

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

Lecture - 11
Codes Over Finite Fields, Minimal Polynomials

So, let us continue with this same things. So, what we are doing is looking at this parity check matrix over F_4 and trying to find some code words, just to get use to the arithmetic, also getting used to the idea of codes over F_4 non binary codes.

(Refer Slide Time: 00:18)

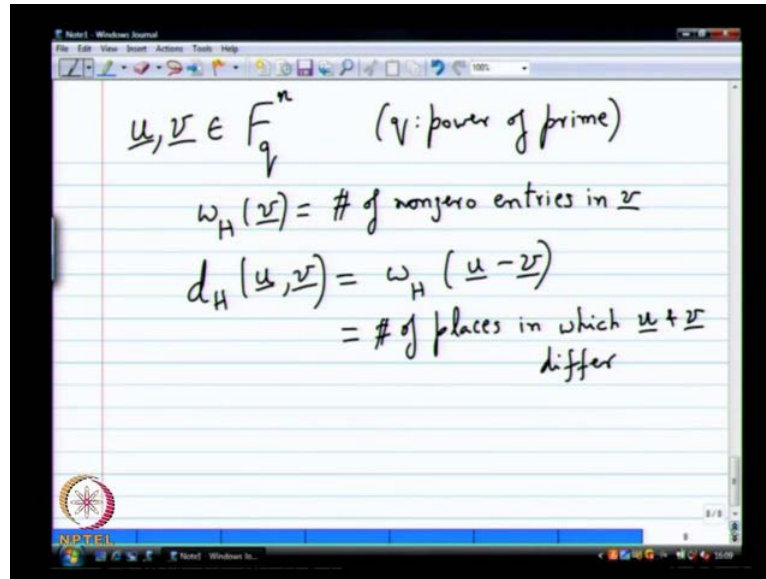
The image shows handwritten mathematical work on a digital whiteboard. The work includes the following:

- A parity check matrix $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 \end{bmatrix}$ and a message vector $\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix}$.
- The text "few code words" followed by the vector $[0 \ 0 \ 0 \ 0 \ 0]$.
- The equation $H \begin{bmatrix} k_1 \\ k_2 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ with the augmented matrix $\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & 0 & 0 \end{bmatrix}$.
- The row reduction step: $k_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + k_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} + 1 \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.
- The resulting vector $\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.
- Augmented matrices for row reduction: $\begin{bmatrix} 1 & \alpha & 0 & 1 & 0 \\ 1 & \alpha^2 & 0 & 0 & 1 \\ 1 & \alpha & \alpha & \alpha & 1 \end{bmatrix}$.

So, let us say I put my message bits as say 0 1 0, if I do 0 1 0 particularly easy. So, I have made two other multiplying factors as 0. So, m_1 simply m_2 simply picks up the second column, which is one and α . So, p_1 and p_2 become to 1 and α . So, that is another code word in this code. So, another one I might want to pick say 0 0 1. If that you would get $1 \alpha^2$, let us say something little bit non trivial.

Let us say $\alpha^2 = \alpha + 1$, so all that is fine. So, couple of definition, which I have to extend are hamming weight and hamming distance. So, remember hamming weight and hamming distance for binary, what is the definition? Hamming weight is the number of one's for non binary for F_4 . All hamming weight will become number of non zero entries. That is the first extension let us do that real quick next page and then come back here. So, if you have a vector V belonging to F_4^n .

(Refer Slide Time: 02:02)



The image shows a digital notepad with handwritten mathematical definitions. The text is as follows:

$$\underline{u}, \underline{v} \in \mathbb{F}_q^n \quad (q: \text{power of prime})$$
$$\omega_H(\underline{v}) = \# \text{ of nonzero entries in } \underline{v}$$
$$d_H(\underline{u}, \underline{v}) = \omega_H(\underline{u} - \underline{v})$$
$$= \# \text{ of places in which } \underline{u} \text{ and } \underline{v} \text{ differ}$$

The notepad also features an NPTEL logo in the bottom left corner.

So, \mathbb{F}_q is some power of prime prime power as we call it the hamming weigh of V is defined as number of nonzero entries in V . I am sure its a very more precise way of wrighting is its clear way of wrighting, but I guess its clear. So, when ever for binary you count the number of one's and non binary you count the number of non zero entries. So, if u have a let us say u and V there two vectors in \mathbb{F}_q^n the hamming distance between u and v is defined as the hamming weight of u minus v .

I have just say minus us here because thinking of the general field in what case will minus will be same as plus? 2 I mean q is right when you have even number outer the prime has to be definitely to that case minus 10 become plus, other wise I have to say u minus v . So, basically if you want this worlds the number of places in which u and v differ that remains the same, it is the same as the binary case. So, the formal extinction of hamming weight and hamming distance from binary to arbitrary fine at x fields. So, let us go back to the examples and train and the questions of hamming weight and many the distance between two vectors.

(Refer Slide Time: 03:55)

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 \end{bmatrix} \quad \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix}$$

few codewords $[0 \ 0 \ 0 \ 0 \ 0] \rightarrow 0$

$$H \begin{bmatrix} k_1 \\ k_2 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad [1 \ 1 \ 1 \ 0 \ 0] \rightarrow 3$$

$$k_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + k_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} + 1 \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

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

Arrows indicate Hamming weights: 3 for the first row, 3 for the second row, and 5 for the third row.

The hamming weight here is zero, what is the hamming weight of this? 3, so is the hamming weight here. So, is the hamming weight here, what is the hamming weight of this? 5 What about distance between this two? 3. So, distance between this two 3, so you can an find, so simple enough definition, so it works. So, I can give you other example, but I think we think that should be enough, that one example will give you an idea of how this code work.

(Refer Slide Time: 04:55)

$$\underline{u}, \underline{v} \in F_q^n \quad (q: \text{power of prime})$$

$$w_H(\underline{v}) = \# \text{ of nonzero entries in } \underline{v}$$

$$d_H(\underline{u}, \underline{v}) = w_H(\underline{u} - \underline{v})$$

$$= \# \text{ of places in which } \underline{u} + \underline{v} \text{ differ}$$

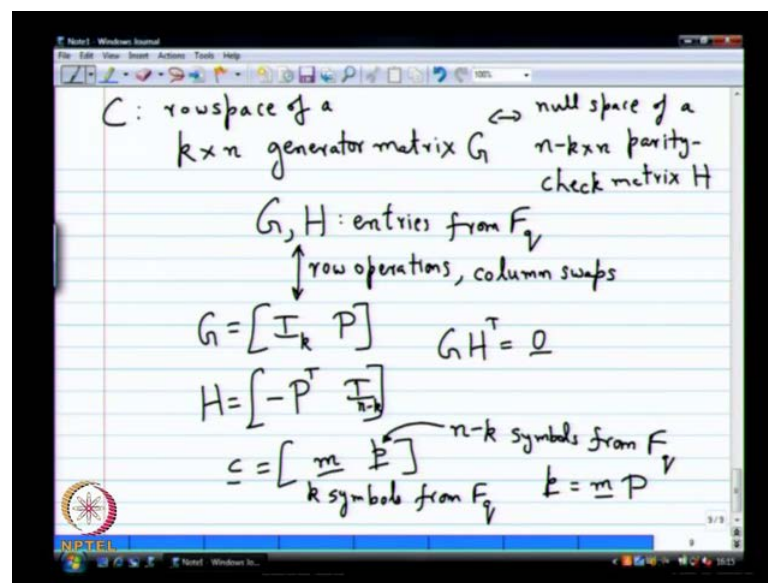
$$C : (n, k, d) \text{ code over } F_q$$

$$\uparrow$$

$$k\text{-dim subspace of } F_q^n$$

So, if we have an $n \times k$ code C , so let me just give definition of codes. Somebody tells you C is an $n \times k$ code over F_q . So, we had this before for the binary case. You had an $n \times k$ code over F_2 and binary code of length n , what does this actually mean? This will be a k dimensional subspace of F_q^n remember q has to be a prime power. It is not a prime power there is no such field and it does not make any sense, since it has to be prime power its subspace of F_q^n . How is this subspace specified using our idea of two different matrices. You will have a generator matrix G and C will also be the row space of G . $k \times n$ generator matrix of G .

(Refer Slide Time: 05:58)



It will also be the null space of a $(n - k) \times n$ parity check matrix H , but know this G and H will have entries for what from F_q . That is the other these will be matrices the elements from F_q , but I should remained you once again the Gaussian elimination of the operation works eminently over any abstract vectors space, defined over any abstract field. Once you have the operations for the field you can do Gaussian elimination on G . Remember, we allow for column swaps when we do some Gaussian elimination. Because, we considered that as an equality and operation was coding as concern, does not change the distance, does not change the weight, does not change anything else only change the order.

So, what you can do is we can start with G and H and do row operations. Basically, the Gaussian elimination operations and column swaps and end up with what is

known as the systematic version. So, that G becomes I P and H in this case go back and check this will become minus p transpose I. In the general case if I know minus 1 is not plus 1. If p could be odd that case it becomes minus be transpose high. If you go back and check the way I derived it the minus will come. I would also followed that under that plus, because that binary the characters is not to you have the carry over the minas. You cannot kill that, it will be the minus P transpolar U can check very quick. This I will be I K this will be I n minus K a.

You can check very quick the g h transpose will be equal to a 0 matrix k k by n minus k 0 matrix. So, you can do all the previous thinks that way, so no problems. So, you can think of the code word C as consisting of a massage part, which is k bits k symbols k elements I should not say k bits, k symbols from if q. Then a parity part p, which contains.

Now, n minus k symbols from f q. Then a parity part p, which contains now n minus k symbols from q, this ms is my C variable to pick, I can m as anything. I want than I can use ether the generated matrix G parity check matrix h and construct the parity as m times speak. So, I will get the parities very easily so this sorry m times capital p should be caps small p equals m times capital. So, let us then I got this theory extinct without any problem. So, the last, so n and k are easy once again. So, d is the next defination d is the minimum distance the similar definition from before goes through without any problem.

(Refer Slide Time: 10:07)

$$d = \min_{\substack{u, v \in C \\ u \neq v}} d_H(u, v) = \min_{\substack{u \in C \\ u \neq 0}} w_H(u - v)$$

$$= \min_{\substack{u \in C \\ u \neq 0}} w_H(u)$$

$$= \text{minimum number of linearly dependent columns of } H.$$

$$u \in C \wedge w_H(u) = w \iff \exists w \text{ cols of } H \text{ that are linearly dep.}$$

$$H u^T = 0$$

So, can do it this way minimum for u, v belonging to the code u is not equal to v hamming distance between u and v , but since we know this linear code. This becomes equivalent to doing minimum u and c u not equal to zero the hamming weight of this becomes the same just by the same proffer. So, this this is the same as hamming weight the u minus v and u minus v also belongs to c . So, linear sub space, so minus v u minus v all this things belongs to the same c . Based on that you can write that very easily formula for d .

So, in particular what happens is the relationship we had between the hamming the minimum distance and the columns of the parity check matrix. How they are linearly dependent that carries over without any problems. Except that you cannot say some 2×0 you have to say linearly dependent. Because, some 0 worked in the binary case will not work for the general case. So, that is that is crucial d also happen to be minimum number of linearly dependent columns of h . Once again this is a very hard to quantitative to compute, like I said it is one of those empty compute things.

I cannot hope for algorithm to quickly compute this things, which the difficult combinatorial problem to solve. So, the minimum number of linearly dependent columns of h . So, how did we prove it the key element in proving it is if u is u belonging to c and hamming weight of u is w . Then what does it mean there exists w columns of h . That are in any dependent how did I show this, is very easy to show this. All you need is h transpose to 0 how do you show this, h transpose 0 , there are only w non zero entries in u . So, clearly fix out only w columns from h those w columns are linearly dependent.

So, that is the idea and this is also if and only, because if u have w column became linearly dependent, then what you do you manufacture a u . So, h times you transfer a zero. So, scale w columns suitably make them zero put the other things is 0 you get the same answer, so it goes both ways. So, this is crucial in this proof, so that kinds of rounds out everything I want to say about the codes over the finite fields a hopefully. Its clear, I do not want do any more examples and this one, may be we will do this one more example. Then after that will call it quits. Let us do a slightly more complicated example may be just hunt for a sample, which is little bit not trivial for non trivial.

(Refer Slide Time: 13 38)

$\text{Ex: } F_8 = \{0, 1, \alpha, \alpha^2, \alpha^3 = 1 + \alpha, \alpha^4 = \alpha + \alpha^2, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = 1 + \alpha^2, \alpha^7 = 1\}$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} \end{bmatrix} \leftrightarrow \begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & & & \dots \\ & & & & & & & 1 \end{bmatrix}$$

$n = 6$
 $n - k = 3 \Rightarrow k = 3$

$$[H]_{ij} = \alpha^{i(j-1)}$$

$j, i = 1, 2, 3$

So, for that lets go to F 8 remember the F 8 table work like this alpha square alpha power 3, which is 1 plus elfin alpha 4 equaled alpha plus alpha square alpha 5, which is alpha square plus alpha plus 1 and alpha 6 equal to 1 plus alpha square and alpha 7 equaled to 1. This kind of tells you the F 8. So, let us construct the parity check matrix. Will give silly more pain full I should give u i will put alpha 5 to make, it more interesting. Let us do that taking a terrible amount of time to write this I am sorry for that. Next, I do not make mistakes alpha 6 of alpha 9 alpha 12 alpha 15.

So, of course you can arrive I do not want, alpha power 8 alpha power 10 and all like what is alpha power eight suchlike alpha power 10 all layer 3 altheas thinks. You can write it as alpha power what let me see who gives me. So, i equals 1 2 3 i j 1 2 3 write it as j into or j into minus 1 it's you can put mod 7. So, hear you can put mod 7 if you like, so it is does not matter, so this is the form. So, let us tried the find out parameter for this code. So, agreed the parity check matrix you have to find n k, n d, so n is the easiest.

So, n is essayist basically primary school problem how can u count case this count that 6 k is at list high school problem not a so much primary school. You have to do goes in elimination what is k, what is n minus k u have to do goes in elimination u can be sour. So, the first three columns are in I know had up first three columns are linearly independent u can do with that. Then you will show I can be formed I can solved its good exercise to try that large you to some time and go back home and try that. So, we

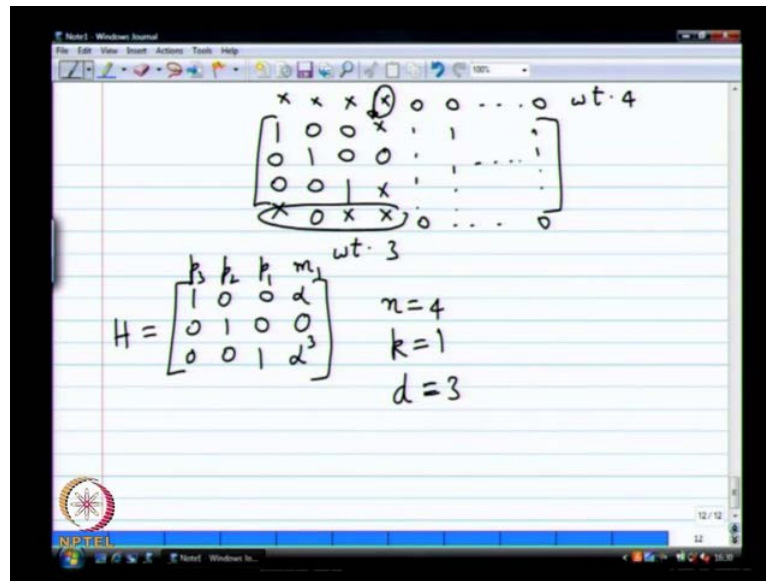
can do the combination of first operation are you do will be, what second row equals the second row minus. The first row minus is the same as the plus is remember F_8 . So, you can do second row equals second row plus first row.

So, you get a zero and then you get the other elements likewise you do third row equals third row plus first row. You will get 0 0 and all these are the elements and then you come back here. Then you divide by whatever you had that to make that one subtract just to same standard Gaussian elimination. Except that your operations are with this field the field that I have written down here is not with anything else. So, will get n minus k to be 3 and this will implies k is 3. Of course, the interesting question is what is interesting question minimum distance. So, that's the most interesting question first tell me about an upper bound. What is the maximum minimum distance that you can have single tonned bounds is something you can use the other bounds, are little bit more difficult.

So, the same cases single tonned bound, you can use what is single tonned bound tell you d is less than or equal to 4. I never showed that this single tonned bound also holds for F_q you can go back. You can do the same proof that I did before the exact same proof that pigeon holding type of argument with k minus 1 carry over, you will get n minus k plus 1. So, 4 is the distance that is possible with this you cannot have anything more than 4. I can easily find a code word of weight 4. You do the Gaussian elimination you can find the code word of weight 4 yes or not? Remember, if you do Gaussian elimination what happens think about this, this is fairly important. Because, you are going to get $i \geq 3$, then you will get several rows may be some row here, I do not know what this is some $h \geq 4$.

So, on you will get now this is a message bit message symbol, which I can pick to be anything non zero and then I pick everything else as 0 then what is the maximum weight that I can possibly have this 1 plus this 3. So, 4 I can easily find 4. Now, after you have reduced it to $i \geq 3$ you can look at each column. There are four entries in three entries in each column and any column has a 0 entry. What does it mean is 0 entry one of the entries in some column is a 0. Then can I have a weight three code word they are able to not able to. So, let us do let us let us see an example it is every certain things, but it is important to know what is happening. Remember, you can do Gaussian elimination and get 1 0 0 and 0 0 1.

(Refer Slide Time: 21:49)



Then I have some additional columns here, which I would have got after the Gaussian elimination. I do not know what it is, but if all three of them are non zero. Then if I put some non zero entry here, i will have a weight four code word. Remember, I have several other columns also if I put zero's all here and I put some non zero entry here something non zero here. Then I will and if all these three are non zero, I will definitely get a non zero entry here. So, I will get a weight four code word if it turns out that this column already had a zero, after I did the Gaussian elimination, what will happen? Clearly, this one will not appear at all. So, the even these three guys are linearly dependent.

So, I put something non zero here put all zeros here this guy will not play a role this will continued to be zero. So, I get a weight three code word this is weight four, this is kind of roughly clear, may be not clear. Let us see a more concrete example if I have a parity check matrix like this it is say alpha, alpha square alpha power 3. So, this is suppose may parity check matrix, let us do n k n k d for this. It is a very easy matrix to do n k d let us say n is 4 k is, what k is and what is d? See, remember this is a parity check matrix what is my message bit message symbol, there is only one message symbol. Then I have three things yes or no? Three parities symbols if I put anything non zero. If I put m equals zero what do I get, M 1 equals 0 will give me the all zero code word.

If I put m 1 as anything non zero what will I get for p 1 p 2 p 3 can I get anyone of them to be 0 or it is m. It is alpha times m 1 alpha squared time m 1 alpha per three times m 0.

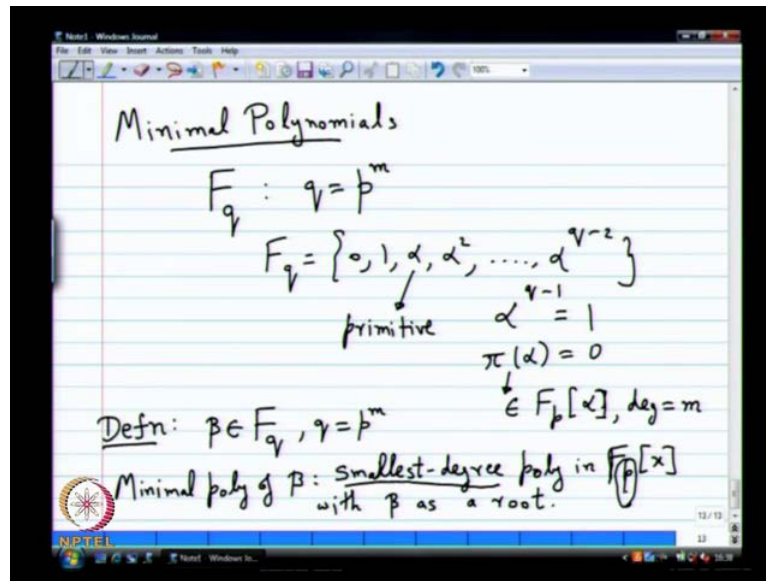
Clearly, if $m-1$ is non zero none of these three guys can be 0. So, from their you see immediately d is 4 do you understand? It is very simple to see that, now in case instead of this α squared. Suppose, I had 0, so you would get d equals 3 did you see that? So, the same point I am making here in the more general case. Even when you have other columns other more messages, because it does not matter. You can make all of them as 0 even if you have one column. Then it becomes there is that, that is an interesting way of finding out minimum distance, which might help you sometimes in the future.

So, you might want to apply something like that here, but still a little bit more confusing you have to check very carefully. You do not know whether it works or not. So, you have to check all possible combinations here to find out the minimum distance. Or you have to be very smart, you should know some the fancy methods to find the minimum distance. In fact you can show I believe that this minimum distance here will be equal to 4 this parity check matrix. It is non trivial anyway you can show that parity check matrix the distance will be 4. You can basically show any three columns that you pick from this parity check matrix. They will be linearly independent you can show that this very standard construction to construct like this.

You can show that this we will equals 4 that is that is the idea here anyways. That is the only other example I wanted to do I know. I did not do complete job of doing with these example, but hopefully this gives you enough idea of kind of things that i involved here. Its not very case even for finding case 5 equals 3. You have to do some work, its not as trivial as binary to do some Gaussian elimination carefully, otherwise can happen, but go home. Try this do the Gaussian elimination and check that every column has completely non zero entries see that will happen.

Then you then you have to do more work that is not enough to show minimum distances 4. You have to say that those three will not give zero to do a lot of careful work. Then you can show that the equals 4 will work or not, but is lot more work. We will do one more one more notion with finite fields. Then we will move on to this BCH code construction is quite simple its very similar to the previous construction, which I had. So, nice nice construction that gives you the minimum distance, but before that we need just one more idea from these finite fields that is the notion of this minimal polynomial.

(Refer Slide Time: 27:59)



So, once we have this notion we are ready to jump into the BCH code construction. So, what let us say we have F_q , which is q is a prime power. Let me say q equals p power m . So, just hold some prime p and q is a finite field, it is been given to you previous question. Go ahead if the entire column is non zero you can say that there is 4, but if there is zero. There might be some other message word, which might will correspond to i have a codeword with minimum distances, for what for this specific case this to be, but in the general case its less than or equal to three. That is the conclusion that is theoretically valid.

You might there might be something else here, which is identical linearly dependent on every check linearly depend linearly dependent. There is a little bit more confusing to check in an arbitrary field right binary. It is very easy to check whether it is identical the other fields. You have to multiply by all powers of α little bit confusing too many possibilities are there. I cannot immediately verify yeah d less than or equal to 3 is the only conclusion. So, forget about that example and now the example is causing some entry may be again forget about it, let's move on. Let us look at minimal polynomials, then we will come back to very similar construction, while we do BCH. That time I will prove to you that the minimum distance cannot be three those kind of checks we will do.

So, F_q is the is the field hence let us say we have written F_q as usual, we have a primitive element. So, we do zero one α α^2 α to the power q minus 2

$\alpha^2 - 1 = 1$. Then $\alpha^0 = 1$ is a polynomial of degree m with coefficient in F . So, this belongs to F if α has degree m . This is the general way of describing q . Such an α is called a primitive element. I do not have a defined formulae or not such an α is called primitive element, it is the root of a primitive polynomial. So, it is all words primitive will show up again these expressions let's say. Now, the definition for minimal polynomial. So, let me give you the definition then I will justify the definition.

So, suppose I have a β belonging to F if q is p^m . So, minimal polynomial of β is the smallest degree polynomial in $F[x]$. So, that is the main difference with β as a root. So, the crucial two things here are p , this p is very crucial. Then the smallest degree is very crucial. These are the two things are important and this definition first of all this definition have to make sense.

I will tell you why this makes sense soon enough, but before that let me ask you another question instead of p . If I had q here what will be the answer β is a polynomial β is a root β . Do you think β is a polynomial is β root of β , it is not. So, what is the smallest degree polynomial, which has β as a root $x - \beta$ correct answer, why everybody is afraid? Constant non zero polynomial has a root right.

So, obviously it is nothing not vanished for anything you put nothing there is plan to put it zero, but allow the zero polynomial. So, if you want if you put q instead of p answer is trivial. You have a degree one answer, which is $x - \beta$, but you do not want coefficient from F if you want coefficient only from F . So, that is the added thing here, which makes definition more interesting.

So, if you had q itself then $x - \beta$ would be the answer. No other problem β itself belong to F if I just have it, but I do not have q here I have p , which is coefficient from F is only allowed. So, if you go back to F_8 for instance I have $0, 1, \alpha, \alpha^2$ and all that. I want a polynomial for which α is a root, but the polynomial should have only binary coefficient cannot have non binary coefficient. So, for F_8 do you know polynomial for which α is a root for binary polynomial, for which α is a root. Let us look at this little bit more closely.

(Refer Slide Time: 35:11)

$\underline{\text{Ex:}}$ $F_8 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$
 $\pi(\alpha) = \alpha^3 + \alpha + 1 = 0$
 $f(x) = x^3 + x + 1 : f(\alpha) = 0 \text{ in } F_8$
 $g(x) = x^3 + x^2 + 1 : g(\alpha^3) = 0 \text{ in } F_8$
 $g(\alpha^3) = \alpha^9 + \alpha^6 + 1 = 0 \checkmark$
Min. poly. of 0 : x
1 : $x + 1$

Let's look at the example I had F_8 , which is $0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$. What this do you know polynomial, which a α primitive polynomial, itself is the answer. So, remember α^3 if you look at the definition of this, field π of α was simply equal to $\alpha^3 + \alpha + 1$ and this was equal to 0. So, one polynomial for which α is a root is $x^3 + x + 1$ has α as root say f of x equals such that f of α equals 0, this is in F_8 that is that.

So, go back and look at the definition once again I said the polynomial is in $F_p[x]$. It has β as a root and β as an F_q , which is a larger field, which contains F_p inside it as a proper subfield. I gave you an argument in the beginning of in the middle of last lecture about how, that is how inside F_{p^n} . There is an F_p sitting inside, which is isomorphic. So, this operation make sense it makes sense the β to be a root of f this polynomial, which has coefficient of p . See, you can do the computation in the larger field F_q , you understand what I am saying it make sense to all.

So, for instance if I have polynomial with rational coefficients. I can think of a complex root for the polynomial but, you cannot say my polynomial has rational coefficients. How will I again an complex number you can say it, but how do you do that? The complexes contain the rationals as a proper subfield. So, you simply do your operations in the complex fields do you treat each number. Each rational number as a complex

number with zero imaginary part and the real part that is the rational number itself. You do your operation the same thing, you do here when I have polynomial with coefficients from F_p . When I plug in x equal to some element of q what will it treat the coefficient has not just belonging to F_p , but belonging to that F_p , which is inside F_q , I know there is F_p inside F_q .

So, I imagine what it is very similar to plugging in a complex value into a polynomial with rational coefficient its actually a same way you tell. So, that is what happening here also yes no may be. So, let us try something here just for fun if you look at this other polynomial g of x equals $x^3 + x^2 + 1$. I want you to check this one not F_g . This will sure work out with zero a in F_8 to do the computation let us try to do it we are plugging g of α^3 .

What am I doing in the binary field little bit misleading. Because, coefficient either 1 or 0 do not have to read the coefficient or anything at all just plug it, in you will get away with it put x equals α^3 . You get what $\alpha^9 + \alpha^6 + 1$ plus that workout to 0, everybody agrees. If you are you can go back and look at the list that you had, so it works out that is.

So, it looks like every every element has has at least one polynomial for which it is a route that I know that seems like it is okay. So, let us let us go back and look at this definition once again, but before that is everybody with this did you check it, let me ask one more question. So, for instance the elements with the α in it are little bit more complicated. If you look at this one for just instance or 0 what about 0?

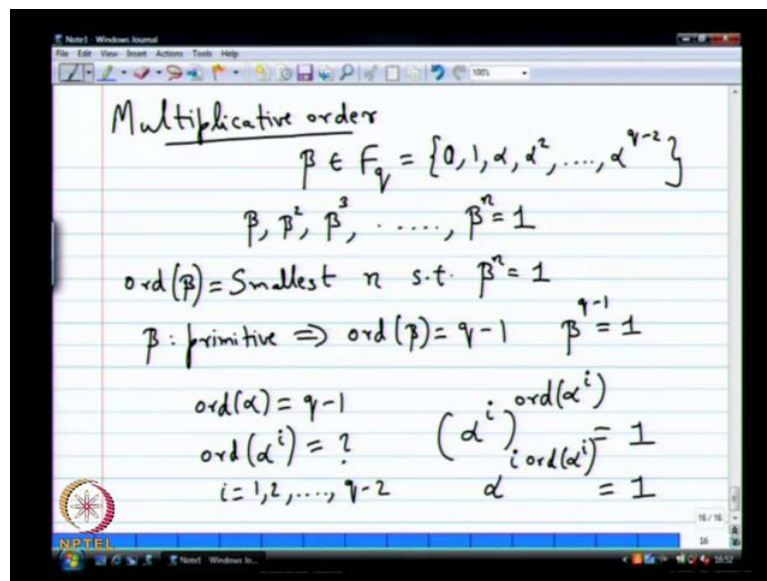
What would be the minimal polynomial of 0 x do not say 0. People say 0 0 is not allowed as a polynomial. We look at only non zero polynomials when we define minimal polynomial x , it is very easy. I do not have to even prove it you know it clearly has to be x . If you find a linear polynomial. Then that has to be a minimal polynomial, there is no problem what about $1 - x$ or $x + 1$ for the other elements you have to do some more work, it is not. So, not difficult, so easy all right.

So, that is one thing, but the other thing I want to quickly point out here before we may be I point it out later. Let us go back to this definition then make sure that this definition make sense. What are the various things that I needed to make sure definition make

sense. What do you mean by making sense I am saying minimal polynomial is a smallest degree polynomial in $F[x]$ with β as a root.

So, first thing I should show is show is that there are some polynomials in $F[x]$, which will have β as a root. If there are no polynomials then this is it does not make any sense. I have to show that first before I even define this cannot say smallest. When I do not even know that there is at least one polynomial, which will have β as a root. Now, I will show you a polynomial, which will have all the elements of finite fields as its roots that is a polynomial. It is a very simple polynomial, which belongs to $F[x]$. It will have all the elements as its roots. This is how we go about doing it and for that you need some notion of an order. So, we going to quickly define it and let us see how it works. So, order of an element multiplicative order.

(Refer Slide Time: 42:34)



So, we will only talk about multiplicative order wait I will write the order is wait we will see. So, if you have β belonging to F_q and you look at this sequence $\beta, \beta^2, \beta^3, \dots$ can this go on forever. Because, I have finite number of elements in my field and every power of β will definitely belong to the field. So, it has to repeat somewhere. So, there will be a smallest n such that $\beta^n = 1$. It will have to repeat at one it cannot repeat some other power of β . Then you can show easily that it has to be have a smaller number, which has 1. So, it will repeat at one, so that is defined the smallest such n is defined as the order of β .

So, smallest n such that it is called order of β such that $\beta^n = 1$ is it fine. So, I will say simply order when I say order its multiplicative order additive order does not this means very easy why is additive order is very easy keep adding β , which itself $\beta + \beta$, $\beta + \beta$. When will I get 0 3 times β 3 time β is definitely one, but may not be the order. May be there will be something smaller give you 0 can I give 0. Anyway if you convince that is good the additive order is not. So, interesting only the multiplicative order is very interesting. So, order of β is smallest n such that $\beta^n = 1$. If β is primitive what is the order. So, let us say F_q is this F_q is some. So, if β is primitive implies what β generates the entire field before it is comes back to 1 k .

So, order of β becomes equal to $q - 1$. So, $\beta^{q-1} = 1$. Now, this tells you some every easy things about multiplicative order of elements in finite fields. So, if I have F_q to be $0, 1, \alpha, \alpha^2, \dots, \alpha^{q-1}$ so on till α^{q-1} I know the order of α is $q - 1$, so this is easy. So, order of α $q - 1$ and any other β in F_q is of the form α^i , it is not of any other form. So, all you have find is order of α^i for $i = 1, 2, \dots, q - 2$. This is what you we have to find and what can you show ah this will be k . Some kind of G C B A to come in. So, is very easy to see why this has to work out. Remember, you have α^i α^i raise to the power of order of α^i is what equal to 1 k .

So, basically you get α^i times order of α^i should be equal to is equal to 1 am I right? So, if you looking for the smallest such element some kind of G C B has to involved. I can prove this to you quite regress if you like it will end p being $q - 1$ divided by G C D of i, n, q , something like that k . So, I do not know how much detail want to go and do, but you will get some number k , but anyway mean I do not know.

If I really need to go and end to the order and anything like that. Basically, I do not even need that I just want to show you a pronominal, which will have a all the element is its roots. Clearly, that is every easy I do not even need to do this k . So, α^i all this say I do not need. Basically, any element α^i raise to the power $q - 1$ become what is basically α^i raise to the power i α^i $q - 1$ is 1.

(Refer Slide Time: 47:44)

$$(\alpha^i)^{q-1} = (\alpha^{q-1})^i = 1$$

$$f(x) = (x^{q-1} - 1)x = x^q - x \in \mathbb{F}_p[x]$$

$$\forall i \quad f(\alpha^i) = 0$$

$$i = 1, 2, \dots, q-1$$

$$f(0) = 0$$

→ Definition makes sense

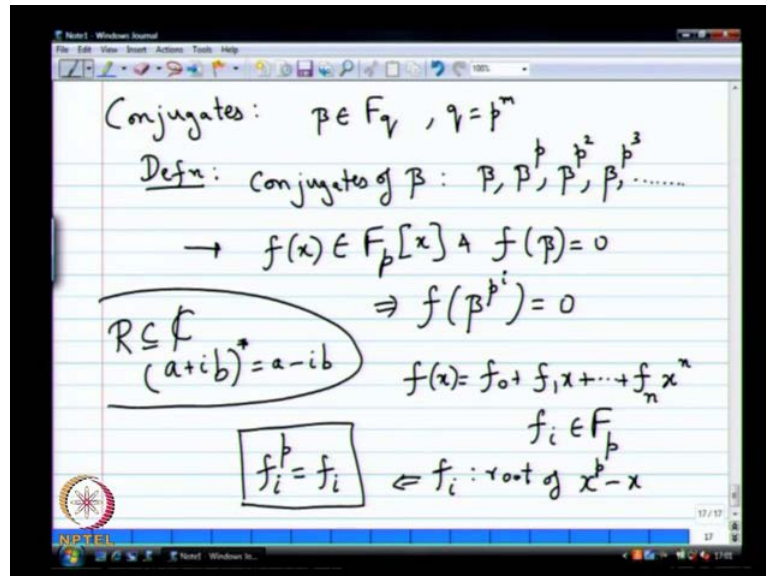
So, you simply get 1 k do not think I even need the order. I do not know why we thought about the order k this is good enough. So, alpha power q minus 1 rise to the power i is 1. So, look at the polynomial x power q minus 1 minus 1. Let us look at the polynomial f of x equals x power q minus 1 minus 1. You can easily show for all i equals what one two soon tell q minus 2. In fact even q minus one why not k f of alpha power i is equal to 0. I do not even need order I do not know why just simply got diverted in to order. You need basically alpha power q minus 1 is 1 k. So, any alpha power i also when you raise to the power q minus 1, it becomes one that is only thing you need k.

So, f of alpha power i is 1, so you can also make a small change. You can simply multiply this by x to get x power q minus x in which case what will happened, I can start with I can say f of alpha power i is 0 and f of 0 is also 0. Just making f of 0 is also 0, remember this is the polynomial, which polynomial, which belong to F p x for any p. You chose it belongs to F p x k, what did I wanted to show is caught, it is long lecture can we very tiring k. So, every element in S q i wanted to have some polynomial with coefficient some f p for which it will be a root for that beta will be a root. Now, here is a polynomial x per q minus.

It's definitely has beta has root, but the question is this the smallest degree polynomial or minimal polynomial polynomial with minimal degree q. I can definitely find q is such large number do you really need q or can something smaller work, this is important

question. The definition make sense that is the main point I want you, definition makes sense. Let's try in smallest degree

(Refer Slide Time: 50:48)



For that this notion of conjugates conjugates is which will help us find minimal polynomial k y will give you definition. Then I will give you to an analogy, which will help and understand what happens here is the definition. If you have data belonging to F q common q is equal to p power m. The conjugates of data, basically you can include beta. If you can one not a problem beta power comma beta power p square and so on. You can include beta power p power three so on. So, when I define order also, I had a sequence like this what beta beta square 3 so on. This a totally difference thing beta beta power p what is this beta power p is the characteristics of beta power beta power three beta power p is p.

So, why is this conjugates interesting on it when I look at minimal polynomial polynomial this is the reason. So, if you have f of x belonging to F p x and f of beta equals zero this implies f of beta to the power p power i is also 0. So, if you beta as a root of polynomial with coefficient with F c what else also a 0. That same polynomial all the conjugates of beta beta power p, square square beta power p 3, with all these things are also roots of that same polynomial k. So, that I us the crucial idea that is the reason why conjugates important I will give a analogy, it is very easy analogy.

So, for this real numbers and complex numbers what is the conjugates of i . Both k the real numbers contains complex conjugates are available a minus i be, F i have polynomial with real coefficients and a plus i b this is root. Then what else also a root minus i b also, that is the way the fundamental reason that is fundamental reason to define conjugates. If you have larger case field and a smaller fields inside it you look at conjugate case with a larger field with respect to the smaller field. This is the definition polynomial should also divide this is the idea to keep in mind. So, want to if you want an analogy if you do not want analogy, forget about it come back to this. Let me try and prove this to you, it is not too difficult its quiet easy.

So, one thing we saw, so let us say f of x belongs to f of x f of x is f_0 plus $f_1 x$ plus so on till say some $f_n x$ to the power n some end degree, do not no each of this f_i is belong to F . Remember this F is finite field it also has a primitive element, I did not really prove to this, but I also said at every finite field had you already accepted it. You all accepted, where can use it every finite field has a primitive value F p also has primitive element. So, that primitive element raise to the power p minus one is going to be one. So, that clearly means its i remember F i is f power p go back to the previous polynomial, so which means F i is the root of what x to the power p minus x .

That is what I showed you to you before, if any element the root of F i clearly a root of $x^p - x$. So, this basically implies $f^p = f$ this an important result, which we will use this also a very standard result in numbers theory $a \equiv b \pmod{m}$ equals $a \equiv b \pmod{b}$. Its named after somebody any else who knows the name. So, this what we recovering this even for $s \equiv q$. We know this is true any element of f q raise to the power q gives the same element does.

(Refer Slide Time: 56:17)

The image shows a digital whiteboard with the following handwritten mathematical expressions:

$$(f(x))^p = (f_0 + f_1 x + \dots + f_n x^n)^p$$

$$= f_0^p + f_1^p x^p + \dots + f_n^p (x^p)^n$$

(check this)

$$= f_0 + f_1 x^p + \dots + f_n (x^p)^n$$

$$(f(x))^p = f(x^p)$$

$$f(p) = 0 \Rightarrow f(p^i) = 0$$

$i = 1, 2, \dots$

So, what I am going to do now is take f of x and raise it to the power p . If I raise it to the power p , what will happen? It's basically 2 plus $f_1 x$ plus 1 , until $f_n x$ to the power n . So, the first set of coefficient efficient are very to write simply take each element raise to the power p of, just remember I am just multiplying this p times. So, very simple multiplication thing to do first thing is f_0 power p plus f_1 power p x to the power of p plus so on. Until, f_n power p x to the power p p whole raise to the power p are n . My claim is there are no other terms.

So, if you do not pick the same element. Every other terms will appear a multiple of p times this is the thing you can check in binomial. It is very easy to check that p is prime x plus y bar p every p choose i for i not equal to 0 will have p as a factor p will be a factor in this the same thing, in this same thing will happen here. So, you can quiet easily prove it I am not going to prove it to you, but no other term will happen here think about that why this true to. Because, there are p terms here and you have a p choice will picking one thing, if you choose to differ.

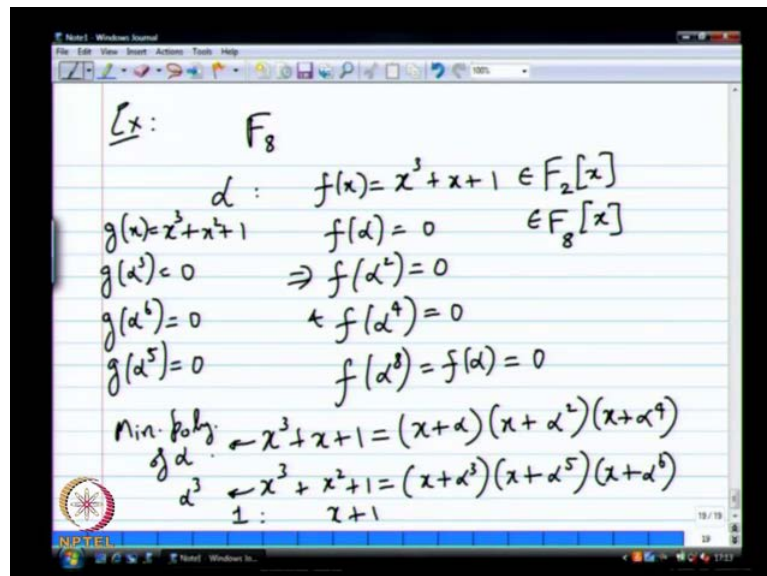
So, that is the idea, so you will get the p multiple happening once you say cannot picking the same element. So, everything else will go up to 0 check this if you like this. It is an interesting exercise or look up one of your multiple nominal thermosphere are extension of binomial to give you arbitrary formulas. Once, p is factor what happens it goes to zero you do not have to worry about it. So, this will be the expression, now I can keep

repeating this. I can repeat this as many times as I want I can do p squared same thing will result, but remember what is f i power p same as f i itself. So, this simply becomes f 0 plus f 1 x power p plus so on till f n x power p raise to the power n , which you can write in a very smart way. As f of x raise to the power p is the same as f substituted with x power p .

So, it is a curious little result which is true for finite characteristics fields, it not true if you do not have finite characteristics real. All you would not have such result, but of x whole to the power p is the same as f of x power p . Now, can you show if β is a root β power p is also a root. It shall this equation is a proof of that put x equals β the left hand side is 0 . So, definitely f of β power p is also a root.

So, how do you show f of power β square does also a root. Second put equal β power p get β power is square. So, f of β 0 implies f of β power this display driver is driving on me too often, β power p power i is 0 For i equals 1 2 . So, let's go back and see the example that we had in a F_8 . Convince us also this is true that, all engineers, unless we say examples will never believes in something is true, abstract truths can go wrong.

(Refer Slide Time: 01:00:26)



So, let us see an example in f eight we had minimum minimal polynomial of α . What was the minimal not minimal polynomial one of the polynomials, which had α had a root was f of x equals x power 3 plus x plus 1 f of α was 0 . You can check that f of

alpha squared will also be 0 and f of alpha power 4 will also be 0, I do not know. If I check of alpha bar 8 alpha par 8 is also very easy to check. Very easy to check as a same as f of alpha.

Now, we have something interesting we see if anyone is noticing is anything. So, anything interesting in what I have written down have f of x, which is polynomial n f p x. Clearly, it is also a polynomial n f q x or any other x does not matter some polynomial treating into is that. I am looking f q how many roots do I have 2 3 3 roots. So, what should happen? So, f of alpha is 0 and n plus alpha should divide x bar 3 x plus 1.

So, x plus alpha squared will also divide x bar 3 x plus 1 x plus 4 also will divide. So, should definitely happened x power 3 plus x power 1 should have definitely been plus alpha minus. Well, should I say minus alpha or plus alpha here I am doing F 8. Now, in general its minus I agree with you, but this is F 8 minus is the same as plus x plus alpha square times alpha power 4. This has to be true check this I think its good the first time you see at to multiplied it out, that check that indeed you are getting x power plus 1. So, polynomial degrees 3, it can have at most three roots. This is true for any field in any field f x.

A degree roots you cannot have more than degree roots because more than degree roots polynomial is identical. That is true for any field here I have three roots. Clearly, it has to be like this no other I know x power 3 matches. So, form is also very easy to write down the coefficient of x power 3 on both sides is one. This is a way to write down it is an interesting thing to check, but on the face of it you would not think this is true. On the right hand side you have all these abstract alphas like you put it. The left hand side we have only the very real once there no abstraction in that. That right, its true this is an equality not happy. So, in a way what is happening here you can check this. I let you check it later I do make a point here, which is quiet important.

So, you take some number some element and form this product x plus alpha x plus alpha square x plus alpha 4 all the conjugates together, but you end up getting of you get a polynomials. On the left hand side it has coefficients from a smaller field. This is true in your real numbers and complex numbers also you do, x minus a into x minus a star looks like complex number, but you do not have any complexes in the after the product. x

squared minus a plus a star becomes simply two times real part of a. Then you have plus a a star which is actually mod a squared, which is again real.

So, these things are these are obvious extension, in the real obvious analogies is real complex side also. This same thing is true for the other case also you can show for instance there was other polynomial. We had right what is g of x x power 3 plus x plus 1. Then I had g of α power 3 is 0 and you square it you get g of α power 6 is 0. The square α power 6 what do you get α power 12 α power 12 is what α power 5. Because, α power 7 is one know, so g of α power 5 is also 0. So, clearly what should be x power 3 plus x power 3 plus 1 x plus α power 3 x plus α power 5 x plus α power 6.

Now, I want to claim that the minimal polynomial of α is actually x power 3 plus x power 1. How would I prove something like that? What is involved in proving something like this? See, if α is a root of a polynomial from $f^2 x$. So, I can say as well this f^2 . If α is a root of some polynomial in $f^2 x$ surely α square and α power 4 are also roots of that same polynomial. So, there is no way the minimal polynomial of α can have degree less than 3 will have degree, at least 3. I have one polynomial here degree is equal to 3. It is clearly this should be the minimal polynomial of α . The same thing is true here minimal polynomial of α power 3 has to be this.

Precisely, the same reason yes the same reason similarly, this minimal polynomial for α power 3. Let me ask you a couple of questions with simple answers. May be make you think what is the minimal polynomial of α square, its same as this. So, one thing that was very obvious all the conjugates will have the same minimal power, this has to be the same. So, the minimal polynomial of α , α square and α power 4 will all be x power 3 plus x plus 1. They are conjugates where ever you start if you keep on squaring you will get the other terms. So, minimal polynomial of α power 3 α power 4 α power 5 and α power 6 is x power 3 plus x square plus 1. What is the minimal polynomial of $1 x$ plus 1. So, let me show you one more impressive fact impressive one.

(Refer Slide Time: 01:08:19)

$$F_8: x^8 - x: \text{roots } 0, 1, \alpha, \alpha^2, \dots, \alpha^6$$
$$x^8 - x = \prod_{\beta \in F_8} (x + \beta)$$
$$= x(x+1)(x^3+x+1)(x^3+x^2+1)$$

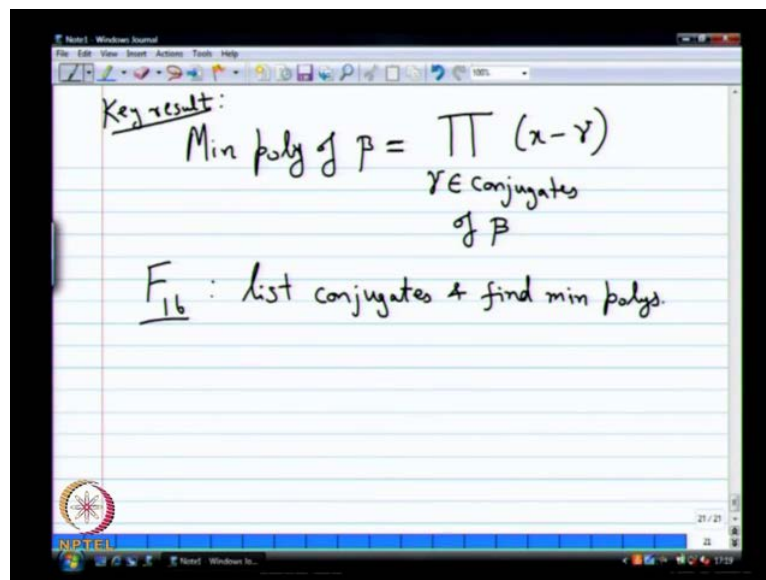
- Conjugates have same minimal polynomial
- Minimal polynomials are irreducible.

So, I told you something about $x^q - x$ in this case $x^8 - x$. The roots are what all the elements of F_8 , how many elements do I have in F_8 . So, what should happen now? I have polynomial of degree eight and it has eight roots. So, what should $x^8 - x$ be minus x or plus x there a small in F_8 , this is all in F_8 . So, minus plus does not matter what should $x^8 - x$ be product of, let say some I do not know beta. We have to use Greek when it is not this a something non Greek belongs to finite. It is a beta beta and $F_8 - x + x\beta$. So, look at what is happening else its where interesting I put beta equals 0, I get x that is one factor put beta equals 1, I get $x + 1$. Then I put beta equals alpha alpha square alpha power 4.

I will multiple those three together what will I get alpha power 3 plus $x^3 + 1$. Then I have alpha power three alpha power 4 alpha power 5 alpha and power 6. I will multiply those three terms together. I will get $x^3 + x^2 + 1$. This is the factorization, which will works only module two. If you do not have modular two this factorization will not make sense of course, it is all in F_2 and F_8 . All that important surprising impressive to seems that impressed. So, let us let me just quickly promise this couple of these facts. The first one is conjugates have same minimal polynomial. You can prove it I do not want to prove it and write it down its question of writing it down have same minimal polynomial.

This is true in general the next fact that did not state anywhere, but that is also very easy to prove is that the minimal polynomials are irreducible. How do you quickly show that the minimal polynomials have to be reduced. If they are not irreducible what will happen you can write it as a factor of two other things. You element has to be the root of one or the other, which would have a strictly smaller degree. That violates you minimally or something, that is the way you can prove it. It can be written down you can show it is reduce minimal polynomials will have to be irreducible. The conjugates have same minimal polynomial the next statement, which is interesting to show is minimal polynomial of beta equals.

(Refer Slide Time: 01:11:55)



Product of its a gamma belonging to conjugates of beta x minus equals I said put in equality. So, this key result which needs proof I will prove it sometime in the next lecture give you a very simple high level, over view kind of proof that also very rigorous face of showing it. Basically, after add an examples and some proof they have come to the key result, which is minimal polynomial of an element in finite field can be found very easily. What do you do first find all the conjugates of the that particular element. How do you find the conjugates list beta beta power beta power b beta power b square. Till you get the reputation no one to get the reputation, you can have stop, you cannot keep on going. So, once you do that you get list of conjugates.

Then it turns out multiply x minus those conjugates you end up getting the minimal polynomial. What does it mean? Means in particular that this polynomial has coefficients from F , so F . So, that is the only non-trivial thing to prove here once you show the coefficients of this polynomial. On the right hand side is from F you have done of course, that has degree equal to the number of conjugates. That has to be minimal point that nothing more to prove beyond that only thing is how do you show that, this guy has coefficients from F .

So, little bit non-trivial the idea is to show you have to basically power p and show that x^p becomes, then you will get the answer. That means that the coefficients when raised to the power p remain unchanged. That means they are in F that has been shown all these things, that is the rough proof will do some time the next class. So, think about it it's very interesting another thing you should try is go to F_{16} , F_{16} conjugate list conjugates.

Find minimal polynomial you can do this right? You have all the elements tools to do it make the table. Take one element find all its conjugates $2 \times$ plus that multiply you from the table. You can do everything, you can find all the minimal polynomial very easily or if you want the simple method. We go to mad club and ask him to find minimal problem. That is the easier way of doing the whole problem, but if you want to do it by hand, in the first time I will gradually. Now, that is it the will meet tomorrow.