisfying the $\alpha^4 + \alpha + 1$. What that does is that if you keep this in mind, when you can you do not have to keep carrying this around.

(Refer Side Time: 35:11)

element satisfying $\alpha^4 + \alpha + 1 = 0$
 \uparrow
 more practical!)

0	$\alpha^5 = \alpha^2 + \alpha$	$\alpha^{10} = \alpha^4 + \alpha^2$ $= \alpha^2 + \alpha + 1$
1	$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
α	$\alpha^7 = \alpha^4 + \alpha^3$ $= \alpha^3 + \alpha + 1$	$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2$ $= \alpha^3 + \alpha^2 + \alpha + 1$
α^2	$\alpha^8 = \alpha^4 + \alpha^2 + \alpha$ $= \alpha^2 + 1$	$\alpha^{13} = \alpha^4 + \alpha^2 + \alpha + 1$ $= \alpha^2 + 1$

Because your element alpha has an sense this condition that you are doing arithmetic modular $x^4 + x + 1$ in built, because $\alpha^4 + \alpha + 1$ is equal to 0, this is more practical. Here again is an example calculations, so you can see that as you take the various parts of alpha, modular making use of this relationship, you can derive and you find that you get 6 all the distinct elements in the finite field. And not only that you recover them and two representations. One representations is the one in which the non-zero elements are powers of alpha, which is this.

(Refer Side Time: 36:06)

The image shows a digital whiteboard interface with a menu bar (File, Edit, View, Insert, Actions, Tools, Help) and a toolbar with various drawing tools. The whiteboard contains the following handwritten text:

Minimal Polynomials

Note: Every element $\beta \in \mathbb{F}_\Sigma^*$ is a zero of $x^2 - 1$. Hence every element of \mathbb{F}_Σ is a zero of $x^2 - x$.

This motivates:

In the bottom right corner, a lecturer is visible, wearing a white shirt and glasses, looking at a laptop.

The other representation is one which every element in the finite field is a polynomial in α of a degree is less than or equal to 3. You can notice that everything eventually reduces to a polynomial of a degree less than or equal to 3 with binary co-efficient, and you know that number of polynomials, whose degree is less than or equal to 3 is 2 to the 3 plus 1, which is 16. Next what we want to actually talk about now that we build up the simple picture of the non-zero elements in the field. We want to build up to different picture and may be what I will do is to motivate this and let me introduce the page here.

(Refer Side Time: 37:50)

Minimal Polynomials (by example)

Eg $p=2$ $f(x) = x^4 + x + 1$

$F_2 = F_2[x] / (x^4 + x + 1)$

$F_q = \left\{ \sum_{i=0}^3 a_i \alpha^i \mid a_i \in \{0,1\} \right\}$

where $\alpha = [x]$ in $F_2[x] / (x^4 + x + 1)$

and hence satisfies $\alpha^4 + \alpha + 1 = 0$

So, what I want to do here is give your preview of what you trying to do next. Now we went to look again. So, I will say minimal polynomials and also by example, and in this example you are going to have characteristics to $f(x)$ is x^4 plus x plus 1 are a finite field of F_q is going to be $F_2[x] \text{ mod } x^4 + x + 1$, and we know that an alternative way of looking at it is that F_q is precisely the set of all polynomials $a_i \alpha^i$ where i is equal to 0 to 3 with the a_i or either 0 or 1 , where α is by the definition the equalling classes of x in $F_2[x] \text{ mod } x^4 + x + 1$ and

hence satisfies $\alpha^4 + \alpha + 1 = 0$. Now, it turns out that if you can organise the elements in the finite field in the following way you can take the elements 0.

(Refer Side Time: 40:07)

$m_\beta(x)$	β
x	0
$(x+1)$	1
$(x+\alpha)(x+\alpha^2)(x+\alpha^4) = (x^4+x+1)$	α α^2 α^4 α^8
$(x+\alpha^3)(x+\alpha^6)(x+\alpha^9) = (x^4+x+1)$	α^3 α^6 α^{12} α^9
(x^2+x+1)	α^5 α^{10}
(x^4+x^3+1)	α^7 α^{14} α^{13} α^{11}

You have 0, you have 1, you have α , α^2 , α^4 , α^8 , α^3 , α^6 , α^5 , α^{10} , α^7 , α^{14} , α^{13} , α^{11} . This is the collection of all elements in the finite field, and it first claims look like the rather peculiar way of organising it does not seem to have any structure.

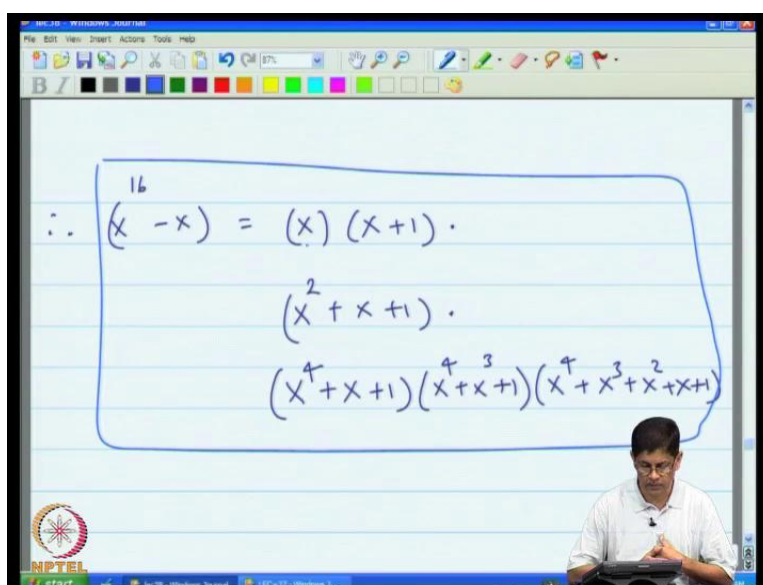
But we actually see what the structure is? First of all we want to identify with, so these this is a bunch of 4 elements, it turns out that all these elements share the same minimal polynomial. What is that minimal polynomial? Here you may think of this as being your β and here what I am going to put down is an α of x . So, it turns out that the β of this is x like. This is x plus 1, here you have $x^4 + x + 1$, $x^4 + x^3 + 1$, $x^2 + x + 1$, $x^4 + x + 1$. So, this is the structure in terms of minimal polynomials. And of course we knew that every element has a minimal polynomial, and we already knew that α had minimal polynomial, I meant we knew that the α has 0 of $x^4 + x + 1$.

So, what this is telling you is that α is as this is minimal polynomial, but it shares the minimal polynomial with all these other elements. You can actually interpret that as telling as

that in fact what is true is that $x^4 + x + 1$ can be factored according to $\alpha x + \alpha^4$, $\alpha^2 x + \alpha$, and then you also have $x + \alpha$ to the 8. So, that means that these collection of 4 elements are precisely the 0s of this, and you can write down a similar statements $(())$ get to of this line, so that you can see things more clearly. So, the similar statements can be made about all these other collections so that means that the 4 0s are these are precisely this. So, we are leading up to this, so we have this feather nice structure for the finite field. What characterises of the polynomials that appear on the left are two things. One is that every one of these polynomials is reducible, that means it cannot be factored. Secondly if you look at the degree of if you have degree 1, and you have degree 4 and you have degree 2; in terms of that every reducible polynomial, whose degree divides four appears here, so where does four coming to the picture

Therefore, comes into the picture, because after all we are dealing with the F of 2 to the 4, and it is those 4, that is actually causing these degrees to be either 4 or else interestingly divides as 4, and this is always going to the case. So, if you have F of p to the m and you write down the minimal polynomials of early elements in the finite field you are going to get polynomials over of the whose degree divides m and you going to get all of them.

(Refer Side Time: 45:04)



$$\begin{aligned} \therefore (x^4 - x) &= (x) (x+1) \cdot \\ &\quad (x^2 + x + 1) \cdot \\ &\quad (x^4 + x + 1) (x^4 + x^3 + 1) (x^4 + x^3 + x^2 + x + 1) \end{aligned}$$

$$\therefore x^4 - x^2 = (x)(x+1) \cdot (x^2 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1)$$

And so along with these you also have the accompanying statement that since we know therefore $x^{16} - x$ is x times x plus 1 times x square plus x plus 1 times x^4 plus x plus 1 times x^4 plus x cubed plus 1 times x^4 plus x cube plus x square plus x plus 1 you is a dot in here. So, that means that you can factor $x^{16} - x$ into the product of reducible polynomials, this reducible polynomials have the property that the degrees divides 2 to the 4 and 4 comes, because 16 can be expressed as 2 to the 4.

So, in fact it may be better for us to actually write these 16 over here, I just to emphasise that fact just write this as 2 to the 4, that is the picture that we trying to build up to...

(Refer Side Time: 46:22)

Minimal Polynomials

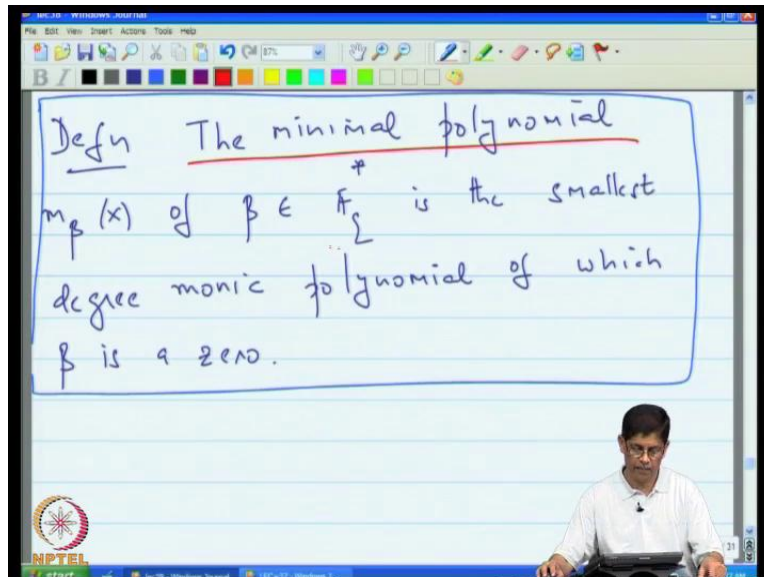
Note: Every element $\beta \in \mathbb{F}_q^*$ is a zero of $x^q - 1$. Hence every element of \mathbb{F}_q is a zero of $x^q - x$.

This motivates:

So, now having motivated the discussion of minimal polynomials, let us go ahead and look at the how would introduce this. So the way we started by discussion on minimal polynomials. Let us to say let every element non-zero element in \mathbb{F}_q is the 0 of x to the q minus 1. We have to see this, because the maximal order is excuse me, a small type of here this really is x to the q minus 1 minus 1.

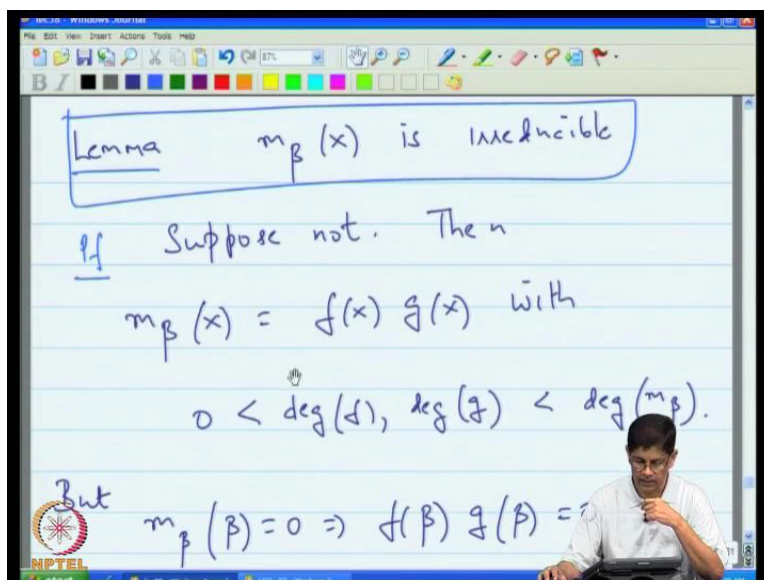
We know that the maximum order is q minus 1, and that the every element has order dividing that consequence of that is that every non-zero element to the finite field is 0 of x to the q minus 1. Only element missing in this description is the 0, but 0 is a 0 of x itself, so by multiplying this by x . We can make now the uniform statement that every element of \mathbb{F}_q is the 0 of the x to q minus x . Now given an non-zero element given an element in the finite field, there is an associative polynomial of which that element is 0, so that then it makes sums to actually define the minimal polynomial m_β of x of β of \mathbb{F}_q star is the smallest degree manic polynomial of which β is 0.

(Refer Side Time: 48:14)



We know that the every element is 0 of this, but may be this is not the smallest degree polynomial of which that element beta is 0. Let us look for that and that is called the minimal polynomial of beta and it is written as $m_{\beta}(x)$. So, in our just concluded an example, these were these polynomials $m_{\beta}(x)$. We had all of these, these are the smallest degree polynomials. For example, you asked what is the smallest degree polynomials approach alpha to the 6 to the 0, then we answer is this, and this would be $m_{\beta}(x)$ from $m_{\beta}(\alpha)$ to the 6

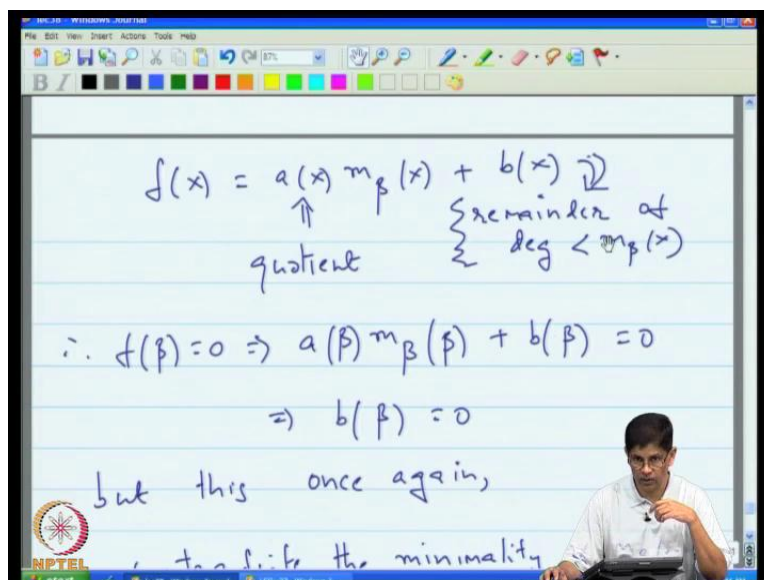
(Refer Side Time: 48:57)



The first lemma says that look $m_\beta(x)$ is reducible aware must that be, because supposing the minimal polynomial was not reducible, and there it could be factor into the product of two polynomials, each of whose degree is less than the degree of m_β . Then, because $m_\beta(\beta) = 0$, that means that the product of the $f(\beta)$ and $g(\beta)$ is 0. So either one of them must be 0, but these polynomials of degree is less than the degree of m_β , but we already said that this is the minimal polynomial.

This is the least degree polynomial of which β is the 0, so that is the contradiction. So, only conclusion that we can draw there is therefore it must be it cannot be that we can factor $m_\beta(x)$, so it must be irreducible. So, the minimal polynomial is always irreducible, and in fact we actually saw that, because already told you that in this listing here, all the polynomials that you seeing here are irreducible, let lemma just told us what that must always be the case. Then the second lemma is that look supposing you have the minimal polynomial $m_\beta(x)$ and supposing you somehow find out that $f(\beta) = 0$, then the only way that can happen is if $m_\beta(x)$ divides $f(x)$. There is the minimal polynomial of β in a way is very possessive, because it says the only polynomials which when evaluated at β will give 0 or those polynomials which $m_\beta(x)$ divides.

(Refer Side Time: 50:06)



How do you prove that basically, we use the Euclidean division algorithm you takes this $f(x)$ of which β is surprisingly is 0. So, that is the hypothesis of the lemma then we use the Euclidean division algorithm divided by m_{β} to get a remainder $f(x)$ is $a(x)$ times on $m_{\beta}(x)$ plus $b(x)$. Now $a(x)$ here is the quotient and $b(x)$ is the remainder. We know that the $m_{\beta}(\beta)$ is 0, which means that $a(\beta)m_{\beta}(\beta) + b(\beta)$ is 0, but since this is the minimal polynomial of β we know that this is 0. So, this can only happen is $b(\beta)$ is 0, then we again look this $b(x)$ has a polynomial, because you are doing division whose degree is strictly less than the degree of $m_{\beta}(x)$.

Now even this polynomial is 0 or it is not, if it is not a 0 polynomial then it would contribute the minimality of the degree of $m_{\beta}(x)$, because $m_{\beta}(x)$ is supposedly the smallest degree polynomial of which β is a root is 0. But you just discover the $b(x)$ has $m_{\beta}(\beta)$ is 0 and it is degree is lesser. So, only possibility is that $b(x)$ is actually 0, but then the $b(x)$ is 0 and you look at this is equation, you see that $m_{\beta}(x)$ must divide $f(x)$, and that is the claim of the lemma, you will put this claim is used at a way, because we already known that every non-zero element is as 0 of x to the q minus x just few minutes ago, we held on this that every element of the finite field is 0 of the x to the q minus x .

(Refer Side Time: 52:41)

unless $b(x) = 0$. Hence $m_\beta(x) \mid f(x)$

Corollary $m_\beta(x) \mid x^2 - x$

Pf. Every element in \mathbb{F}_2 is a zero of $x^2 - x$. Hence $\beta^2 - \beta = 0$
 $\Rightarrow m_\beta(x) \mid x^2 - x$.

But we just proving that the only way that can happen is if the minimal polynomial divides the x to the q minus x . So, what happening is that we shown, that the minimal polynomial of every element in the finite field divides x to the q minus x .

(Refer Side Time: 53:01)

unless $b(x) = 0$. Hence $m_\beta(x) \mid f(x)$

Corollary $m_\beta(x) \mid x^2 - x$

Pf. Every element in \mathbb{F}_2 is a zero of $x^2 - x$. Hence $\beta^2 - \beta = 0$
 $\Rightarrow m_\beta(x) \mid x^2 - x$.

So, that is where we are perspective minimal polynomials, so just to recap. So, in this lecture what we done is we first left out the multiplicative or structure of the finite field. We are actually

going through the deductive approach to the finite fields. The first thing we establish is that given a finite field of size q , there is an integer called the characteristic. And that characteristic is prime first of all then the size of the finite field must be the power of the characteristic is true, and then the finite field contains the primitive element. That is an element such that its powers generate all the non-zero elements in the finite field, and such an element is called the primitive element. So, that allows you to have the very simple picture of the finite field in your mind; one in which the finite field appears simply as the powers of some special element α which is called special element α , you can see the 16 element front out here.

So, in general we assign that this would be the structure of the finite field. And after that then we said look we can organise the finite field the elements in non-zero elements in finite field. Actually all these elements in the finite field in a different way we can kind of classify them and group them together, according to the minimal polynomial; that is the minimal polynomial being the smallest degree polynomial of which that element is 0. So, here are the 16 elements in the finite field of size 16, here are the associative minimal polynomials.

Now, we shown that each of this necessarily reducible, that each of this is necessarily divides x to the 16 minus x in general x to the q minus x . We will shown that and that is about, we are against the other thing that we also know has the reduction is that look. If you take the x to the q minus x , we know that it is 0s are all the elements in the finite field; on the other hand the elements in the finite field are 0s of minimal polynomials. So, clearly these relationships between these polynomials and the minimal polynomials, it is going to take the little bit more effort in the next class by us to actually show that this is the case there is in fact that if you multiply all the minimal polynomials together after finite field you will get x to the 16 minus x .

(Refer Slide Time: 56:07)

p.e. (primitive element) of \mathbb{F}_{16} .

Minimal Polynomials (by example)

Eg $p=2$ $f(x) = x^4 + x + 1$

$\mathbb{F}_2 = \mathbb{F}_2[x] / (x^4 + x + 1)$

So, I will said here this is the preview may be as should emphasise that and put that in the statement here. So, let me write down preview, the preview of minimal polynomials. I think this is the good place to stop, so we will continue and it one take as the very much long to find up our discussion on finite fields and that point we can talk start talking about cyclic codes. So, thank you.