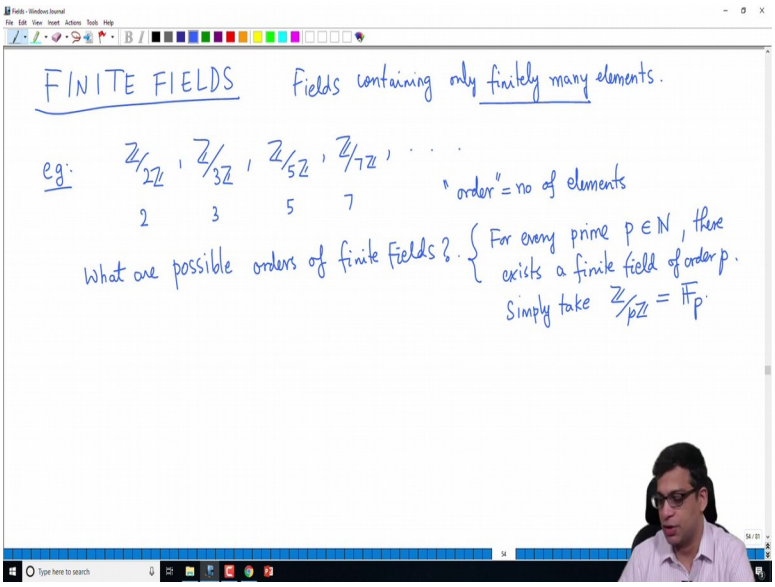
Introduction to Rings and Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 40
Finite fields 1

(Refer Slide Time: 00:17)



Let us continue now, we have so far looked at field extensions, algebraic field extensions, transcendental field extensions, degree of an algebraic element, degree of an extension of fields. And we also looked at how to add roots of a polynomial and we learned about splitting fields. So, now, we come to the final topic of the course which is finite fields. So finite fields are fields which simply are finite sets.

So, these are fields containing only finitely many elements ok. So, in this part of the course which is the final topic, we are going to study these and we will prove a structure theorem for finite fields. So, what are some examples of finite fields that we know. So, for example, we know that Z mod 2 Z is a finite field containing two elements, Z mod 3 Z Z, mod 5 Z, Z mod 7 Z and so on all right.

So, these are clearly fields because 2 Z, 3 Z, 5 Z, 7 Z are maximal ideals of the ring of integers, so when you quotient by them you get a field. And as you observe the order in each case here is a prime number; in fact, you do not get a field if you take Z mod 4 Z

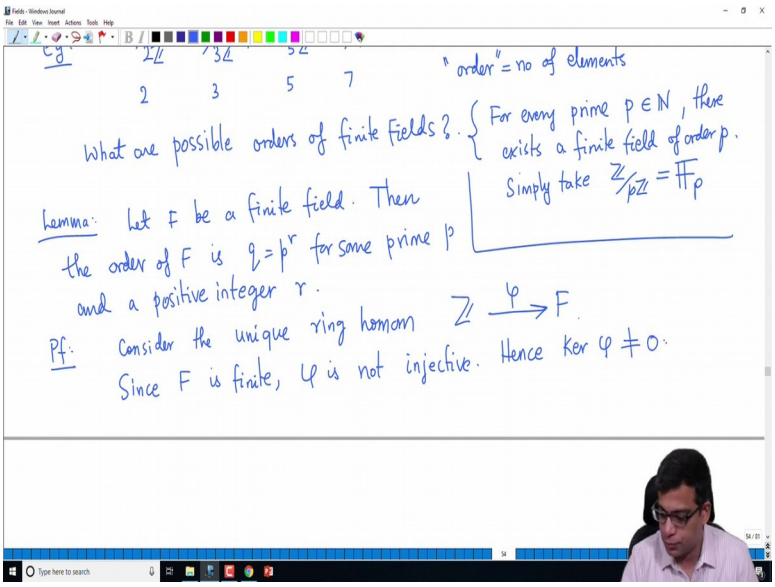
ok. Similarly you do not get a field if you take Z mod 6 Z and so on, so these are the orders.

So, orders of order remember means number of elements, so remember from group theories I am going to use that terminology. Now, that we are talking about finite fields the number of elements is a finite number, so we call that order. So, the first question I want to address is what are possible orders of finite fields.

So, I want to eventually prove a theorem which completely classifies finite fields and tells us a lot about their structure. But, in order to motivate the theorem I want to quickly discuss some examples and some initial observations what are possible orders. So, clearly for every prime p remember prime number when I say prime in this context it is a prime integer there exists a field of finite field of course, of order p.

So, simply take and we will prove as part of this structure theorem that this is the only such field up to isomorphism. So, we can usually because of that we denote this by F p, F written in this bold fashion, so F p stands for the finite field of order p, so certainly for every power we have that.

(Refer Slide Time: 03:39)



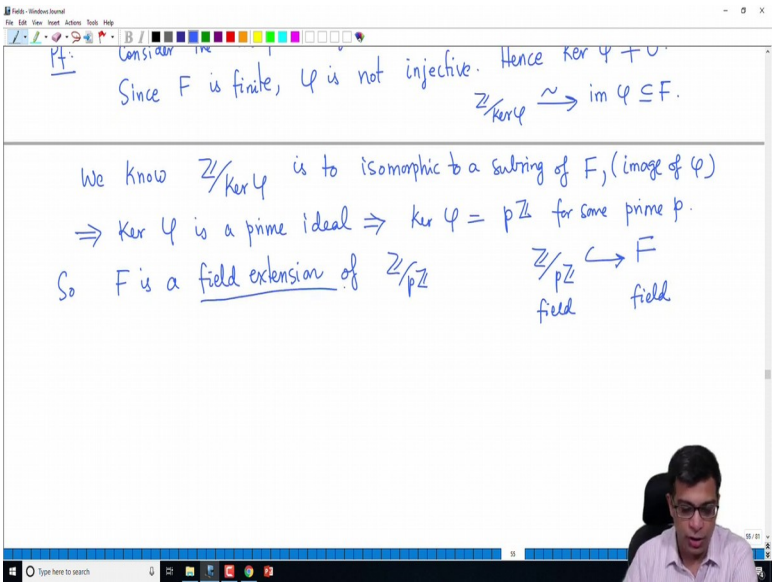
On other hand I will prove small lemma here it says that if F is a finite field, then the order of F is p power r. So, q which is p power r for some prime p and a positive integer r p is of course prime integer. So, the lemma says that if F is a finite field then it is order is a

power of a prime number, it cannot be any other, order of a field cannot be any other number.

So, for example, there can be no field of order 6, because 6 is not the power of a single prime number. So, I will write that after proving this, this is the most standard thing that you learn when you start talking about finite fields, what is a possible order of a finite field, it must be power of a single prime number. So, the proof is very simple: consider the unique ring homomorphism from Z to F. Remember earlier in the ring theory part of the course we showed that for every ring R there is a unique ring homomorphism form Z to R sending 1 to 1.

So, F being a finite field is also a ring, so there is a unique ring homomorphism like this. So, immediately we observe that phi cannot be injective, since F is finite phi is not injective, why not, if phi is injective, Z sits inside F right is the language we will use that, but Z is infinite. So, then F would also be infinite, so F is finite phi cannot be injective, hence kernel of phi is not 0 right not injective means kernel is nonzero.

(Refer Slide Time: 05:53)

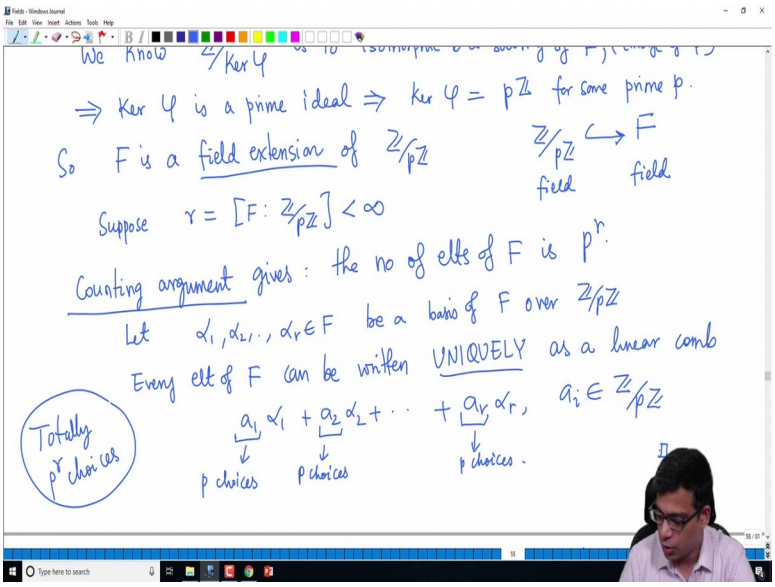


Since kernel of phi is a prime ideal, so note that I will say that we know Z mod kernel phi is isomorphic to a sub ring of F. So, is isomorphic to a sub ring of F, that is the first isomorphism theorem right, so namely the image of F image of phi. So, we have an isomorphism from Z mod kernel phi to image phi which is of course, a sub ring of F, so F is a field any sub ring of F is an integral domain.

So, Z mod kernel phi is an integral domain hence kernel phi is a prime ideal and it is non zero, because capital F is finite. So, kernel phi remember all ideals in Z are multiples of a particular integer n, prime ideals are either the 0 ideal or prime number multiples. Because kernel phi is not zero, it is of the form p Z for some prime p, so the upshot of all this is.

So, F is a field extension of Z mod p Z right, Z mod kernel phi is Z mod p Z is an injective it is sits inside F. Now, this is a field this is a field and what do we call such a situation where we have a field contained in another field that is what we call a field extension, so F is a field extension of Z mod p Z.

(Refer Slide Time: 08:03)



Suppose r equals the degree of this field extension, because F is a finite field the degree of the field extension cannot be infinite right. This is simply the dimension of F as a Z mod p Z module, p Z mod p Z vector space; it certainly cannot be infinite because F itself is a finite, so there is certainly a basis containing finitely many elements, so this is finite.

Now, this is a simple counting formula, counting argument shows that the number of elements of F is p power r as claimed and the reason. So, this I will not do in detail because this is something that you would have seen similar argument you would have seen in other courses. This is because r is the degree of the extension right, so I will give the sketch of the argument, not the full argument.

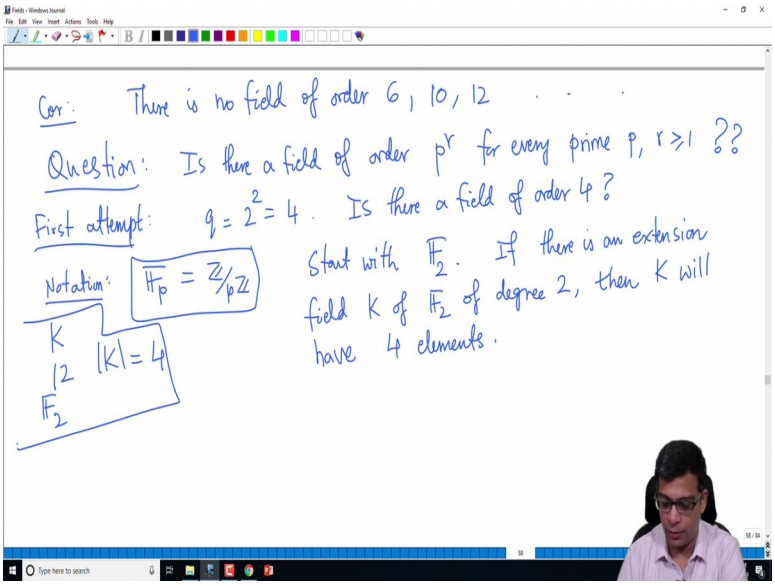
So, let us say v 1 let me use alpha 1, alpha 2, alpha r in F be a basis of F over Z mod p Z ok. If this happens then every element of F can be written uniquely as a linear combination a 1 alpha 1, a 2 alpha 2, a r alpha r right. And where are a i's are in Z mod p Z now this is where the counting comes in.

So, essentially the choices come from how many choices we have for a 1, so these are r choices sorry p choices right. Because, a 1 can be any of the p elements of Z mod p right, similarly you have p choices here similarly you have p choices here. So, totally p times, p times p r times so p power r choices, so the important thing to notices is that each different choice gives a different element that is a consequence of the fact that alpha i's are a basis.

And no two choices can give the same in other words no two choices can give the same element because they are linearly independent, every element of F can be written like that because they span. So that means, they are exactly p power r choices; that means, the number of elements of f is p power r, so the order of F is p power r ok.

So, now, this we have proved this theorem that finite fields can have finite fields can have order sorry I wanted to insert page here. So, finite fields can have only order p power r, so corollary, so I am doing this because I have written that next theorem already.

(Refer Slide Time: 11:29)



So, corollary is as a simple example there is no field of order 6 right there is no field of order 6 there is no field of order 8 sorry order 8 is not a problem. But 10, 12 and so on right, but still this leaves a question the proposition that I proved earlier says that it a finite fields exists it is order cannot be a only of the form p power r but the converse is a true.

Is there a field of order p power r for every prime p and every positive integer r at least 1. So, this is the question that we want to address in this video when we talk about the structure theorem for finite fields. So, as a first attempt, so the answer is going to be yes and much more in fact, is true, but as a first attempt we will observe the following.

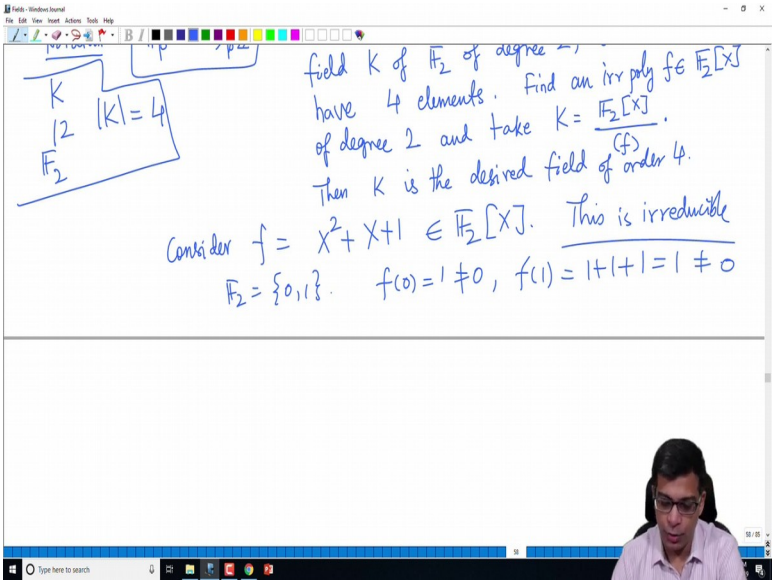
Let us look at q equal to 2 squared which is 4, this is not prohibited right from the lemma, we do not know if there is a field like this or not, but it is not excluded by the lemma, so is there a field of order 4? So, what we do is certainly we cannot at Z mod 4 Z because Z mod 4 Z is not a field, we cannot take Z mod p Z for any prime because Z mod p Z as order p. So, and 4 is not prime.

So, we have to do something new right, we have we cannot use the existing collection of finite fields, so what do we do? So, just the notation here I have already mentioned this before the notation is I will use F p to denote Z mod p Z, and more generally I will use F sub q to denote a field of order q. So, for prime numbers we know they exist, so I have introduced it, we will also prove as part of the structure theorem that any two finite field of the same order are isomorphic.

So, that justifies using the single notation for such fields ok. So, let us take, how do we construct a field like this. We know a method to construct new fields right we can take a field and consider its extension fields by killing irreducible polynomials. So, let us start with Z mod 2 right, so I will call it F 2. So, if there is an extension field K of F 2 degree 2, then K will have 4 elements right.

So, if K is a degree to extension of F 2 then order of K which I will denote by the symbol will be 4 by the argument that I counting argument that I gave in the previous slide ok. Because there is basis of two elements, coefficient of each basis can be any of the two elements of F 2, so there will be two times two many elements.

(Refer Slide Time: 15:09)



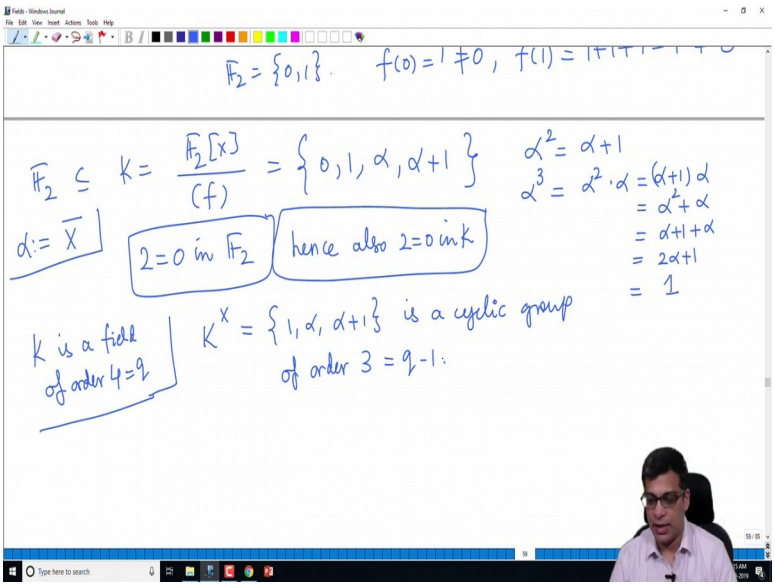
Now, the question is how do we construct a degree two extension? All we need to do is. Find an irreducible polynomial in F 2 X of order 2 of degree 2 and take. So, irreducible polynomial let say F, an irreducible polynomial F in F 2 X of degree 2 and take K to be F 2 X mod F right. That is all we need to do because of everything that we have done so far, F 2 X is a polynomial ring in one variable or a field and as such it is a principal ideal domain.

And if you take an irreducible polynomial the ideal generated by that is a maximal ideal, so when you go modulo that ideal you get a field call it K. So, first of all K is a field, moreover because it is generated by X bar over capital F 2 and small f as degree 2 K colon F 2 will be degree 2. This is something we have shown, the degree of an element is equal to the degree of the extension, so then K is the desired field of order.

So, all we need to do is find such an irreducible polynomial of degree 2, so now how do we if you do that we have a field of order two how do we select such a thing. So, simply take F equals X square plus X plus 1 in F 2 X. So, I claim that this is irreducible; how do we show that this is irreducible, this is very easy, why is that. See if a degree two polynomial verifying that it is irreducible or not is very easy, all we need to check is that it has no roots because if it splits it is not irreducible; that means, it is reducible and it splits then because it is degree 2 factors have to be linear and linear factors correspond to a root.

So, does it have a root or not? There are only two elements right F 2 has two elements, we call them 0 and 1. So, f of 0 is 1 which is not 0 and f of 1 is 1 plus 1 plus 1 what is one plus 1 plus 1 in F 2 that is also 1 right because that is 3 which is 1, so f has no roots, so it is irreducible.

(Refer Slide Time: 17:47)



So, take K to be F 2 X mod f and it is supposed to have four elements, I want to list the four elements like this. So, we have 0 and 1 remember it is going to contain F 2 it is going to contain F 2 the other elements will be alpha remember X square plus X plus 1 is declared to be 0.

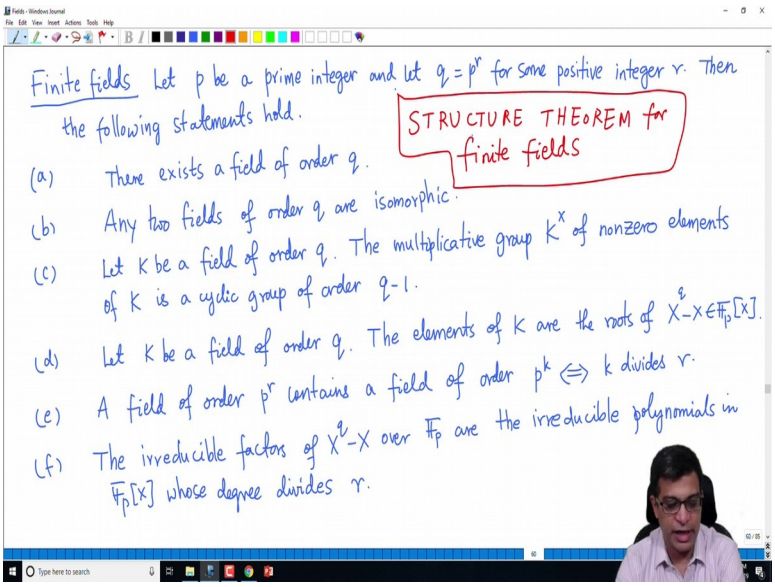
So, you take X bar to be alpha the notation is you call alpha equal to X bar, then you will have X bar X bar plus 2 and that is all. Remember 0 comma 1 comma alpha is a basis and these are all the elements, if you take alpha squared that is already alpha plus 1. So, what I am saying is it alpha squared is alpha plus 1 what is alpha cubed that is alpha plus 1. So, you can write it like this alpha square terms alpha, so that is alpha plus 1 times alpha that is alpha square plus alpha.

And what is alpha squared alpha squared is alpha plus 1, so this alpha plus 1 plus alpha this is 2 alpha plus 1, what is 2 alpha in this field? 2 alpha is actually 0 right. So, 2 is 0 in F 2 that is the crucial point and hence also 2 equal to 0 in K it is an characteristic 2 field characteristic is a term we use for the generator of the kernel of the unique ring map from Z to F 2 in F 2 case it is 2.

So that means, 2 is 0, so this becomes 1, so all powers are alpha are also here similarly you can check the powers of alpha plus one are also here. So, what we know is that K cross which is the nonzero elements of K is actually a cyclic group of order 3, K is a field of order 4, K cross is a field of order.

So, this is q and this is q minus 1 ok, so I am trying to do in this example the structure theorem that I will now state. So, that you see what the theorem says in general and these are very simple example, but it is. In fact, it is illustrative to do this ok. So, now let me, I have already written this let me show to you the statement of structure theorem for finite fields.

(Refer Slide Time: 20:21)

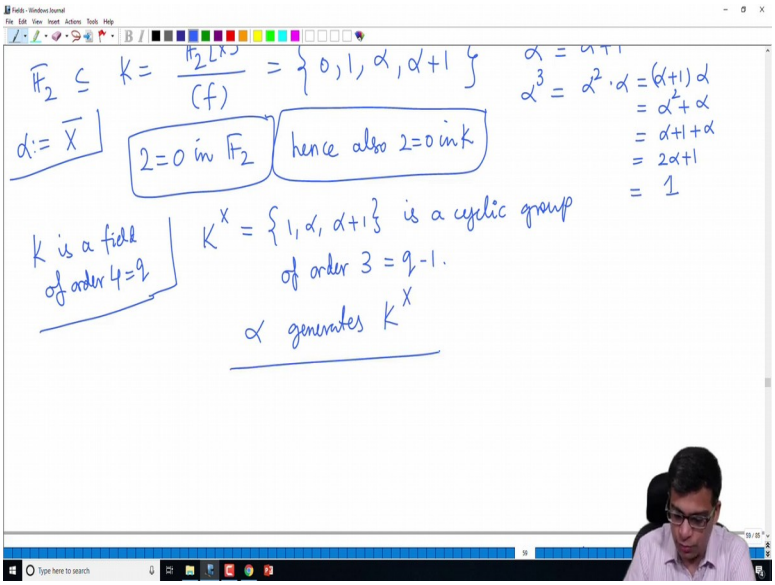


So, this is why I call this structure theorem for finite fields. So, it nicely groups together all the statement that we can prove about finite fields and together they tell us a lot about finite fields. Finite fields are well understood unlike extensions of Q where there is infinitely many elements and there is many things to study, finite fields are sort of completely understood from this theorem.

So, I have already written this to save the time, so let me just read through this if p is a prime number and q is any power of p the first statement is the answer of the question that which stated earlier. Does there exist a field of order p power r for every p and r and the answer is yes, I am fixing an arbitrary prime p and an arbitrary r and taking q to be tp power r.

The first statement is there exists a field of order q, second statement is that any two fields of order q are isomorphic which we will prove. Third statement is that if you take a field of order q and take the multiplicative group of non zero elements certainly it will be a multiplicative group of order q minus 1, but it is in fact, is cyclic group ok, so that is the third statement which remember I illustrated here.

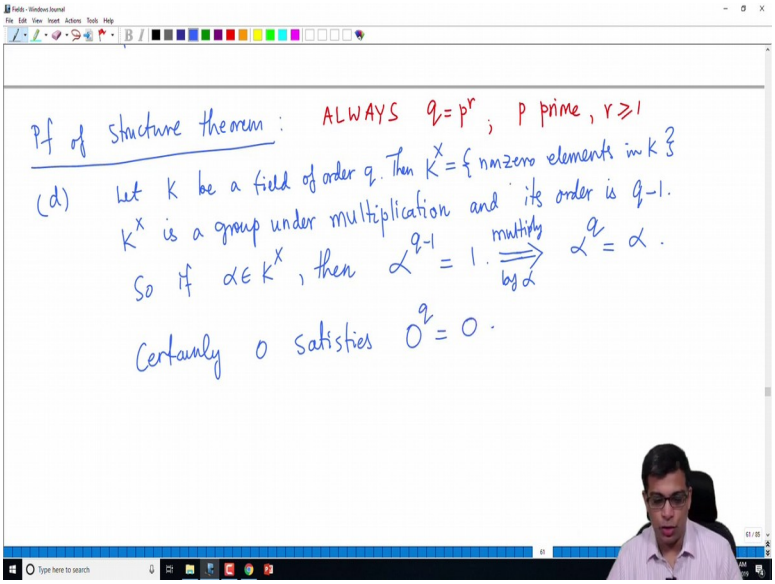
(Refer Slide Time: 21:59)



Here alpha generates k plus k cross, so it is a cyclic group. The fourth statement says that if you have a field of order q the elements of K are actually roots of this particular polynomial X power q minus X, every element satisfies that. And a field of order p power r contains a field a order p power k if and only if k divides r and finally, tells also that the irreducible factors of these are exactly those irreducible polynomials whose degree divides r ok.

So, this may not seem very clear, but we will prove all these statements; I will actually skip some of the proofs because they involves some group theory and some calculations which I would avoid try to avoid, now I will try to sketch the proof of all of them. But, I will quickly finish the proof and I will focus on examples ah, one example we have already done and we want to now prove this I want to prove this structure theorem.

(Refer Slide Time: 23:01)



So, remember in the example that I did before stating the theorem how do we construct a degree 4 order four field extension order 4 field. We started with order two field found a polynomial of degree two which is irreducible and went modulo it. So, now you can see how to construct a field of order 8 all we need to find is a degree 3 polynomial which is irreducible go modulo that.

In general, if you want to construct a field of order 5 power 5 what you do is start with F 5 which is Z mod 5 right, find a polynomial of order degree 5 which is irreducible and go modulo it. Only problem with this approach is that it becomes tricky to exhibit such irreducible polynomial and it is actually not easy, how do you know that there is such an irreducible polynomial and then go modulo that.

So, we will take a different approach and this is an indirect, but easier approach to show the existence. So, I will not prove this in the order in which I wrote in that order because this is a sequence that you should remember, but we will prove it in a different order, so we will prove d first.

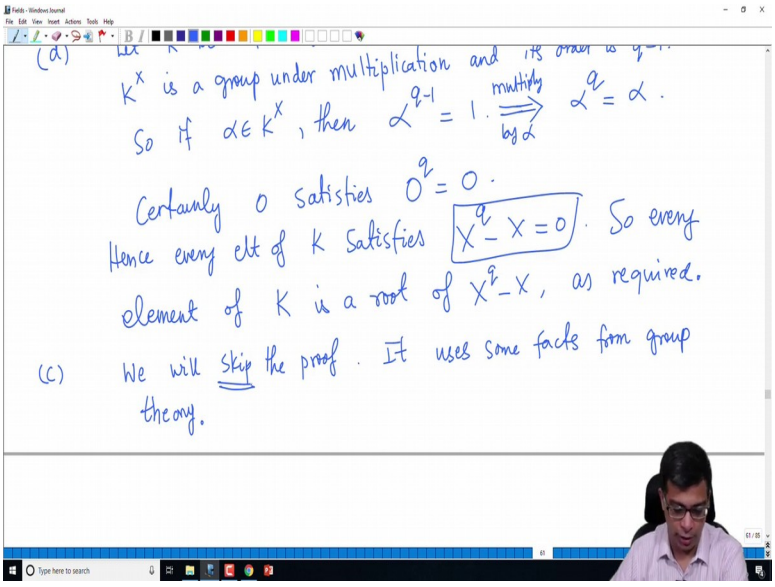
So, I will prove all of this one by one, so let us prove d. So, what is d? (d) says that if you have a field of order q elements are the roots of this, so this is very easy, so let K be a field of order q. So, remember always we will keep this in mind, so I will put it in red always q is equal to p power r p prime r at least 1 ok, so this is the notation q stands for that.

So, let K be a field of order q we will prove later that such a field in fact, exists; let K be a field of order q then K cross let say is the non zero elements of K right. So, this is a group, so by definition of a field is a group under multiplication K cross is a group under multiplication right every non zero element has an inverse.

So, it becomes a group under multiplication and its order is q minus 1, because K has q elements you removed 0, so it has q minus one elements. So, it is a multiplicative group of order K minus 1, q minus 1. So, if alpha belongs to K cross then by Lagrange's theorem alpha power q minus 1 is 1 right, if you have a group of 100 every element has order dividing 100 so; that means, that element power 100 is identity element.

So, alpha power q minus 1 equal to 1, so now if you multiply both sides by alpha you get alpha power q equals alpha right. Multiplied by alpha I am taking this equation and multiplying by alpha both sides alpha power q minus 1 becomes alpha q and 1 becomes alpha.

(Refer Slide Time: 26:37)



So that means, every element of K cross satisfies this, certainly 0 satisfies this right, so now; that means, every element of K satisfies this relation. So, every element of K is a root of X power q minus X as required right this is very simple. So, remember what did I say in d, I said every element of K is a root of X power q minus X which is of course, a polynomial in F q F p remember, because the coefficients are one and minus one which are in F p.

So, this is true, so d is done, so what I am going to now do is c ah; in fact, I will not prove c, so we will skip the proof of c, c says that the non zero elements of K which form a multiplicative group of order q minus 1. In fact, is a cyclic group this is an important statement that we will use later, but we will skip this it uses some facts.

So, this is really a group theory statement, it uses some facts on group theory; one way that you can prove this is using something called the structure theorem for finite abelian groups. So, it takes me away from what I want to do and I do not want to spend time on that. So, I will skip the proof you can read this proof in any book for example, Artin's Algebra is what I am using clearly proves this.

So, you can read the proofs it is not a difficult proof at all, but it uses some group theory which I want to avoid. So, we will skip the proof of c which is that every the multiplicative group of non zero elements of K is a cyclic group of order q minus 1. So, let me stop this video here; in the next video we will continue the proof and finish the proof and then do some examples.

Thank you.