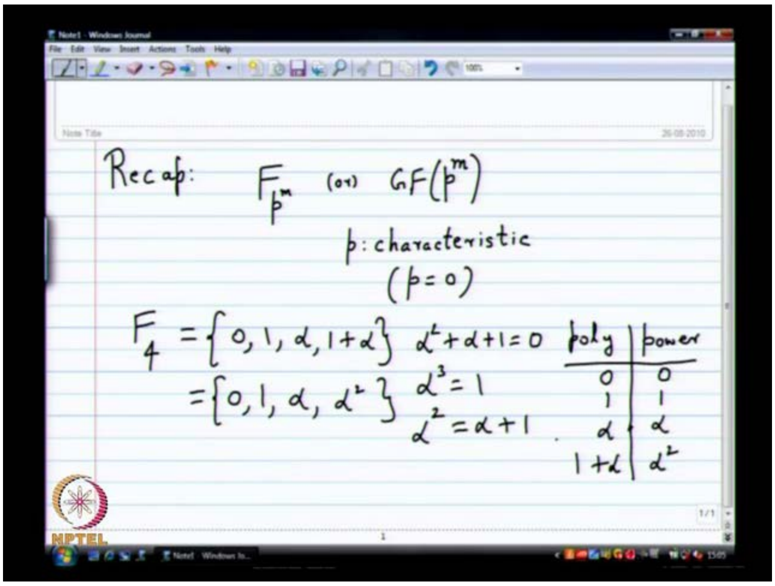
Coding Theory
Prof. Dr. Andrew Thangaraj
Department of Electronics and Communication Engineering
Indian Institute of Technology, Madras

Lecture - 10
Computations in Finite Fields

(Refer Slide Time: 00:22)



Recap: $\mathbb{F}_{p^m}$ (or) $GF(p^m)$

p: characteristic

$(p=0)$

$\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$ $\alpha^2+\alpha+1=0$

$= \{0, 1, \alpha, \alpha^2\}$ $\alpha^3 = 1$

$\alpha^2 = \alpha+1$

poly	power
0	0
1	1
α	α
$1+\alpha$	α^2

So, let us begin once again with the recap, so in the last few last few may be this is the last lecture we been looking at construction of finite fields. So, we looked at construction of fields with p power m elements, so we looked and we denoted at either as F p power m or G F p power m. So, these are finite, so they have finite number of elements, so this p and m we can we can give them some names. So, p is called characteristic, m is usually not called anything, if you want you can call it exponent or you can just say m.

So, p is called the characteristic of the field, the reason why it is called characteristics is basically p equals 0, so that is why it is called the characteristics that is the that is the reason. So, let us do a recap by looking at three very prominent examples which will which we will use quite often in this course at least. So, the first example we want to run through once again is F 4, so moment I say a field with four elements what are the immediate things that you should, you already know.

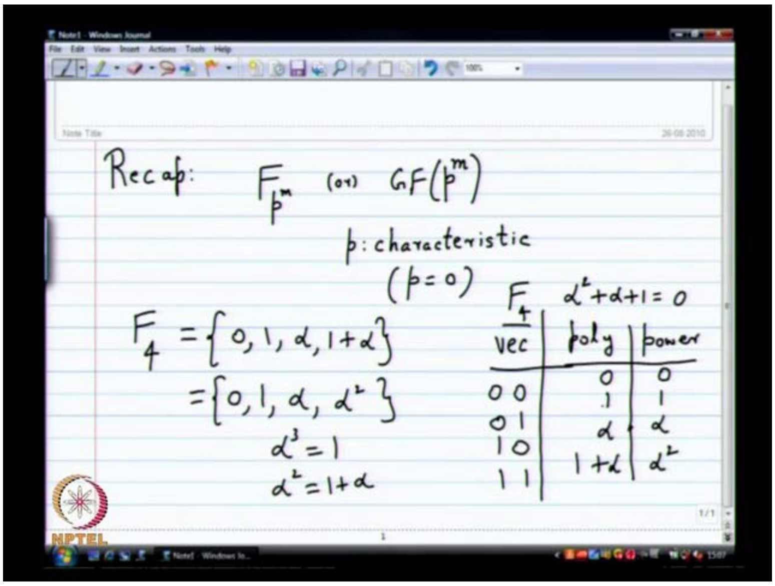
So, p is 2 and m is 2, so characteristic has to be 2 and m will be 2, all those things you immediately known, so the moment I say 4, you know all that and then is F 4 worked to have this form 0, 1 alpha 1 plus alpha. Then what else do I need to describe this field completely, I need the primitive polynomial. So, I will have to say alpha square plus alpha plus 1 equals 0, so this is the thing and with this, it will turn out that you can also show that this field can also be written as 0, 1 alpha square alpha per 3 is 1. Then I will say Alpha Square is alpha plus 1, so all these things are equivalent ways of describing this field, so one can show that this is a proper field, you can check all the axioms what the main axioms in a very high level are.

You have addition with inverse and then multiplication with inverse except for 0, everything has an inverse and multiplication is closed. So, those are the things that you can check quite easily, here the inverse is also very easy to find, so if you want some kind of a representation or a table for this field it is a its common to write the table in this form. So, you can write a table has just four elements 0, 1 alpha and 1 plus alpha, this is the polynomial notation and then you have the power notation what is the power notation 0, 1 alpha square. So, these are two ways of representing the four elements of this finite field with four entries.

So, both these notations are useful what are they useful for the polynomial notation is useful for what for doing addition and the power notation is useful for doing multiplication. If you want to do both multiplication and addition what would you do go back and forth with this, now you have to add say for instance alpha plus Alpha Square what can you do very easily go to the polynomial notation and find that is equal to 1. So, in a 4, really there is it not very complex addition and multiplication is very easy, but in larger fields such things will be very useful.

So, the polynomial notation sometimes is also written as a vector notation, so what would what would a vector notation mean. So, there is also this vector notation for polynomials do not seem to have room there, so I am going to erase this and then write the vector notation next to it.

(Refer Slide Time: 04:33)



Recap: F_{p^m} (or) $GF(p^m)$

p : characteristic

$(p=0)$

$F_4 = \{0, 1, \alpha, 1+\alpha\}$

$= \{0, 1, \alpha, \alpha^2\}$

$\alpha^3 = 1$

$\alpha^2 = 1+\alpha$

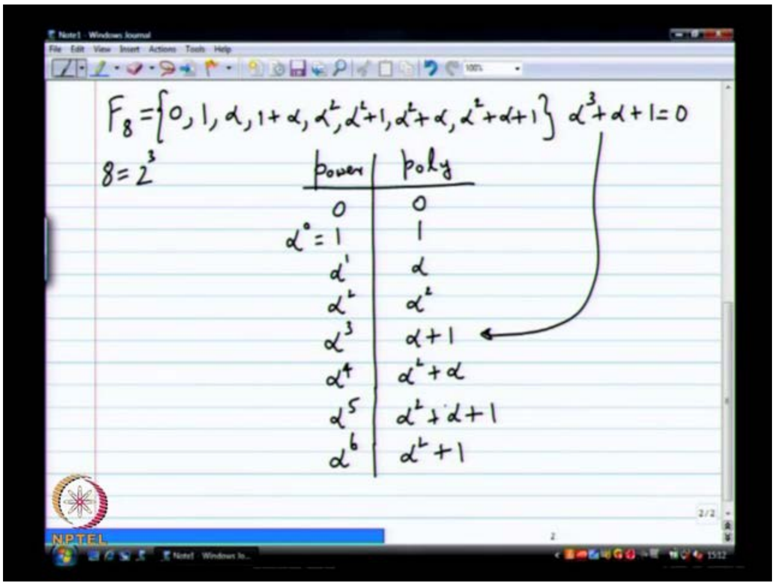
F_4 $\alpha^2+\alpha+1=0$

vec	poly	power
0 0	0	0
0 1	1	1
1 0	α	α
1 1	$1+\alpha$	α^2

So, I will write the conditions here, I will write the vector notation here, so the vector notation is also popular. So, basically you write the coefficients as vectors remember what is F 4, F 4 has polynomials with coefficients from F 2 of degree less than or equal to 1. So, it will have the two coefficients the constant term and the linear term, so you write both the coefficients as vector. So, this would be 0, 0, this would be 0, 1 this would be 1, 0, this would be 1, 1, so what is the advantage of the vector notation over the polynomial notation, but in it if you want to write a computer program, you might want to think of a vector or something that you can represent, it still does not really matter.

So, all are the same, there is really no advantage for the vector notation, let us compare to the polynomial advantage notation it is used. So, you should know that this used, I mean these conditions are crucial conditions are very crucial. So, usually on the top you have to save what the primitive polynomial is you have to save this. Once you save this, it is when I define F 4, but still I mean you have to save that condition, if you just look at it algebraically by looking at this, it is not consistent unless you say alpha square plus alpha plus 1 is 0. So, that is F 4, I am going to make a table like this for F 8 and I will also urge you to make a similar table for F 16. It is important that you do it from for various reasons and definitely it will be useful for you and for problem solving and all that, so let us do that for F 8.

(Refer Slide Time: 06:54)



$F_8 = \{0, 1, \alpha, 1+\alpha, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$ $\alpha^3+\alpha+1=0$

$8 = 2^3$

Power	Poly
0	0
$\alpha^0 = 1$	1
α^1	α
α^2	α^2
α^3	$\alpha+1$
α^4	$\alpha^2+\alpha$
α^5	$\alpha^2+\alpha+1$
α^6	α^2+1

You have eight elements, of course 0, 1, so once again I say 8, the two things we can figure out are p and m, so 8 is 2 power 3. So, clearly characteristic has to be 2 and the field is made up of polynomials in some alpha with coefficients from F 2 and degree less than or equal to 3. So, those are 8 elements that you have, so if you want you can write it down alpha 1 plus alpha, where you will have the alpha square terms alpha square, alpha square plus 1, alpha square plus alpha square plus alpha plus 1. Then the primitive polynomial is important, you have these 8 polynomials, then what is the primitive polynomial, you can take any one of two possibilities, we will take this one, so that is F 8.

So, to make the table the polynomial verses power table, it is good to go from the power notation to the polynomial notation. So, it is something that I used, you might also have other ideas to do this, but this is one idea which works quite well, 0 and 1 are the easiest. They just they remain the same in both notations, so no confusion 0 is 0 and 1 is 1 by the way there is one thing you will find. For instance, if you look at mat lab in the power notation, you cannot write 0 as alpha power anything, of course from alpha power 0 onwards 0 is nothing.

So, what they usually do is they say in the power notation minus infinity alpha power minus infinity alpha power minus infinity is 0. So, in mat lab, the symbol minus capital I n F is used for 0 in the power notation, so if you are doing Galois field arithmetic in mat lab, you might see that usage in in the in the polynomial notation, there is no confusion. Sometimes, the power notation they use minus infinity on the other hand the latest mat lab only uses the polynomial type of notation. You cannot have any way, so minus infinity is sometimes used for 0, I just want to point that out.

So, alpha power 0 is 1 and then you have alpha power 1 which is just itself, then alpha square is also alpha square up to here, there is no problem in the polynomial notation. Then when you go to alpha power 3, clearly it is not in the list of elements, I have for have in F 8, but I know I can simplify it using the primitive polynomial, so that is the idea, so alpha power 3 would become alpha plus 1.

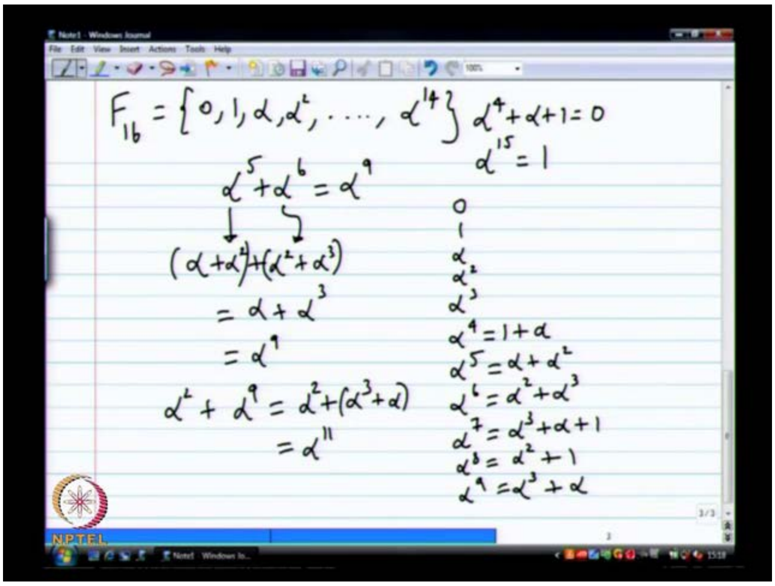
So, you simply use this equation here to get alpha power 3 to be alpha plus 1, then alpha power 4 is quite easy, what do you do, you simply multiply the previous thing by alpha. So, that is the idea you can use to build this table very easily. Here, alpha power 4 is alpha power 3 times alpha, so when you multiply this alpha, you get alpha square plus alpha and that is very much in the F 8 that I have written down here.

Then, you have alpha power 5 for which once again we have to multiply the previous thing by alpha, but then what would you get alpha power 3 plus alpha square and then once again the alpha power 3 has to be substituted. So, you would pretty much get alpha squared plus alpha plus 1, then the last thing alpha power 6, we can write down by elimination which is alpha squared plus 1. Now, we can do the computation again you will see you will get alpha square plus 1.

So, this table is crucial if you want to do any computations with finite fields, so for instance if I give you matrix with finite field entries and you have to do Gaussian elimination on it, then this field becomes this table becomes crucial, So, when you do finite field when you do a row operations, you are doing, you have to do what the finite field arithmetic is for that this table is fairly useful.

So, we will come back and see that little bit later, so this is how you construct F 4 and F 8. If somebody asked you what is F 4, you should not say I do not know, you should say I know F 4, F 4 is simply 0, 1 alpha squared with alpha squared being equal to 1 plus alpha and alpha per 3 being 1. So, that is the very simple way of the finding, so if I have 16 also, you can do a very similar thing.

(Refer Slide Time: 12:04)



$$F_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\} \quad \alpha^4+\alpha+1=0$$

$$\alpha^{15}=1$$

$$\begin{aligned} \alpha^5 + \alpha^6 &= \alpha^9 \\ \downarrow \quad & \downarrow \\ (\alpha+\alpha^2)+(\alpha^2+\alpha^3) & \\ = \alpha+\alpha^3 & \\ = \alpha^9 & \end{aligned}$$

$$\alpha^2 + \alpha^9 = \alpha^2+(\alpha^3+\alpha)$$

$$= \alpha^{11}$$

0

1

α

α^2

α^3

$\alpha^4 = 1+\alpha$

$\alpha^5 = \alpha+\alpha^2$

$\alpha^6 = \alpha^2+\alpha^3$

$\alpha^7 = \alpha^3+\alpha+1$

$\alpha^8 = \alpha^2+1$

$\alpha^9 = \alpha^3+\alpha$

I am not going to do it, I will simply write it down just to show you how you can easily write down alpha squared all the way till alpha power 14. I will write it in the power notation because it is very easy to write in the power notation and then the primitive polynomial you have to say what it is. So, for instance one thing you can take is alpha power four plus alpha plus 1 if you use this you will get alpha power 15 to be equal to 1 known, you can write this alpha power 15 equal to 1 quite easily by the fact that this is a primitive polynomial.

So, because you remember by the definition of that polynomial the smallest n for which it divides x power n minus 1 is when n equals 15. So, it will divide, so you might ask will it always divide any polynomial of that form, it turns out it will all those things we would not see in this course at least. So, it is a very consistent definition do not be worried about why that definition make sense, so it makes a lot of sense, it will define 15, so that is the result here.

So, for this, now we can make a table, you can make a table for instance, if I ask you to do some summing up for instance, let us say alpha power 5 plus alpha power 6, if I ask you this, what would be the answer in this case? It may be a little bit easy because one of those equations will readily give you the answer if you multiply both sides by alpha power 5, so you will get any way it does not matter.

So, to the readymade way of doing it is to have that table, once you have the table, you go and look up what alpha power 5 is and then you look up what alpha power 6 is then add it up you will get the answer in the polynomial notation. Then you can go back to the power notation, so let me do that real quick for this case, so when the power notation you are getting 0, 1 alpha square alpha power 3 alpha power 4 alpha power 5 would be what alpha power 4 is 1 plus alpha. What would be alpha power 5 alpha plus alpha square, what would be alpha power 6, alpha squared plus alpha power 3, now we can do this addition.

So, let me do a few more just to get to the point where this will come alpha power 3 plus alpha plus 1, then alpha power 8 is alpha squared plus 1, then alpha power 9 is alpha power 3 plus alpha. So, with some foresight, I know the answer will come within this, so let us say alpha power 5 plus alpha power 6, how I do this computation, so this is the table I am assuming that this table is given to you or you have generated it.

Using the equations, I have given you, so how do this summation you substitute what you have for alpha power 5 that would be alpha plus alpha squared. Then you use what you have for alpha power 6, what is that alpha square plus alpha power 3. So, these two when added what do you get alpha plus alpha power 3 is that, now you go back to this table and look it up you see that this is the same as alpha power 9.

So, using this I can now say these two things will add up to give me alpha power 9 another thing you can do is you can take this equation alpha power 4 plus alpha plus 1 equal to 0 and multiplied by alpha power 5. So, you directly get the answer alpha power minus that is what I said, this addition is very easy to do in this equation, but there are there is many more algorithmic way of doing it. This is may be a creative way of doing the answer, but algorithmic way of doing is still you look up this table and do it.

So, this is the same as what I did to the multiplication, so for instance if you have to do a little bit something a little bit more complicated, let us say alpha square plus alpha power 9. So, it is not very obvious, what it is, so you have to look it up, so you have to find out alpha power 9 and then you will get alpha square plus alpha power 3 plus alpha. You have to look it up in the table, so we have not gone all the way up, so if you that, you will get the answer, what do you think the answer is, let me see who is going to tell me what this works out 11 alpha 11, so many of you people are saying 11, so you would get 11.

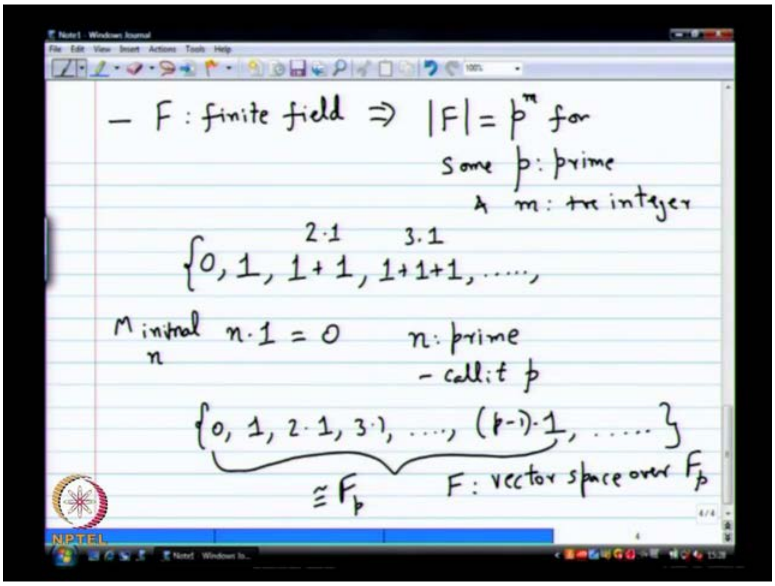
So, when these are the kind of computations that you have to become comfortable with doing. This is how we work with finite fields, so the only field that you might be very familiar with I do not know, let me not think I can say, but rational field I guess is most people are quite comfortable with doing additions and multiplications and real numbers. Also, you have a calculator may be right, so things like that you will you can do very easily, but when you do complex arithmetic your are implicitly doing something like this.

So, remember every complex number you write it as a plus b i, then whenever you multiply what rule do you use for i square i square gives minus 1. So, that is very similar to this rule, so this actually something very similar happening, here also you write a rule for this alpha. Then you do the multiplication with that, so that is the idea, so it is a bit of a pain to go from power notation to vector notation or polynomial notation and back, but there is no other way to do the computation. In a way it is easy, but it is also little bit time consuming if you are not comfortable with this.

If I give you 5 by 10 matrix with entries from F 16 and ask you to do Gaussian elimination to find rank, it will take the better part of one hour exam and then you cannot answer any other question following. So, it is a good idea to practice these things, so you be comfortable with what the arithmetic is its fairly crucial any questions on how the arithmetic is working out.

So, the next thing I am going to do in this lecture is to give you a brief idea for why is one for some abstract reason, why all finite fields will be this way. I would not I would not do it completely, I would not do give all the proofs, but just a brief idea from a high level for why there will be no other finite fields.

(Refer Slide Time: 19:23)



– F : finite field $\Rightarrow |F| = p^m$ for some p : prime & m : +ve integer

$$\{0, 1, \overset{2\cdot 1}{1+1}, \overset{3\cdot 1}{1+1+1}, \ldots,$$

Minimal n $n \cdot 1 = 0$ n : prime – call it p

$$\underbrace{\{0, 1, 2\cdot 1, 3\cdot 1, \ldots, (p-1)\cdot 1}_{\cong F_p}, \ldots\}$$

F : vector space over F_p

So, what are these there are couple of facts which are quite interesting which you should know but may be in an advance course. You will see the proof the first fact is if F is a finite field, what do we mean by a finite field? A field that has a finite number of elements, so this implies size of F that is the number of fields in F will be number of elements in F, sorry will be equal to p power m for some p which is prime and m which is a positive integer.

So, this is I mean reasonably a powerful statement and we will see finally, complete proof of this it is not too difficult to prove this. So, on the top of the top of the hat, you might think this is a very impressive result, do you think or not this is because I say F is finite number of has finite number of elements. It is a field it has to have the size p power m, so I will give you a simple argument it is a bit of an abstract argument. If you do not follow every step it is not too crucial, but just to give you a feel for how this proofs work, so suppose I tell you F is a finite field what are the possible elements that F can have.

So, the first element that you know for sure F will have is the additive identity 0, the next element which you can be sure, it will have is the multiplicative identity 1. Beyond that, you really do not know same abstract field, I mean it has a bunch of elements and it has follows all those rules. These are the only two things you know, first thing is you might suspect is may be one is equal to 0, if one is equal to 0, then there will be nothing else in the field.

So, it is a becomes a very trivial ridiculous little field, so you do not worry about it too much and then you ask the question what else can I create from these two elements what field operations. I can do with these two elements to may be generate more elements in this field what can I do, so the only thing you can do to generate non trivial elements of this field is to take one and add it to itself. It was anything else, you do you will only get the fields that are elements that are in this, so you can take 1 and add it to itself, so you might want to do say 1 plus 1.

I have no idea what this element is 1 plus 1 has to be in the field when you can do it once again, you can do 1 plus 1 plus 1, so I can use a short hand, I can represent 1 plus 1 as 2 times 1 this is just a short hand notation for 1 plus 1, I do not want to keep on writing 1 plus 1 plus 1. So, instead of 3, 3 when I added 3 times I might say 3 times 1 s. So, that is those all these guess must be there and eventually what should happen, can it go on and on and on forever.

Now, the field is finite I know the field is finite, it has to be it has to end somewhere, so there has to be an n times 1 which will become which will repeat which will give you another thing, how can I know that? It will be in this same set, so you believe me when I tell you right leave that leave one of these things only, so you have to there has to be n times 1 which has to repeat and it has to repeat in 0 because if it does not repeat in 0, you can do some small with while respecting the field axioms.

You can show that there is some violation, it has to result in 0, so there has to be a minimal n times 1 which will become 0, so this is minimal n minimal n such that n times 1 is 0 in this field. Now, with out to much effort you can show that this n has to be prime, so may with too much effort I do not know we can show that n has to be prime because if n is not prime, then you can take a times 1 and show that when it multiplies with b times 1 you will get 0.

This means either a times 1 has to be 0 or b times 1 has to be 0, so these are things that you can prove in abstract field axioms you do not need any actual field elements to show these things. So, using some arguments like that you can show n has to be prime, so let us say we will take n is prime, so if the number is prime it violates some law to call it n you have to call it p. So, you make it p, so you know in this field you will have elements of the form, so n is prime, so you call it p, so this p is called a characteristic of the field, so that is why you called it characteristic, so p is equal to 0 and that is the minimal p that will be 0 p times 1 will be 0.

It is also very common in fields to write 2 times 1 as 2 itself, so you do not have to say its 2 times 1, you can say its 2, now just because I said F is finite, I already know F has elements of the form 0, 1, 2 times 1, 3 times 1 all the way to p minus 1 times 1. Then p times 1 it would not have p times 1, it comes back to 0, so may be some other elements, now the next thing to show is disguise here is actually what is known as isomorphic are very similar to F p. So, we can show this is F p in disguise, now you can do a very simple proof that it is not too hard just laborious writing you have to do based on the axioms to show that this is F p.

You can identify 2 times 1 with 2 itself 3 times 1 with 3 itself and you see every addition and multiplication will be constant whether you do it in this abstract feel that I do not know about or you can do the same thing in F p. You will get the exact same result, so this 2 will be i, some it is not too difficult to prove p is equal to 0 and p is equal to 0 and my F p also and we do the any addition or multiplication. Remember, this all 1 plus 1 plus 1, so if even if you do multiplication or addition it is same as multiplying integers and adding integers mod p.

So, it is not too difficult to show that see you see this is F p all right the next step is little bit more abstract what you can show is once you know that F p is contained in F. So, in some my somewhat if it form and F is finite field F p is contained in this and p is 0, all that is true, so what will happen is F will become a finite vector space over F p, you can show that. So, it is also not too difficult, we can prove all those axioms for abstract vector space, so you can show not only is F p contained in this F f is a vector space over F p. Now, that is enough to show that size of F as to be equal to p power m for some positive integer is a finite set.

So, it is a finite vector space finite dimensional vector space over F p which means what there will be some dimension for it. So, you will have let us say m is the dimension if you have dimension m for a vector space over F p it has to have only p per m elements how will I know that there will be m basis vectors. You take just m possible co efficiency to multiply an add them to make linear combinations, you get all vectors in F, so clearly it has to be p power m.

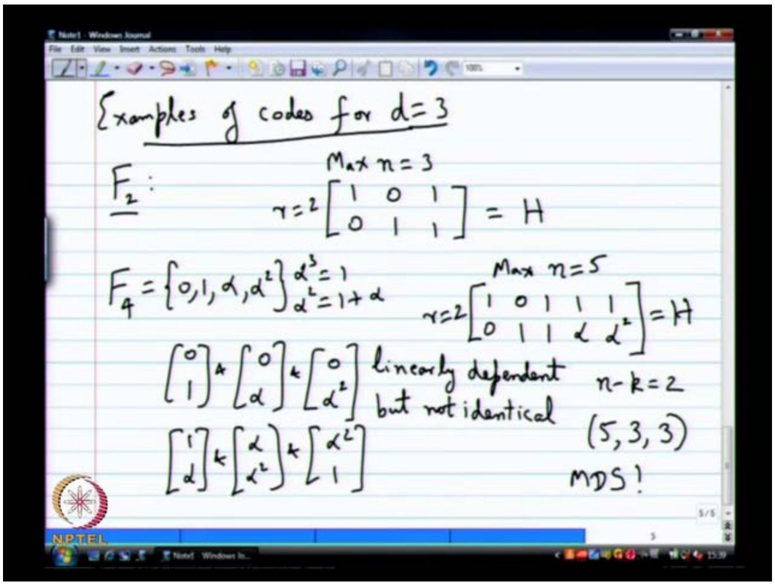
So, across a very quick half a page argument, but usually if you read a book it takes some time to write down you know mean you have to carefully write it down. So, all those things when you write down you can show just because F is a finite field the number of elements in F as to be equal to p power m.

That p is some prime and m is some positive integer, so it is not too difficult from here to show a polynomial notation. Then you to have to show primitive polynomial all those things are not very hard what is a little bit involved are to show the existence of the primitive element of that one element which will generate all the elements of this F p by powers. The power notation is a little bit more tricky to prove, but there are proves there are very much eminently elementary proves for that fact also if you are interested.

I can point you to some good references for up, so that is enough of abstract stuff, so I am sure you wondering if is a finite feel, but what do you mean it subtract it does not exist meaning of course in x is do not worry about it. So, what is more important for you is this table, so this kind of tables it should be very comfortable with, so once I tell you F 8, you should know that I have to look for a primitive polynomial of degree 3 with co effecients from F 2 and then I should be able to write down both the power notation and the polynomial notation.

Once I do that, I can do any computation I want an in F 8 that is the basic idea in tutorials may be there will be some problems to help you get acquainted with these computations. So, that takes me to some let see some highly interesting coding stuff with this feels before we move on to really good codes. So, what did I promise you when we embarked on this finite feel adventure d equal to 5, d equal to 5, so we would not see d equal to 5 will just see d equals 3 for now, but still you will see that finite feels give you something more.

(Refer Slide Time: 29:17)



Examples of codes for $d=3$

F_2 :

Max $n=3$

$$r=2\begin{bmatrix}1&0&1\\0&1&1\end{bmatrix}=H$$

$F_4=\{0,1,\alpha,\alpha^2\}$ $\alpha^3=1$, $\alpha^2=1+\alpha$

Max $n=5$

$$r=2\begin{bmatrix}1&0&1&1&1\\0&1&1&\alpha&\alpha^2\end{bmatrix}=H$$

$$\begin{bmatrix}0\\1\end{bmatrix}\sim\begin{bmatrix}0\\\alpha\end{bmatrix}\sim\begin{bmatrix}0\\\alpha^2\end{bmatrix}$$ linearly dependent but not identical

$$\begin{bmatrix}1\\\alpha\end{bmatrix}\sim\begin{bmatrix}\alpha\\\alpha^2\end{bmatrix}\sim\begin{bmatrix}\alpha^2\\1\end{bmatrix}$$

$n-k=2$

$(5,3,3)$

MDS!

So, with F 2, so let us see some examples of codes construction for d equals 3 only I am not promising anything beyond that let us see for d equals 3 first. So, let us say we start with just F 2 first you just binary codes I want to construct a parity check matrix with 2 rows. So, this my parity check matrix, I want to have d equals 3, I want to have 2 rows what does the maximum n that is possible 3, I cannot do better than 3, so I can do 1, 0.

It is going to become linearly independent, there is no problem n equals 3 is the max, now let us try to think about the same question, but with F 4 remember what does F 4 0, 1 alpha squared alpha per 3 is one and alpha squared is one plus alpha. So, this is F 4, let us try to ask the same question, but now I have to be a little bit careful here because I did not really define codes over F 4 we are defined codes over F 2, but I did not really spend a lot of time defining codes over F 4. Let us just briefly try to construct a parity check matrix which will satisfy the constrains for d equals 3, so remember what is a constrain for d equals 3 for the parity check matrix no all zero column no identical column is there enough for F 4.

So, no to column must be linearly independent, so you should refresh that a little bit an F 2 it was the same as identical in F 4. It is not the same why you can have you can have two non identical vectors which are linearly dependent in F 4 why that is. So, you could take intense 0, 1 and 0 alpha this 2 are not identical, but they are linearly dependent linearly dependent why alpha time. So, you see somehow disagree with that because you know is it is everybody with that this two are linearly dependent, so it is like there are on this y axis both of them are on the y axis if you think of this top thing as the x axis bottom is y axis.

Both of them are on the y axis is you multiply this guy will alpha you get 0 alpha n in fact even this guy is linearly dependent if you want a slightly more complicated example you can have one alpha. Then what alpha squared and alpha squared one, these three guys are also linearly dependent, but not identical, so linearly it dependent, so those 2 conditions are enough. You cannot have the all zero column and you cannot have 2 columns being scaled versions of each other. So, you cannot have linearly dependent columns, now let us try to construct a parity check matrix like that, once again with the r equals 2 you have to tell me what the max n.

Now, you seen simple enough how any columns can you have is it just 3, can you do more than 3, no you cannot do more than three you cannot stare at the board an answer this question. You would write something down, no you just try give me something with n equals 3 first. So, let us do 1, 0, you can put right 0, 1, you can put now what does this rule out first of all how many possible length to vectors are there with F 4, y is a 4 set of it 4 for the first and 4 for the second that is 4 squared that. So, it is a very simple computation, but think about it for a while set rate you convinced 16 different, there will be one which will be just 0, 0 and that is ruled out.

I cannot do it. So, I have 15 different choices for for each column, but if I select 1 column, how many columns, how many vectors get ruled out.

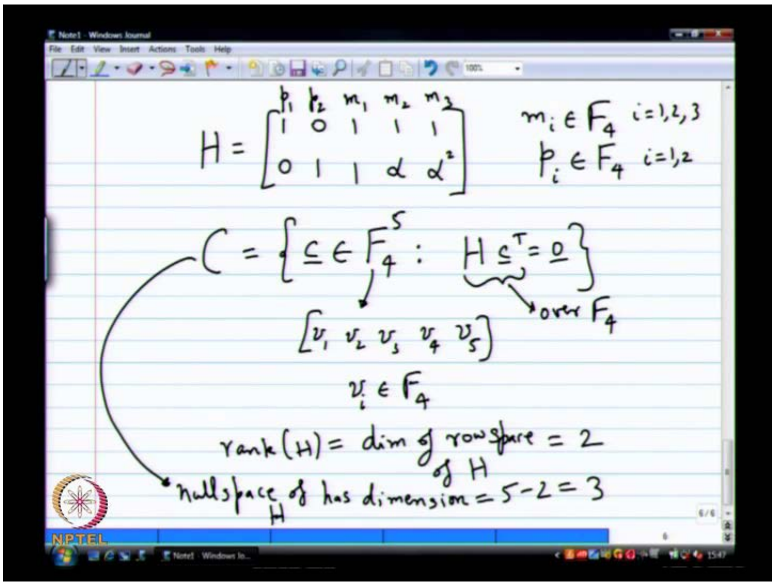
Student: ((Refer Time: 34:30))

Two are the 2 are thus get ruled out right, what are the 2 are thus get ruled that that get ruled out well, that way that row it is that column itself gets ruled out that is one, and then 2 others what are the others? Alpha time alpha time start, an alpha squared times that do you agree those those 3 get ruled out. So, the moment I put, 1 0 I cannot put alpha 0 are alpha squared 0 the moment I put 0 1, I cannot put 0 alpha 0 alpha squared or 0 alpha, then what else can I put? Just take anything else let us say 1 1. So, if I take 1 1 what can I not put alpha alpha alpha square alpha square is there anything left yeah, definitely 1 alpha as left, right. What about 1 alpha squared? 1 alpha and 1 alpha square are not linear not linearly dependent, 1 alpha square is also there. Now I cannot really do more. So, maybe you cannot prove it, but in max's in this case will turn out to be 5 is this ruled out everything, all the other vectors are linearly dependent with one of this things. You can pick there are various other choice sum I am not saying this is the only choice for the h, but this is one of them which satisfies the condition for d equals 3.

Yes or no, yes. What is the rank of this matrix? Two yes, because you have an eyes sitting there right. So, it has to be 2. So, so n is 5, n minus k is 2. So, you have 5 comma 3 comma, what is d? It is equal to 3 can you find a code with 3 non zero entries yeah. So, do you. So, question is do you have 3 columns which are linearly dependent yeah, very much definitely there, right. The first 3 columns are linearly dependent, and several other you think any 3 if you take it will be linearly dependent 5 3 3 code, no surprises what type of a code is this it meets one of those bound set we had a it is an m d s code. So, d equals n minus k plus 1. So, this an m d s code.

So, it will meet this singleton bound. So, something somethimg you cannot do with binary, for r equals 2 right for equals 2 and binary there is no unless unless you have some trivial like n equals 3 are something it is there, but if you have larger n you cannot have it is no none trivial bound code that meets a singleton bound. So, mounts (( )) mountly go to f 4 you have code that meets the singleton bound. So, it is... So, it gives you something more, and you can see it very easily yes or no, but I am actually cheating a little bit here, but may be in right now you cannot see it immediately later on I will point out what does the cheat, what the cheat is at that time you will know oh really that will be your response anyway see that, but anyway it does not matter at least from n k d you get a larger range by going to from f f 2 to f 4, definitely. And you can also get to d equals 5 and all very easily in a very systematic way that I the real selling point right, this is not there major selling point d equals 3 you anyway know how to do? And binary it is not much better takes some time to digest, this is an important thing I am going ask where is my several more questions after this. Let us see is that everybody convinced all right.

(Refer Slide Time: 38:38)



$$H = \begin{array}{c} \\ \\ \end{array}\begin{array}{ccccc} p_1 & p_2 & m_1 & m_2 & m_3 \\ \end{array}$$

$$H = \left[\begin{array}{ccccc} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 \end{array}\right] \qquad m_i \in F_4 \;\; i=1,2,3 \qquad p_i \in F_4 \;\; i=1,2$$

$$C = \{ \underline{c} \in F_4^5 : \underbrace{H \underline{c}^T = \underline{0}}_{\text{over } F_4} \}$$

$$[v_1 \; v_2 \; v_3 \; v_4 \; v_5]$$

$$v_i \in F_4$$

rank(H) = dim of row space of H = 2

nullspace of H has dimension $= 5-2 = 3$

So, now let us look at this parity check matrix a little bit more closely, and try and do something with it. So, just to learn what is this? What is the alpha exactly? What is 1 exactly that is the question you have to ask. So, does not matter what the alpha is right. So, it is just obey certain rules for multiplication and addition.

Yeah. So, that is the question that most people have when they learn abstract algebra for the first time what is alpha. So, you should find out first what is what does what mean the otherwise you cannot answer ask that question, it is a difficult question to answer what does 1 mean. So, you are usually use to counting an. So, you say 1 is 1 know, but what does 1 right it is not the only way you define 1 is when it adds to itself it gives you two, but what is 2 . So, it is not… So, at the end of the day even then familiar numbers that you know are abstract you just that this a familiar (( )) learned from whatever preschool or second standard or something.

So, you do not question it too much. So, these are also like that you should not ask what the alpha is, it is not a question that is relevant, right. So, when the Greek alphabet alpha is the beginning the first, let that is the way to think about it. So, let us say it is let us look at this… So, suppose I talked about a parity check matrix, and like I said I haven't strictly define codes over a finite feel an arbitrary finite feel, I am going to do that real quick, but with this example first and then will formularize. So, it is a bit easier to see that way. So, so suppose I want to think of a code word define by this parity check matrix what am I actually saying, the code is basically what set of code words in what in a vector space, what does it vector space now? It is not F 2 n it is F 4 5. So, what does F 4 5? the 5 dimensional vector space with co affiance from F 4.

So, you have to think of this as things of this form v 1 v 2 v 3 v 4 v 5, each v i belongs to what? F 4. So, how many vectors are there in F 4 5 in 4 to the 5, how many vectors will that be 4 power 5, and what does that 10 24 1 0 2 4 2 power 10 count that. So, it is a very finite vector space all right, such that what h times c n g minus C transpose is 0. So, this definition carries over for the parity check matrix, I do not have to worry about anything here right, but except now what are the operation in h times c transpose over f 4 it is not modular four. So, lot of people after a course in finite feels always say F 4 is 0 1 2 3 mod 4 it is not true, totally not true that is not a feel, it does not work at all F 4 is a completely different thing 0 1 some god knows what alpha and then alpha squared also. So, and then alpha path 3 is 1 and I have first code is 1 plus alpha. So, those are the abstract rules, it you have to follow and you deal with this numbers.

So, those rules are basically the feel F 4 basically defines those rules remains as a h times C transpose previously I could just say modular 2, and your happy about that because everything was binary now everything is in F 4. And the only thing I can say is operations over F 4, I cannot say modular or anything it is not modular anything. So, it is operations over F 4. Now, F 4 is a proper field, F 4 to the 5 is a proper vector space. So, all the results you had from rank and Gaussian elimination carry over to that also in that in the linearly zebra setting everything works. So, feel it is a vector space.

So, there is no problem. So, for instance rank of H is 2, which means if you want the fine set of all C you will have 3 free variables and 2 dependent variables. So, this null space of h this defines the null space of H, null space of H will have dimension the row space of h has dimension 2 which means the null space of h will have dimension 3. So, that result carries over without any problem. So, you notice rank of H equals dimension of what row space of h equals 2, I mean you can prove this by doing Gaussian elimination.

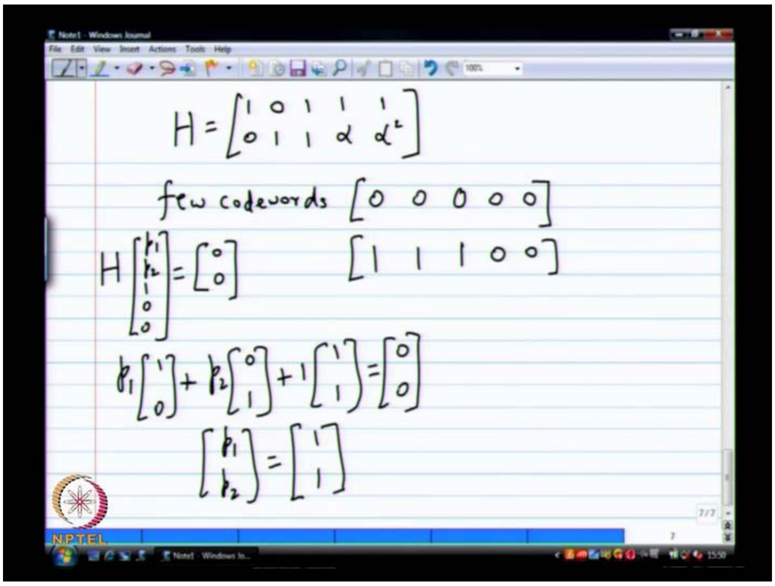
And here in this case Gaussian elimination is already done you already have thus 0 1 1 0, and there is no problem you can immediately write 2. What is the dimension dimension of the column space of H, is it equal to rank of H, yes it is equal to rank of H that result is also true this nothing wrong were that all the results did you knew from linear algebra carry over without any change in this setting, even though you do not know what alpha is. So, remember the proves there you might have learned a very with very much very being very conscious of the real field all the time, but you can do linear algebra without reference to nothing about the real numbers. You would not have used anything about the real numbers except that it is a feel then you can do division, and addition, etcetera. I mean I do not know depending on how it is start I think the way it is thought in map methods you do some abstract stuff also. So, you know you know how it works. So, column space also as a same dimension. So, if you want to look at the null space of H remember, C is the null space oh H right, this will have dimension what it will be number of columns minus rank of H. So, it will be 5 minus 2, which is 3. All these results carry over to arbitrary abstract vector spaces over abstract vector feels abstract finite feels, there is no problem, there is it just works without any worries.

So, that is the advantage of learning abstract I mean you are asking me what does the alpha, I do not know what does the alpha if you learn it no how many (( )) abstract everything out the same thing applies to anything with satisfies those minimal axioms. What are the minimal axioms that I needed. So, and you have that power with you when you know it in abstract when you do not know it an abstract you are not sure it is works for real numbers does it works for this does it work for that you are always confused, and you learn it purely in abstract that is the advantage. So, this is true. So, basically what does it mean once I say null space of H s dimension 3, when I try to solve h c transpose 0 I will get 3 free variables, and 2 dependent variables, and the way I have written it down here you can associate the free, free variables to the message part. And then dependent variables to the parity part, which is what we did in the binary case, right.

So, now m 1 m 2 m 3 belong to what field, each m i what does m i? m i belongs to m i just 1 there is say m 1 it belongs to F 4 F 4 nobody is really scared now to say anything. So, p I also belongs to F 4. So, now, I cannot say bits any more the m 1 is not a bit m 1 is actually what yeah, you can call it as symbol are an element of F 4. So, it is common in communications pralines to call it a symbol for intense, it is couple of bits right. Is it 2 bits can I say m I is 2 bits yeah, I mean it is 2 bits you can represented with 2 bits, 2 bits. So, but it is a little bit more, because I know it is element of F 4.

So, you can multiply things, so it is a bit different, so what we going to do next is it is only like 3 minutes left. So, I am going to ask you to write down some code words of this code. It is good practice, there is not too difficult, but think it little, tell you something about the arithmetic involved and how to quickly come up with it. You will actually believe that there are code words any one though looks like null space of H, we should write down some code words.

(Refer Slide Time: 47:35)



$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 \end{bmatrix}$$

few codewords $\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \end{bmatrix}$

$$H \begin{bmatrix} p_1 \\ p_2 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$p_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + p_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} + 1 \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

So, let us write down some code words, so once again let me produce the h, so few code words, so it is easy to write down a message bits first and then ask you for the code word. The first code what is the easiest code word is let us say 1, 0, 0 if my message is 1, 0, 0 or may be 0, 0, 0, my message is 0, 0, 0, let us start with much more basic question message is 0, 0, 0.

What is the code word 0, 0 right some areas pug it in here and multiply it out you can do it in your head, so will do it slightly more complicated examples. So, which one 0, 0 what happens 0, 1, 1, 1, 1 you agree or not yes remember. When I put 1, 0, 0 what am I expecting, I want a fine p 0 and p 2 such that h times p 1 p 2 1, 0, 0 equals what 0, 0 let me do this multiplication. When I do this multiplication what happens p 1 times 1 0 plus p two times 0 1 plus 1 times 1, 1 plus 0, 0 and all that this is equals 0, 0.

So, this is the same thing is what we saw before, so from here you will see in the next step you can do this p 1, p 2 equals what 1 1 is it minus 1 minus 1 or 1 1, why is it same an F 4 no were not an F 2. It is characteristic you still 2, so that is the technical way of answering the question you can say F 4 has characteristic 2 which means minus 1 is 1 it is the way to think about this 2 is equal to 0 an F 4.

That is the way it works, so p 1, p 2 is 1, 1, so you can do this computation in your head with matrices, so of a binary you might have done it very quick, but in F 4 it will take a little bit more practice to get used to it. Remember, this is just I am multiplying I with p 1 p 2, so essentially what I will have is p 1, p 2 to be equal to be equal to this part 1, 1, 1 alpha 1 alpha squared times what m 1, m 1, m 2, m 3.

So, the moment I give you m ,1 m 2, m 3 all you have to do is scale them, scale this is 3 rows this columns with m 1, m 2, m 3 and then add it up that is the only operation you have to do. That will be equal to p 1, p 2 and you can simply put that down here for bits, it is might be very easy simply you have to simply multiply an x or x all nothing more F 4. It will be little bit more complicated, but you do it, so times up, now we will pick up from here in the next lecture.