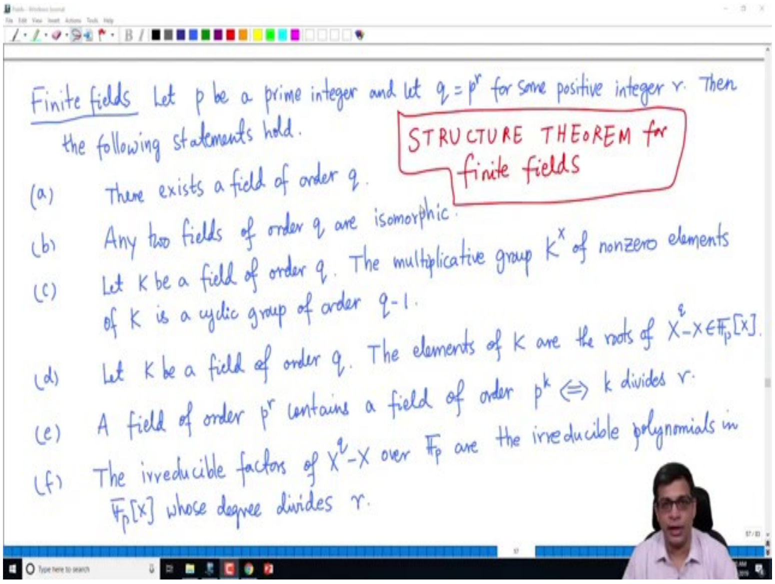
Introduction to Rings and Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 41
Finite fields 2

(Refer Slide Time: 00:17)



Finite fields Let p be a prime integer and let $q = p^r$ for some positive integer r. Then the following statements hold.

STRUCTURE THEOREM for finite fields

(a) There exists a field of order q.

(b) Any two fields of order q are isomorphic.

(c) Let K be a field of order q. The multiplicative group $K^\times$ of nonzero elements of K is a cyclic group of order $q-1$.

(d) Let K be a field of order q. The elements of K are the roots of $X^q - X \in \mathbb{F}_p[X]$.

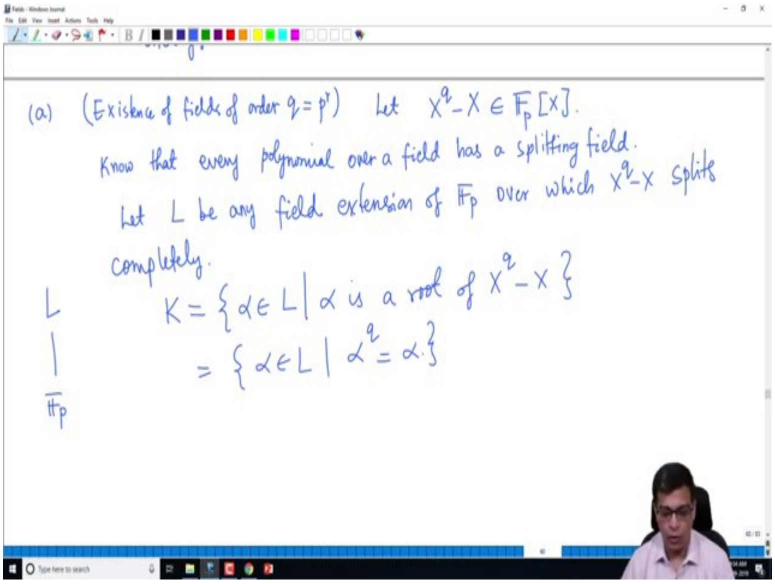
(e) A field of order p^r contains a field of order $p^k \Leftrightarrow k$ divides r.

(f) The irreducible factors of $X^q - X$ over $\mathbb{F}_p$ are the irreducible polynomials in $\mathbb{F}_p[X]$ whose degree divides r.

Let us continue now, we are in the middle of proving the structure theorem for finite fields which is this statement, it says a lot of information; gives a lot of information about finite fields. We proved a couple of these statements and let us now do the remaining parts.

So, far we have proved (d) and we have actually not proved (c), but I told you that I will skip the proof, because it uses some group theory facts which I do not want to do now. And now, let us now prove which is the main theorem that we want focus on.

(Refer Slide Time: 00:46)



(a) (Existence of fields of order $q = p^r$) Let $X^q - X \in \mathbb{F}_p[X]$.

Know that every polynomial over a field has a splitting field.

Let L be any field extension of $\mathbb{F}_p$ over which $X^q - X$ splits completely.

$$\begin{tikzcd} L \arrow[d, dash] \\ \mathbb{F}_p \end{tikzcd}$$

$$K = \{\alpha \in L \mid \alpha \text{ is a root of } X^q - X\}$$
$$= \{\alpha \in L \mid \alpha^q = \alpha.\}$$

So, (a), which is exactly the existence of finite field; existence, so I will write it here existence of fields of order q. Remember in the example that I did in the before the stating the theorem in the last video. We constructed a field of order four by looking at F 2 and a degree two irreducible polynomial and going modulo that. But I also commented in the last video, that in general this method is difficult to implement. Because how do you know that there is a irreducible polynomial of degree r over F p; if it exists, then we can go modulo 8 and get the field that we want which is p power r.

So, we are going to take a different approach using what we have already observed which is that elements of such a field if it exists are going to be roots of X power q minus X. So, what we are going to do is use a theorem that I have proved earlier in the video, earlier in the course about splitting fields. So, let us do the following.

So, let I considere the polynomial X power q minus X in F p X. We already know that, every field every polynomial over a field has a splitting field. If you go back and look at that splitting fields video, you will see that we proved that in general capital F was any field small f was any polynomial and we constructed a splitting field. So, that was not specific to finite fields or infinite fields or anything like that. So, we will apply that to F p and X power q minus X.

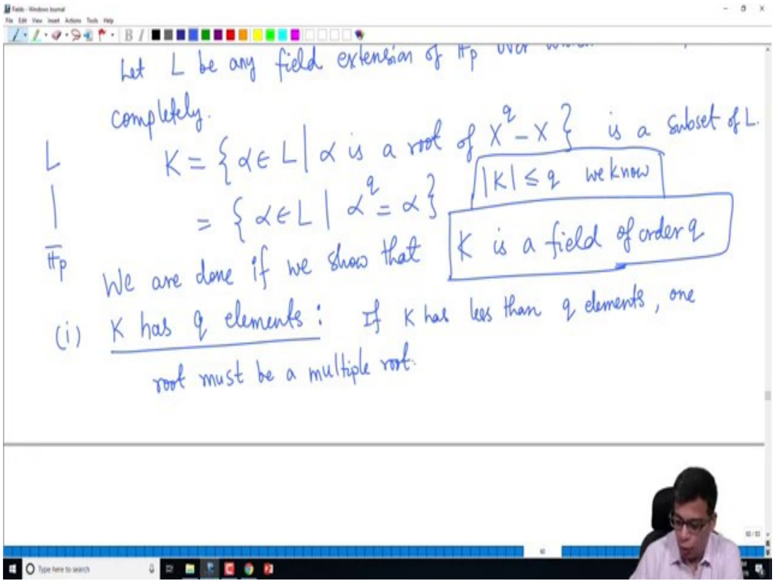
So, let us take some splitting field. So, let L be a splitting field actually we do want a splitting field, but I will state it like this. So, that it becomes slightly easier to understand what I am saying. Let any, let L be any field extension of F p over which X power q minus X splits completely. So, we have such a field.

So, you have F p here and some extension exists where X power q minus X splits completely; that means, it is a product of linear polynomials. What we want is that just look at the roots of this by part (d) that I already proved; remember, part (d) that I already proved that any field of order q that we are now trying to show exists is going to be exactly the roots of X power q minus X.

What I have now done is I have constructed a big field where X power q minus X splits completely; that means, it L contains all the roots of X power q minus X. We know that K is supposed to be the desired field K of order q is supposed to be this collection of roots of this.

So, we want to just take K to be alpha in L such that alpha is a root of X power q minus X. We know that alright, I am just rewriting that we know that K if it exists is supposed to be like this. So, I will define K like this and hope for the best, what do we need to show? It is a subset of L now.

(Refer Slide Time: 04:48)



Let L be any field extension of $\mathbb{F}_p$ over

completely.

$$\begin{tikzcd} L \arrow[d, dash] \\ \mathbb{F}_p \end{tikzcd}$$

$K = \{\alpha \in L \mid \alpha \text{ is a root of } X^q - X\}$ is a subset of L.

$= \{\alpha \in L \mid \alpha^q = \alpha\}$ $\boxed{|K| \leq q \text{ we know}}$

We are done if we show that $\boxed{K \text{ is a field of order } q}$

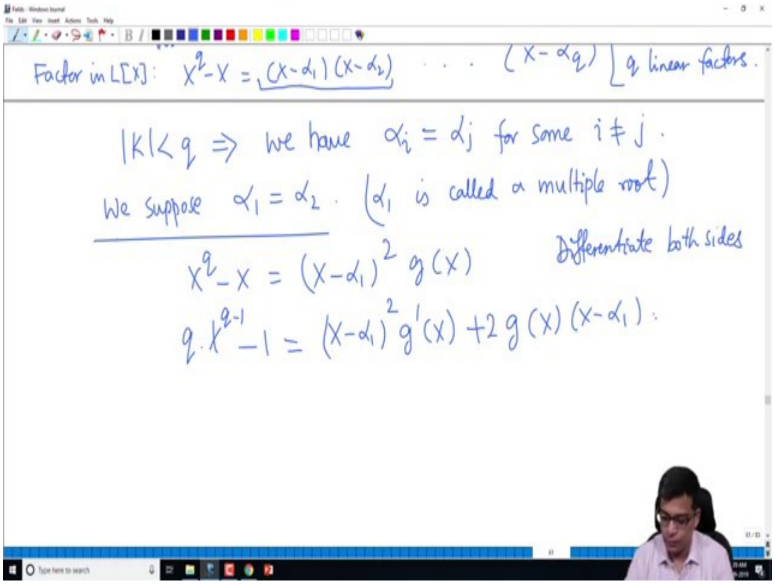
(i) K has q elements: If K has less than q elements, one root must be a multiple root.

We get what we want, if we show that K is a field, right. If K is a field it certainly has we also need to show that containing q elements. So, let us say we are done if K is a field of order q. So, I need to also show that it has order q. So, I need to show that it is a field and that its order q. So, two things; K has q elements.

So, there are two things I will break up the proof into two parts, K has q elements and that K is a field. So, this I will not do in detail because I did not do the notion of multiple roots of the polynomial in detail. So, I am going to just quickly tell you that K has q elements, because how can it have fewer than q elements? If it has fewer than q elements that means, some root is a multiple root; if K has less than q elements.

So, remember K is the collection of roots of X power q minus X, it is an exercise that there are at most q of such elements so, but it can be in general less than q. So, certainly what I am saying is that maybe I will do this as an exercise later. Order of q K is less than or equal to q we know this. If you have a polynomial or a field of order q degree q its roots is at most q and we are now trying to show that it is exactly q. Suppose, it has less than q elements then one root must be a multiple root.

(Refer Slide Time: 07:01)



Factor in L[X]: $X^q - X = \underbrace{(X-\alpha_1)(X-\alpha_2) \quad \cdots \quad (X-\alpha_q)}$ q linear factors.

$|K| < q \Rightarrow$ we have $\alpha_i = \alpha_j$ for some $i \neq j$.

We suppose $\alpha_1 = \alpha_2$. (α_1 is called a multiple root)

$$X^q - X = (X-\alpha_1)^2 g(X)$$ Differentiate both sides

$$q \cdot X^{q-1} - 1 = (X-\alpha_1)^2 g'(X) + 2g(X)(X-\alpha_1).$$

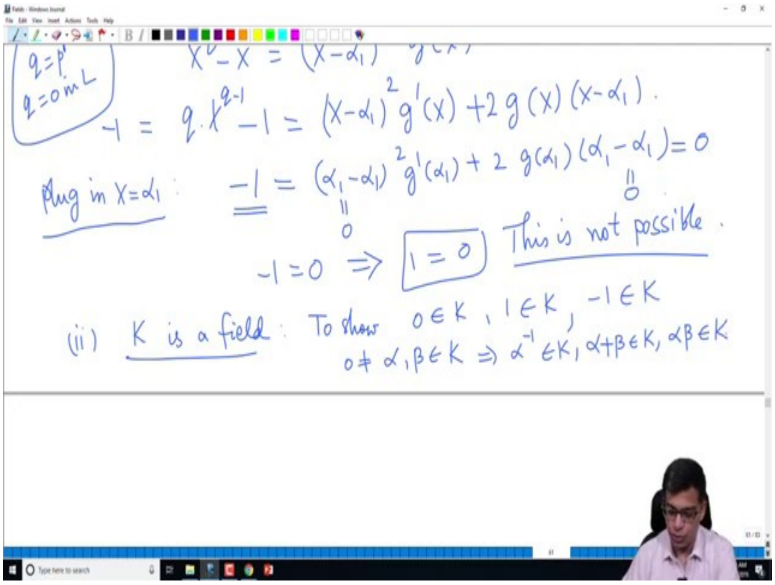
What I mean is you can write X power q minus X factor in L X. You can factor at L in L X, X power q minus X as X minus alpha 1, X minus alpha 2, all the way up to X minus alpha q. You because this is degree q and you have every factor is a linear factor. So, there must be q linear factors right, there must be q linear factors.

If the q linear factors are all distinct then you have q distinct roots and that is the claim that I am making. Suppose q has fewer than K has fewer than K elements q elements; that means, something is repeated. So, if order of K is strictly less than q, then we have alpha i is equal to alpha j for some i not equal to j. So, without loss of generality, so we suppose alpha 1 is equal alpha 2.

So, some factor is repeated so, it is called a multiple root alpha 1 is called a multiple root. But then I want to rewrite this X minus; X power q minus X as X minus alpha 1 whole squared times g X. The remaining thing I do not care right, because alpha 1 is equal to alpha 2; the first two things I will combine and write it like this.

Now, if you differentiate both sides what do we get? We get q times X power q minus 1 minus 1 that is the derivative of the left hand side, the right hand side I am going to use the product rule. So, I will have X minus alpha 1 whole squared times g prime X. Let us g X times 2 times g X times X minus alpha 1, right. So, I have this.

(Refer Slide Time: 09:15)



$q = p^r$
$q = 0$ in L

$X^q - X = (X-\alpha_1)^2 g(X)$

$-1 = q \cdot X^{q-1} - 1 = (X-\alpha_1)^2 g'(X) + 2g(X)(X-\alpha_1).$

Plug in $X=\alpha_1$:

$\underline{\underline{-1}} = \underset{0}{\underset{\shortparallel}{(\alpha_1-\alpha_1)^2}} g'(\alpha_1) + 2g(\alpha_1)\underset{0}{\underset{\shortparallel}{(\alpha_1-\alpha_1)}} = 0$

$-1 = 0 \Rightarrow \boxed{1=0}$ This is not possible.

(ii) K is a field: To show $0 \in K$, $1 \in K$, $-1 \in K$

$0 \neq \alpha, \beta \in K \Rightarrow \alpha^{-1} \in K, \alpha+\beta \in K, \alpha\beta \in K$

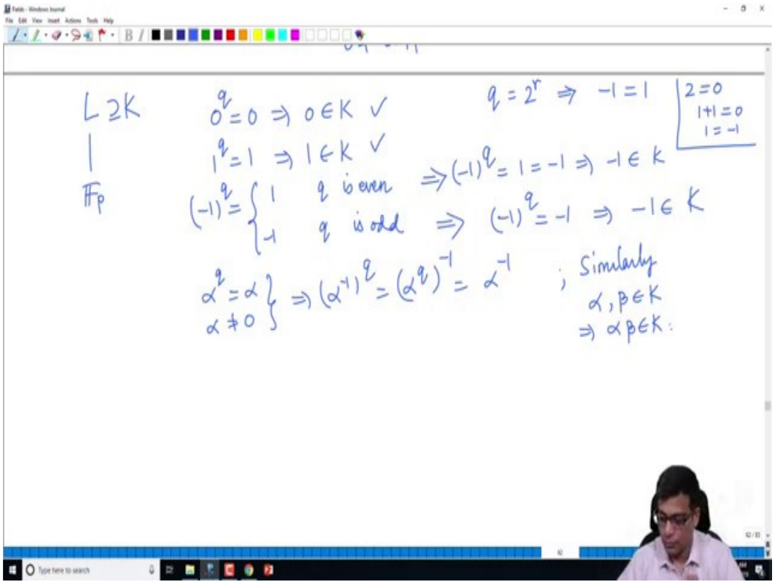
Now, plug in X equal to alpha 1, what do I get? I get so, this is actually equal to minus 1, why is that, because q is 0 right, q is p power r; that means, q is 0 in L. If L contains Z mod pZ; that means p is 0, once p is 0, p squared is 0, p cubed is 0 p power r 0. So, q is 0; that means, minus 1.

So, if you plug in minus alpha equal to X; on the left side nothing changes because it is a constant. On the right hand side you get alpha 1 minus alpha 1 whole square times g prime alpha 1 plus 2 times g of alpha 1 times alpha 1 minus alpha 1, but this is 0. Because this is 0 and this is 0, but; that means, minus 1 equals 0; that means, 1 equal to 0, because I can take negative of both sides this is not possible. Because in any field you have at least two elements and 0 and 1 are going to be different.

So, this is not possible, so; that means, no root can repeat, that is a point. In multiple root must be a common root of the polynomial and its derivative. But, the derivative of the special polynomial that we are interested in here X power q minus X is actually minus 1. So, it cannot have any roots. So, the derivative and the polynomial cannot have common roots. So, the polynomial in question has q distinct roots. So, K has q elements.

So, now, second part is K is a field. This is a very rare situation, we are taking a polynomial and taking its roots, very rarely do they form a field, roots of a polynomial rarely form a field. But, it happens over finite fields and these specific polynomials. So, what do we have to show? So, I am going to skip most easy things, what are we going to show? So, we want to show 0 is there, 1 is there, minus 1 is there, if alpha and beta are in K and let us say alpha is not 0 then alpha inverse is there, alpha plus beta is there, alpha beta is there and so on.

(Refer Slide Time: 11:48)



$L \supseteq K$

$\mathbb{F}_p$

$0^q = 0 \Rightarrow 0 \in K$ ✓

$1^q = 1 \Rightarrow 1 \in K$ ✓

$q = 2^r \Rightarrow -1 = 1$

$2 = 0$
$1+1 = 0$
$1 = -1$

$(-1)^q = \begin{cases} 1 & q \text{ is even} \\ -1 & q \text{ is odd} \end{cases}$

$\Rightarrow (-1)^q = 1 = -1 \Rightarrow -1 \in K$

$\Rightarrow (-1)^q = -1 \Rightarrow -1 \in K$

$\left.\begin{array}{l} \alpha^q = \alpha \\ \alpha \neq 0 \end{array}\right\} \Rightarrow (\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$; Similarly

$\alpha, \beta \in K$
$\Rightarrow \alpha\beta \in K$:

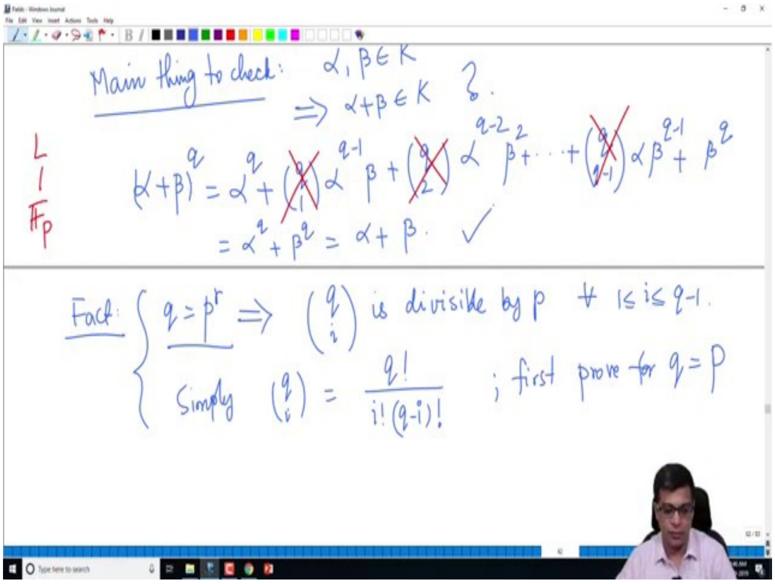
So, these are the conditions right, we have a subset of K of L and we are claiming that it is a field; that means, take two elements their product is there, the sum is there, if nonzero, then its inverse is there, 0 is there, 1 is there and so on, ok. So, let us check all these things one by one; 0 power q is certainly 0 that means, 0 is in K. Remember the definition of K, K is the set of roots of X power q minus X. So, if any root any element of L satisfies X power q minus X, it is in K.

So, I hope you are following everything if not please pause the video think about it, this is the most crucial part of the whole structure theorem. In fact, (a) and (b) are the most important statements. So, 0 is there, 1 power q is 1 so, 1 is there right similarly minus 1 power q is either minus 1; so, there are two possibilities right, if it is 1 if q is even, minus 1 if q is odd.

In this case of course, we are done because minus 1 power q is minus 1 and hence minus 1 is in K. But, if q is even also we are done, because if q is even; that means, q is of the form 2 power r, right. The only even numbers which are powers of primes or powers of 2, in which case minus 1 is 1; because its characteristics is 2. So, 2 equal to 0 means 1 plus 1 equal to 0 that means, 1 equal to minus 1.

So, again in this case minus 1 power q is actually equal to 1 which is equal to minus 1 so, minus 1 is in K, ok. And if alpha power q is alpha and alpha is nonzero then alpha inverse exists in L and its power q is also alpha power q minus 1 which is alpha power minus 1. Similarly, the easier thing is alpha beta are in K and alpha beta is in K. So, this is easy.

(Refer Slide Time: 14:10)



Main thing to check: $\alpha, \beta \in K \Rightarrow \alpha+\beta \in K$?.

L
$|$
$\mathbb{F}_p$

$$(\alpha+\beta)^q = \alpha^q + \cancel{\binom{q}{1}}\alpha^{q-1}\beta + \cancel{\binom{q}{2}}\alpha^{q-2}\beta^2 + \cdots + \cancel{\binom{q}{q-1}}\alpha\beta^{q-1} + \beta^q$$
$$= \alpha^q + \beta^q = \alpha + \beta. \quad ✓$$

Fact: $q = p^r \Rightarrow \binom{q}{i}$ is divisible by p $\forall\ 1 \leq i \leq q-1$.

Simply $\binom{q}{i} = \frac{q!}{i!(q-i)!}$; first prove for $q = p$

So, the main thing to check is the sum; all these things are easy, main thing to check is the sum. Let us say alpha and beta are in K, we want to show that alpha plus beta is in K and this is where the characteristic again comes to our rescue. Again let me remind you, what is the meaning of being in K? That means, its power its q th power is itself. So, let us take the q th power alpha plus beta power q.

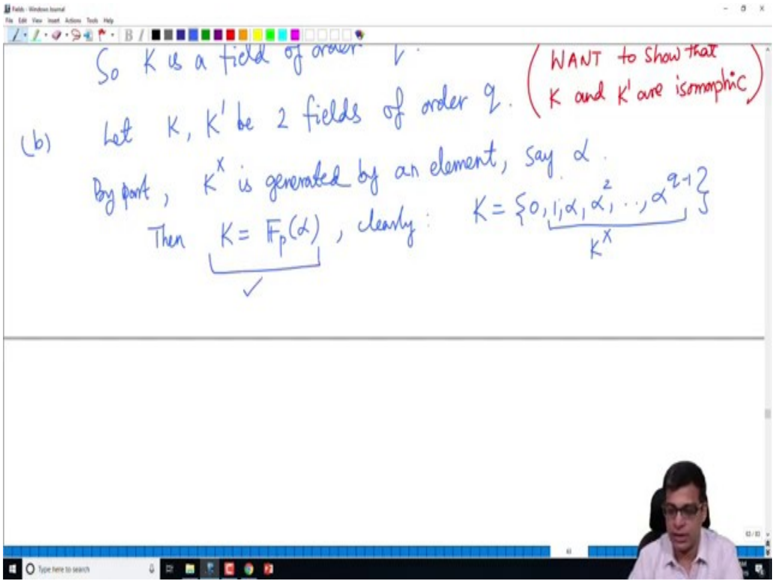
If you apply binomial theorem you get alpha power q; q choose 1, alpha power q minus 1 beta; q choose 2, alpha power q minus 2 beta as square dot dot dot, q choose q minus 1 alpha beta power q minus 1 plus beta power q, right. This is the binomial expansion of alpha plus beta power q.

Now, this is a simple fact which I think came up in the earlier part of the course. Since q is of the form p power r, you can show that q power; q choose I is 0 for all I between. So, all you need to do is simply write q power i as q factorial divided by factorial times q minus I factorial. And first prove it for P itself in which case it is trivial then by induction extend to powers of q. So, I am going to skip this again, this is going to lead me in a different direction.

So, I will skip this sorry, actually I should not say this is not 0. In general I can say it is divisible by sorry divisible by p for all i between 1 and q minus 1. Because there will be a factor of p in the numerator that will survive after cancelling all the factors in the denominator.

So, it is divisible by p, but if it is divisible by p we are in a field which contains F p whose characteristic is p; that means, p 0 in F p hence p 0 in L. So that means, this is 0 this is 0 this is 0. So, every intermediate term is 0 so, this is alpha power q let us beta power q, only the first and the last terms survive, but alpha and beta are in K. So, alpha power q is alpha beta power q is beta. So, alpha plus beta all power q is alpha plus beta.

(Refer Slide Time: 16:56)



So K is a field of order q.

(b) Let K, K' be 2 fields of order q. (WANT to Show that K and K' are isomorphic)

By part, $K^{\times}$ is generated by an element, say α.

Then $\underbrace{K = \mathbb{F}_p(\alpha)}_{\checkmark}$, clearly: $K = \{0, \underbrace{1, \alpha, \alpha^2, \ldots, \alpha^{q-1}}_{K^{\times}}\}$

So, this is an indirect proof, but it is a very nice proof. So, K is a field of order q. So, we have shown that for every prime power there is a field of that order. So, let me now prove part b, which is the second most important part of this whole structural theorem, let K and K prime be two fields of order q.

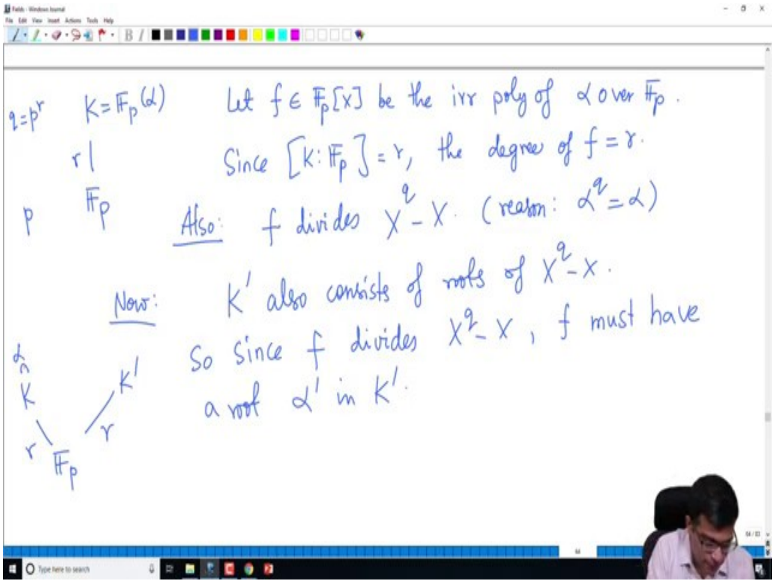
We want to show that K and K prime are isomorphic as fields, of course, which is same as rings, ok. So, let us prove that, what we have is by part so, I forget the part. So, part (b) is the statement that any two to fields of order q are isomorphic. We know part (c), though we did not prove it we are going to make use of it. Part (c) says that K cross which is the multiplicative group of non-zero elements of K is generated by a single element let us call that alpha, right.

So, in particular we must have that K is F p alpha, right; remember all these extensions are finite K and K prime are finite fields. So, they are finite extensions of F p, because certainly if you finite field there the dimensions is also finite. So, it is a finite extension so it is an algebraic extension. And in fact, alpha generates it because remember this is easy.

Because, what is K? It is actually 0, 1, alpha, alpha squared up to alpha power q minus 1. Because other than 0, the remaining elements are in K cross which is a cyclic group of order q minus 1 generated by alpha. So, K cross contains elements of the form 1 alpha alpha squared alpha power q minus 1 and K of course, contains 0 so, K is this. What is the meaning of being F p alpha? That means, every element of K is supposed to be a polynomial in alpha.

In fact, every element of K is a very simple polynomial in alpha, every element of K is either 0 or in fact, the power of alpha. So, this is certainly true in fact, much more than this is true this is a very weak statement. I am saying that this is certainly true what we have here is a much stronger statement than this, but I will only use this fact so, ok.

(Refer Slide Time: 19:46)



Let $f \in \mathbb{F}_p[X]$ be the irr poly of α over $\mathbb{F}_p$.

Since $[K:\mathbb{F}_p]=r$, the degree of $f = r$.

Also: f divides $X^q - X$. (reason: $\alpha^q = \alpha$)

Now: K' also consists of roots of $X^q - X$.

So since f divides $X^q - X$, f must have a root α' in K'.

Now, we can actually draw this picture K, F p and K is F p alpha. What is the degree of this extension? It is r right, because this has q power r elements sorry, this has q elements which is p power r and this has p elements. And we used the counting argument in the earlier video, which says that if the elements are p power r here over a field of order p the dimension is r; so, the irreducible polynomial.

So, let f be in F p X be the irreducible polynomial of alpha over F p it is an algebraic element. So, we can take irreducible polynomial. Since K colon F p is equal to r the degree of f is r, right. This is way back when we talked about degree of field extensions versus degree of elements; so, degree of F itself is r. Also we know that f divides X power q minus X, why is that?

The reason is alpha power q is equal to alpha, alpha being an element of K and by part maybe a d or d I think we showed that every element of K is a root of X power q minus X. So, in particular alpha is a root of X power q minus X, but f is a irreducible polynomial of alpha; that means, f divides that.

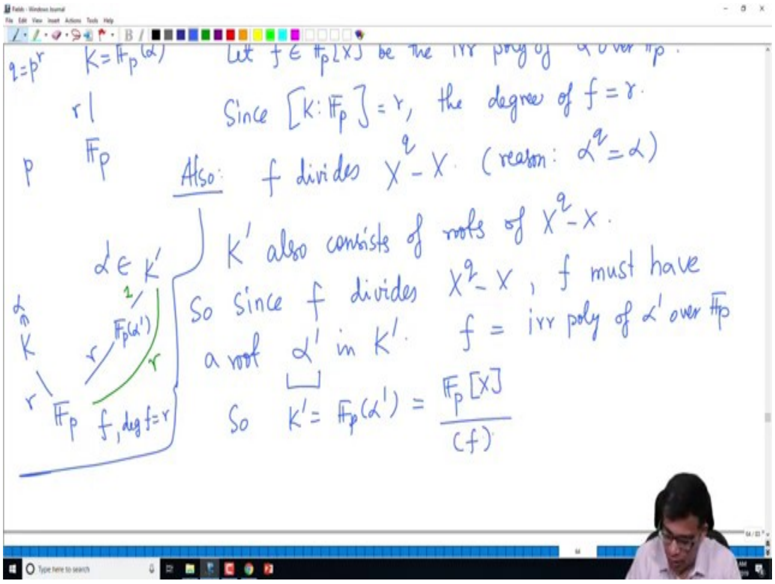
Now, K prime which is a field of order q also consists of roots of X power q minus X right also consists of roots of X power q minus X. So, since f divides X power q minus X, f must have a root alpha prime in K prime ok. So, this is a bit tricky, but what I am saying is that K is there it is an extension of F p of degree r.

Similarly, K prime is there this is also an extension of degree r, because K prime also contains p power r elements; alpha is here, right. The irreducible polynomial of alpha is small f; which lives over capital F p. That small f divides X power q minus X, X power q minus X splits completely in K prime, because K prime exactly consists of roots of X power q minus x; that means, f must have a root in K prime. I am calling that alpha what you have to be careful about is, you cannot compare and K prime they can be very different. They are not contained in each other or they are not contained in a bigger field.

So, you cannot say alpha is in K prime that could be incorrect. But we can say that f has a root alpha prime in K prime. Then, what would be? So, I am going to squeeze in here F p alpha prime and I have a K here prime here. So, F p alpha prime is here which is a root of; so, now, I will remove that r here F p alpha prime is the field generated by alpha prime where alpha primes is the root of f. So, f must be the irreducible polynomial of alpha prime over F p, because f is an irreducible polynomial, alpha prime is a root of f. So, f must be the irreducible polynomial of alpha prime.

But, then degree of f is r; so, this must be r right a degree of an extension is equal to degree of a extension generated by single element is equal to the degree of that element. But this whole thing is also r, right that is because K prime has q elements which is p power r so, this is r that means, this must be 1.

(Refer Slide Time: 24:19)



Let $f \in \mathbb{F}_p[X]$ be the irr poly of α over $\mathbb{F}_p$.

Since $[K : \mathbb{F}_p] = r$, the degree of $f = r$.

Also: f divides $X^q - X$. (reason: $\alpha^q = \alpha$)

K' also consists of roots of $X^q - X$.

So since f divides $X^q - X$, f must have a root α' in K'. f = irr poly of α' over $\mathbb{F}_p$

So $K' = \mathbb{F}_p(\alpha') = \dfrac{\mathbb{F}_p[X]}{(f)}$

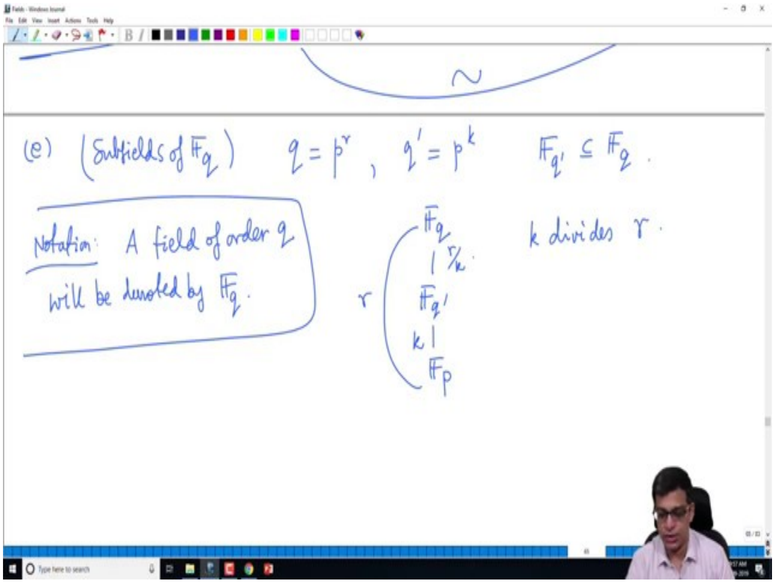
When is something 1, when is a degree of field extension 1 so, K prime is equal to F p alpha prime. But, what is F p alpha prime? This is another way of writing, F p X modulo f, right. This was done in the beginning of our field theory part. Because anytime you adjoin an algebraic element it is isomorphic to do this ring modulo, the ideal generated by the irreducible of polynomial that algebraic element.

But this is also same as F p alpha, because F p alpha is also obtained by going modulo the irreducible polynomial of alpha which is f, but of course, that is K ok. So, K is isomorphic to K prime as required. So, this completes the proof of part b. So, part b; remember part b and a are the important things for us, part b was that any two fields of order q are isomorphic.

So, this I have shown; I have shown that there is a field of order q we are shown today in the beginning. In the last video I have shown that any ok so, not sure, but I have commented that this is true because of the fact in group theory and I will not prove that. So, c is taken care of and in the last video we have proved d that every field of order q consists of roots of X power q minus X. So, that leaves two parts.

So, I am going to go fast over this and I would rather give examples to illustrate this instead of proving this because proof can get a bit tricky. So, I will instead of proving all directions both directions, so I will prove some parts of it. So, let us now come to e. So, let us now come to e.

(Refer Slide Time: 26:15)



(e) (Subfields of $\mathbb{F}_q$) $q = p^r$, $q' = p^k$ $\mathbb{F}_{q'} \subseteq \mathbb{F}_q$.

Notation: A field of order q will be denoted by $\mathbb{F}_q$.

$$\begin{tikzcd}\mathbb{F}_q \arrow[d, dash, "r/k"] \\ \mathbb{F}_{q'} \arrow[d, dash, "k"'] \\ \mathbb{F}_p\end{tikzcd}$$

r

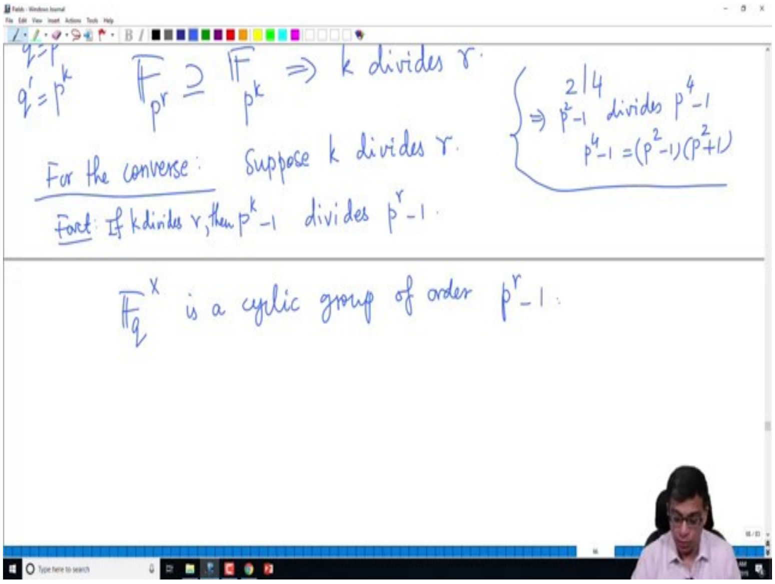
k divides r.

So, let us come to e; e was talking about sub fields of F q. So, one direction is clear that is because so, let us say q is p power r and q prime is p power k, ok. Suppose so, also a notation I should have written this before writing that a field of order q will be denoted by F q by the part b any two fields of order q are isomorphic.

So, up to isomorphism I am allowed to use this symbol to denote any two fields. So, any field of order q will be denoted by F q. So, now, I am considering sub fields of F q. So, suppose F q prime is contained in F q; that means, if you draw the picture they have F p F q prime F q, right.

And what is the degrees of these extensions, what is the degree of F q prime over F p? Because q prime is p power k, I claim this is k right, because q is q prime is p power k at the dimension will be the exponent. What is the degree of this? That is r that is what we have been doing; q is p power r so, this is r. So, by the multiplicativity of degree X field extension degrees of field extensions we know that k divides r. In fact, this will be r by k. So, then the product of this two is r.

(Refer Slide Time: 28:11)



$q' = p^k$ $\quad \mathbb{F}_{p^r} \supseteq \mathbb{F}_{p^k} \Rightarrow k$ divides r.

$2 | 4 \Rightarrow p^2-1$ divides p^4-1

$p^4-1 = (p^2-1)(p^2+1)$

For the converse: Suppose k divides r.

Fact: If k divides r, then p^k-1 divides p^r-1.

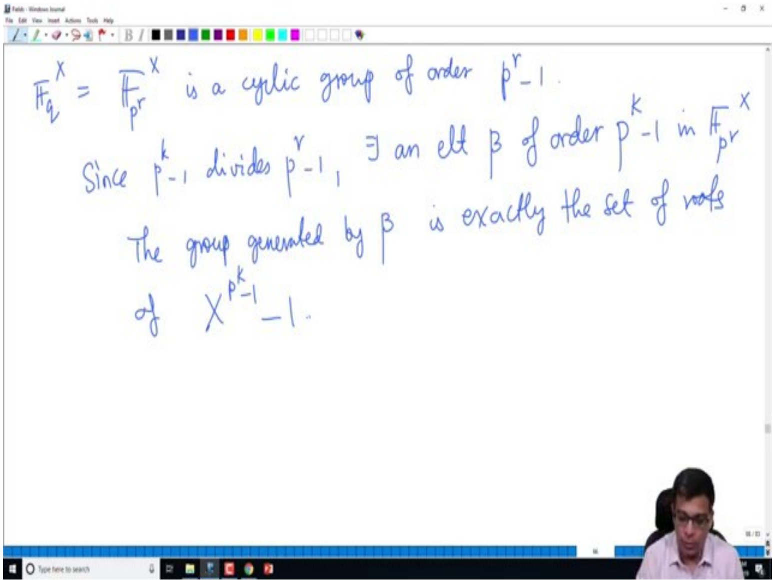
$\mathbb{F}_q^{\times}$ is a cylic group of order p^r-1.

So, the statement we have just proved is that F q; let me write it like this even though it is a bit messy, but if F p power r contains F q F p power k; that means, k divides r. The converse is also part of the statement, the converse I will not prove in detail, but only comment on the following for the converse. Suppose k divides r ok, suppose k divides r the fact here it is a simple numerical verification which I will leave this as an exercise for you.

If k divides r you can just this you can be; this you can find in any book. And one can show that p power k minus 1 divides p power r minus 1. So, I will skip this. If k divides r so, this is if k divides r, ok. So, if k divides r what I am saying is for example, 2 divides 4; that means, p squared minus 1 divides P power 4 minus 1 this is because P power 4 minus 1 can be written as P squared minus 1 and P squared plus 1, ok.

Something as simple as that, but in general you need to prove this. So, if I will assume this if k divides r then p power k minus 1 divides p power r minus 1 minus. In this case let us look at F q, remember we are trying to show that F q contains F p q is again let me remind you p power r q prime is p power k. I am assuming k divides r and I am trying to show that F q contains F q prime. F q cross is a group of order, cyclic group even of order p power r minus 1 q minus 1.

(Refer Slide Time: 30:33)



$\mathbb{F}_q^\times = \mathbb{F}_{p^r}^\times$ is a cyclic group of order $p^r - 1$.

Since $p^k - 1$ divides $p^r - 1$, $\exists$ an elt β of order $p^k - 1$ in $\mathbb{F}_{p^r}^\times$

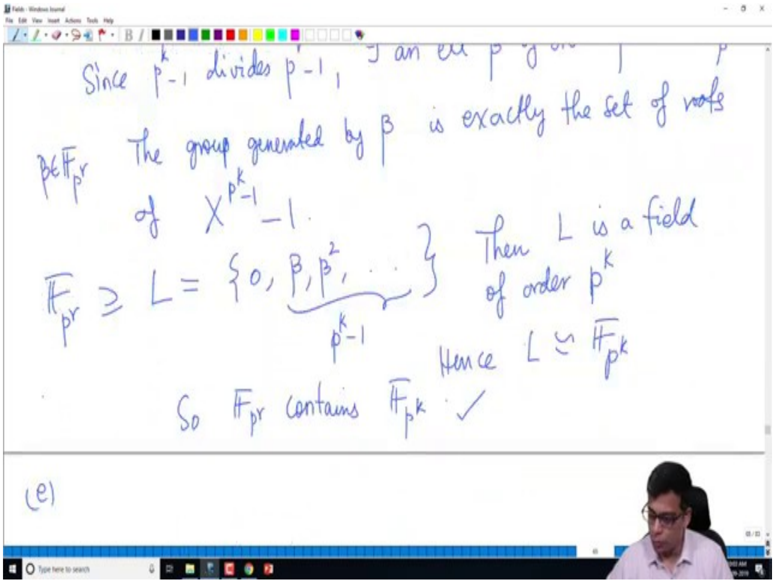
The group generated by β is exactly the set of roots of $X^{p^k - 1} - 1$.

So, I am trying to avoid the q here because there is q and q prime it is a bit confusing. So, this is p power r F q cross is, it is a cyclic group of order p or r minus 1. Since p power r; p power k minus 1 divides p power r minus 1 there exists an element of, let us call it beta of order p power k minus 1 in F power r cross.

So, this is a group theory statement. If you have a group cyclic group of order 100 any number dividing a 100, there is an element of that order, right. So, this is a statement about cyclic groups p power k minus 1 divides p power r minus 1 so, there exists an element beta of ordered p power k minus 1.

So, now, the group generated by beta are the roots can is exactly the set of roots of X power p power k minus 1 equal to 1 right, roots of the polynomial this. Because if b has order p power k minus 1 means b power p power k minus 1 minus 1 is equal to 1. Similarly b square has that property b, q as a property all powers of b have that property.

(Refer Slide Time: 32:11)



Since p^k-1 divides p^r-1, $\exists$ an el

$\beta\in\mathbb{F}_{p^r}$ The group generated by β is exactly the set of roots of $X^{p^k-1}-1$.

$\mathbb{F}_{p^r} \supseteq L = \{0, \underbrace{\beta, \beta^2, \dots}_{p^k-1}\}$ Then L is a field of order p^k

Hence $L \simeq \mathbb{F}_{p^k}$

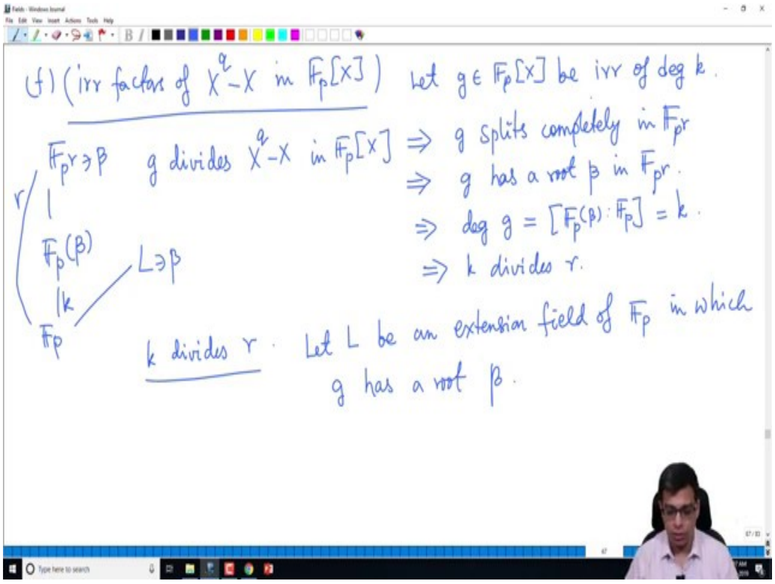
So $\mathbb{F}_{p^r}$ contains $\mathbb{F}_{p^k}$ ✓

(e)

Now, if you define L to be 0, beta, beta squared and so on. Then by the same argument that we have used earlier L is a field of order p power k exactly equal to p power, k, because there will be p power k minus 1 elements here and you are adding 0 to it. So, this is a field of order p power k. And hence so and L is of course, in L, L is of course, in F q because these are all elements in F q, right.

So, beta is in F p power r so; that means, these are all in F p power r. Hence L is isomorphic to F p power k right, because it is a field of order p power k. So, it is isomorphic to the unique field of that order. So, F p power r contains F p power k, ok. So, this is part d. So, finally, let me quickly prove part e which finishes this statement about sorry this is part e I think, so I want to do part f the final part.

(Refer Slide Time: 33:30)



(f) (irr factors of $X^q - X$ in $\mathbb{F}_p[X]$) Let $g \in \mathbb{F}_p[X]$ be irr of deg k.

g divides $X^q - X$ in $\mathbb{F}_p[X]$ $\Rightarrow$ g splits completely in $\mathbb{F}_{p^r}$

$\Rightarrow$ g has a root β in $\mathbb{F}_{p^r}$.

$\Rightarrow$ $\deg g = [\mathbb{F}_p(\beta) : \mathbb{F}_p] = k$.

$\Rightarrow$ k divides r.

k divides r. Let L be an extension field of $\mathbb{F}_p$ in which g has a root β.

So, this is the irreducible factors of X power q minus X in F p X that last part is this ok; so, let us prove this. So, suppose and we remember so, let me show you the theorem. So, the factors of X power q minus X or the irreducible polynomials in F p X whose degree divides r, ok. So, let us prove this.

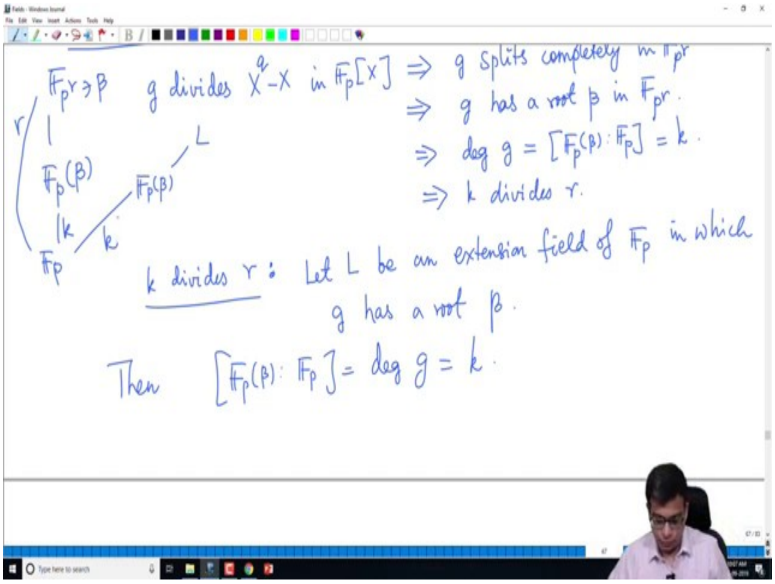
So, let g in F p X be irreducible of degree k. So, suppose it is irreducible of degree k. So, now, we are going to work with K which is F p power r sitting over F p this is a field extension of degree r. And remember X power q minus X splits completely in F p power r. It is in fact, X minus each element of F p r and you take the product. So, this is degree r extension.

So, now suppose g divides X power q minus X in F p X. So, it is same as dividing in F q X, but I will not stress that here. Suppose g divides this in F p X, then g splits completely in K which is F p power r, right. Because X power q minus X splits completely so, g being a divisor of it also splits completely.

This implies g has a root beta in F p r, right. So, g has a root in F p r so, let us call that beta. So, what I will now do is, I will expand this what I get is F p beta F p right so; that means, and what is the degree of this? Degree of g is equal to the extension field the degree right and we call that k. So, k is the degree of k of g. So, the degree of the field extension is k, this is again degree of a field extension generated by an algebraic element is equal to the degree of that particular algebraic element. But that means, this whole thing is r right. So, k divides r. So, if g divides that k divides r.

On the other hand, suppose k divides r, let beta in L. So, let L be an extension of F p in which g has a root. So, what I am saying is that you have a root let us call it beta again. I remember that for any field in any polynomial over there you can construct a bigger field in which it has a root. Because g is irreducible all you need to do is go modulo g, F p X mod g will do the job.

(Refer Slide Time: 37:24)



g divides $X^q - X$ in $\mathbb{F}_p[X]$ $\Rightarrow$ g splits completely in $\mathbb{F}_{p^r}$

$\Rightarrow$ g has a root β in $\mathbb{F}_{p^r}$.

$\Rightarrow$ $\deg g = [\mathbb{F}_p(\beta) : \mathbb{F}_p] = k$.

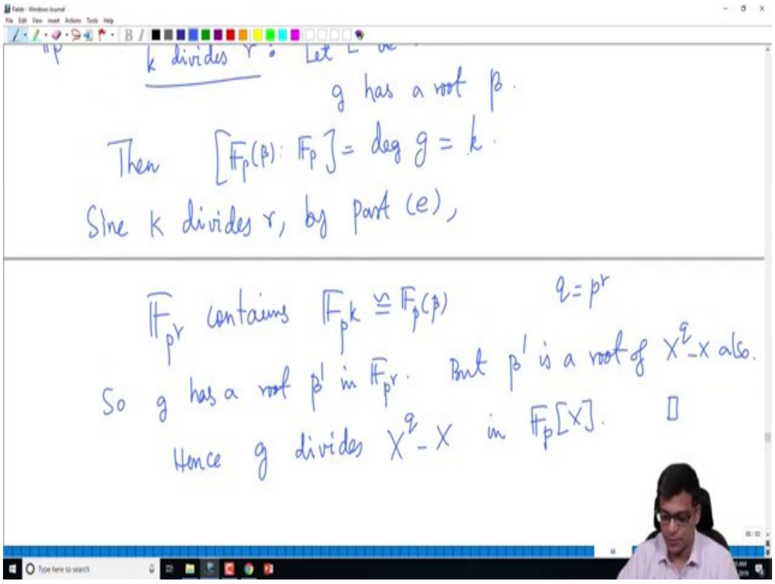
$\Rightarrow$ k divides r.

k divides r: Let L be an extension field of $\mathbb{F}_p$ in which g has a root β.

Then $[\mathbb{F}_p(\beta) : \mathbb{F}_p] = \deg g = k$.

So, now I can actually take a F p beta L. So, now, what is their degree of F p beta by the same reason as before, F b beta over F p is equal to degree of g which is k, so that means, this is k.

(Refer Slide Time: 37:50)



k divides r: Let

g has a root β.

Then $[\mathbb{F}_p(\beta) : \mathbb{F}_p] = \deg g = k$.

Sine k divides r, by part (e),

$\mathbb{F}_{p^r}$ contains $\mathbb{F}_{p^k} \cong \mathbb{F}_p(\beta)$ $\quad q = p^r$

So g has a root β' in $\mathbb{F}_{p^r}$. But β' is a root of $X^q - X$ also.

Hence g divides $X^q - X$ in $\mathbb{F}_p[X]$. $\square$

Now, by the previous part, since we are assuming k divides r by part e, F p power r contains a field which is isomorphic to F p power k by power p right, this is exactly power p. We have shown in part e, if k divides r, F p power r contains F p power k. So, F contains F p power r contains F p power k; which is actually isomorphic to F p beta because F p beta as degree k or this; that means, this is F p power k, right.

Because this is p elements this dimension is k; that means, this is p power k elements. So that means, the corresponding element there is an isomorphism here, this is contained in this in sort of you can put this loosely speaking you can put this line here; that means, you can think of this as a subfield of this. So, because of that, because F p beta can be thought of as a subfield of F p r, g has a root in F p power r.

All we need to do is look at the isomorphism of its sub field and look at the image of beta; that means, it as a root in F p r. But that means, let us say root that root is called b prime in F p r, but b prime is a root of X power q minus X also; because every element of F p power r is the root of X power q minus X where q is p power r.

So, g is irreducible polynomial of beta prime, X power q minus X is another polynomial that has beta prime as a root. Hence, g divides X power q minus X actually in F p X I will say and this is r, last part I will wave my hands. If you have field extension and two polynomials in the smaller field and if one divides the other in the bigger field, it divides in the smaller field also.

Because, the division process does not keep track of which field you are working with, assuming you have started with the polynomials in the same base field, ok. So, that is an aside, but we conclude that g divides X power q minus X. So, if k divides r any and if we have g irreducible polynomial degree k it divides X power q minus X.

So, now let us go back to the statement of the theorem. We showed that irreducible factors of X power q minus X are exactly the irreducible polynomials. So, its degree divides r; because we have shown that any irreducible factor of X power q minus X has a degree dividing r. And we have also shown that if you have any irreducible polynomial whose degree divides r, it divides X power q minus 1, X power q minus x. So, this is done and we before that we have shown e.

So, all the parts are done, so this is the proof of the structure theorem and I admit that I have gone very fast maybe in the last two parts. But, the statements are important and I will do some examples in the next video to illustrate how to apply those results. But, the most important thing to keep in mind is that there exists a field of order q always, any two fields of order are q isomorphic.

And of course, q is p power r that is very important; because if q is not p power r it cannot exist, that we have already shown; only possible finite fields are order p power r. And we have also mentioned that the multiplicative group of any field finite field is a cyclic group of order q minus 1 and elements of field of order q are roots of X power q minus X.

And then we have two statements about subfields of F q and irreducible factors of f: X power q minus X. So, let me stop this video here; this completes the proof of the structure theorem. And also completes the course except that I will do now a video with examples on finite fields. And then I will do one or two videos on problems.

Thank you.