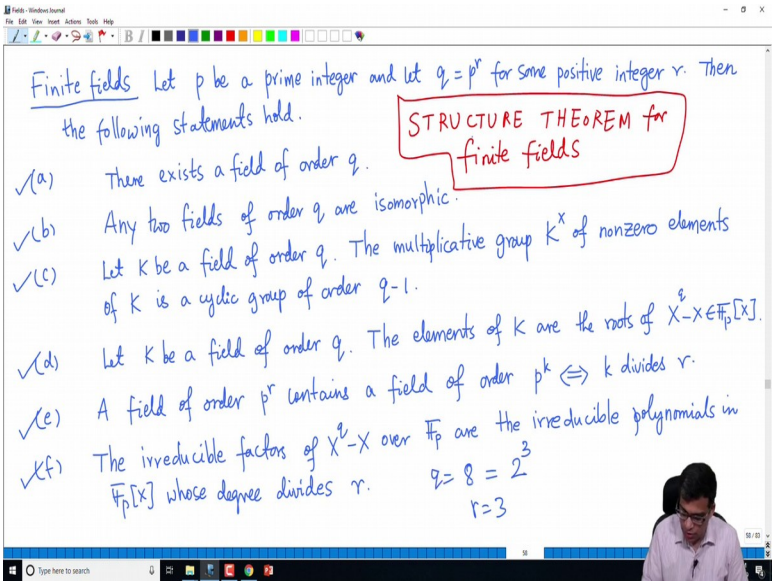
**Introduction to Rings and Fields**
**Prof. Krishna Hanumanthu**
**Department of Mathematics**
**Chennai Mathematical Institute**

**Lecture - 42**
**Finite fields 3**

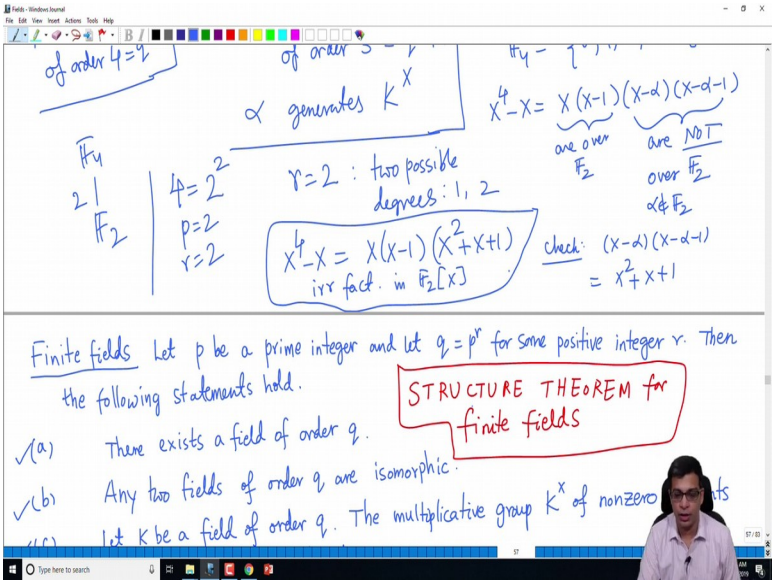
(Refer Slide Time: 00:16)




In this video I want to give some examples of Finite Fields and illustrate the structure theorem that we proved in the last couple of videos. So, here is the structure theorem for you and as I said this is the most important result that you need to know about finite fields.

So, we have proved each statement in fact, we did not prove one of these statements, I simply said c follows from a group theory fact which I did not do. And e and f, I went somewhat fast, but hopefully overall it is clear to you. So, what I want to do now in this video is to illustrate these results with some examples ok, we did one example. So, I will actually talk about this example where we constructed a field of order four right.

(Refer Slide Time: 00:58)




So, in this example we constructed F 4 which I denoted like this, so this is F 4 right, so I will just use the same slide here to illustrate this. So, just to illustrate all the facts that we have proved here it is a field of order 4 it has 4 elements and everything satisfies this polynomial.

So, in fact this polynomial splits completely like this right, so this is not surprising, every element of F 4 by this part d here is a root of X power q minus X in this case q is 4. So, it is a root of X power 4 minus X, it has four distinct roots we observed in the proof in the 4 distinct roots are this. And if you try to draw the extension diagram it is degree 2 there is nothing in between.

So, the statement about subfields does not apply here, but if you take the statements about irreducible factors we can say something interesting. This remember these are over F 2, these of course, are not over F 2, because alpha is not in F 2. So, the irreducible factors of X power 4 minus X over F 2 are the irreducible polynomials in F 2 who's degree divides r.

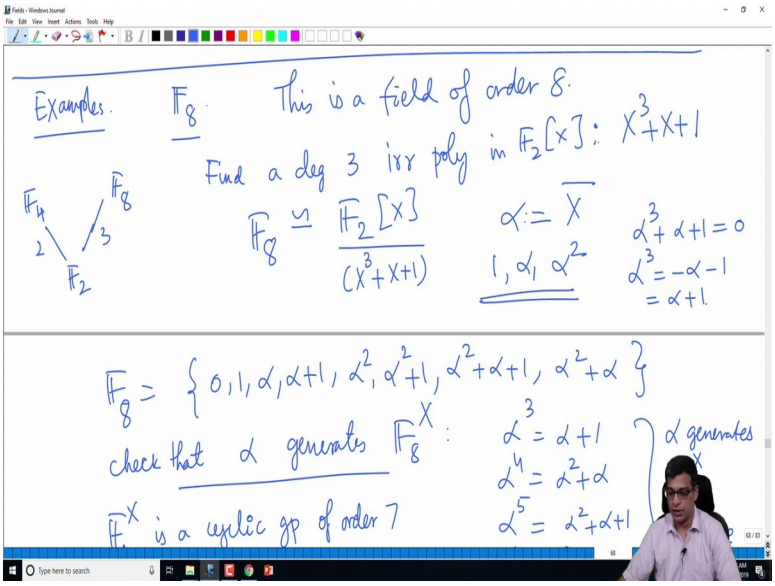
So, in this case r is 2 right, so because 4 is 2 squared remember p is 2 here r is the exponent which is also 2. So, we are looking for irreducible factors whose degree divides 2, there are two possible degrees right, so what are the numbers that divided to 1 and 2. So, X power 4 minus X can be written as X which is the degree one term another degree one

term X minus 1 and actually you have to multiply these X squared plus X plus 1 which we know is irreducible.

In fact, we went modulo that polynomial right f was X squared plus X plus 1 ok. So, that is the irreducible factorization, clearly if you check these as an exercise, if you multiply X minus alpha and X minus alpha minus 1 you get X squared plus X plus 1 which is irreducible over F 2 x. So, this is the factorization in F 2 X ok, so that is what I should say.

It conforms the last part of the structure theorem: irreducible factors are those that have degrees that divide two in this example. So, it cannot have 3 for example, there cannot be a factor of degree 3, because 3 does not divide 4 or 3 does not divide two ok. So, now, let me do some other examples to illustrate this theorem more carefully, so more examples.

(Refer Slide Time: 04:13)



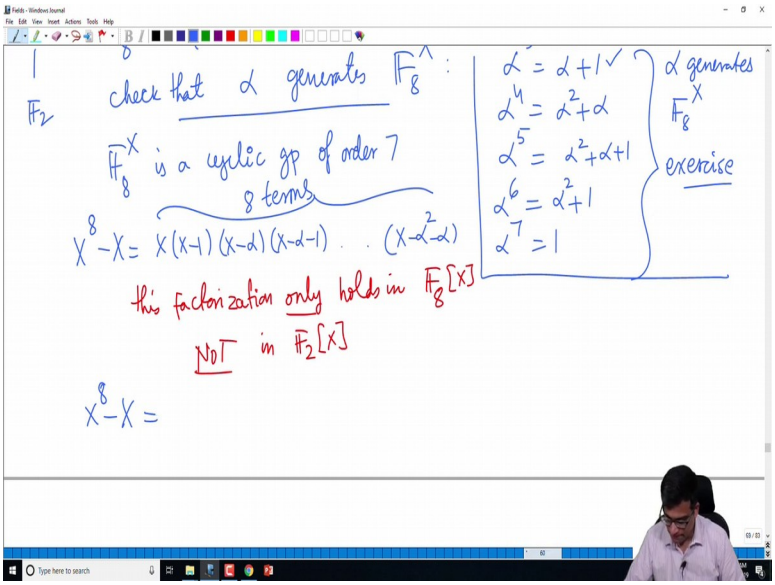

So, I am going to study F 8 right, this is a field of order 8, we know from the theorem that such a field exists and any two fields of order 8 right are isomorphic. So, in fact, I will write this as F 2 cubed and it will contain F it is degree 3, so it will not contain any other field in the middle because no other number divides 3 other than 1 and 3.

And if you want to understand where F 4 fits into this picture you have F 4 here and F 8 is not comparable to this is 2 this is 3, there is no containment result between F 4 and F 8 ok. So, I am going to do another example after discussing this where I draw this picture of subfields for a given field.

So, then you will understand this more, but let us think about what we have to do here and let us try to not go through the irreducible polynomial part via that root, but use the proof of the structure theorem. So, here we have, in fact, ok, so to actually understand the elements we need to get hold of a degree 3 irreducible polynomial in F 2 X ok.

So, it is very easy to check for example, that that is given by X 2 plus X plus 1 this has no root 0 is not a root of this. Because, 0 plus 0 plus 1 is 0, 1 is not a root of this because 0 plus 0 plus 1 is 1 which is not 0, 1 plus 1 plus 1 is 1 which is not 0. This is irreducible and F 8 will be actually equal to F 2 X modulo X square plus X plus 1.

(Refer Slide Time: 06:21)




So, if you as before declare alpha to be X bar there will be 8 elements remember; there will be 8 elements which correspond to how you put coefficients in front of these three basis elements. So, I am going to just list them in some order you will have 1, 0, 1, alpha, alpha plus 1. So, I will just follow the way I have written this, alpha squared, alpha squared plus 1 alpha squared plus alpha plus 1 alpha squared plus alpha.

So, let see 1, 2, 3, 4, 5, 6, 7, 8; 1, 2, 3, 4, 5, 6, 7, 8, 8 elements right these are all distinct elements remember these are given by putting one of the two possible coefficients in front of 1. Similarly, one of the two possible coefficients in front of alpha one of the two possible coefficients in front of alpha squared, one can check here that check that alpha generates actually F 8 cross ok.

Because I have, you can check here alpha squared is there already, alpha cubed is alpha plus 1. You can check that alpha power 4 is alpha squared plus alpha, alpha power 5 is alpha squared plus alpha plus 1, alpha power 6 is alpha squared plus 1 ok, and alpha 7 will be 1. So, F 8 cross remember is a cyclic group our theorem tells us this, but you can actually verify that alpha generates F 8 cross it is order 7 ok.

So, this verification I will leave this for you as an exercise, this is easy right, we know that alpha this is something is wrong here it is not X squared, but I put X cubed. So, we know that alpha cubed plus alpha plus 1 is 0; that means, alpha cubed is minus alpha minus 1; that means, it is actually equal to alpha plus 1 because minus alpha is alpha minus 1 is 1.

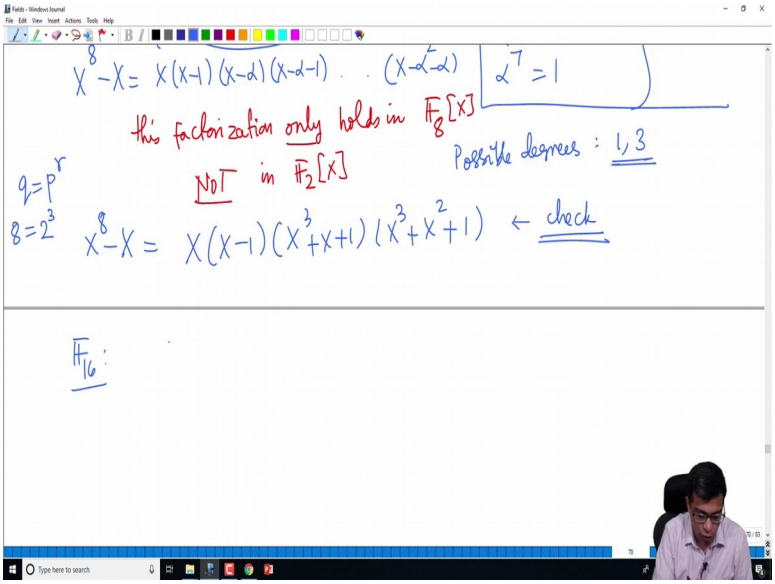
So, using that reduction you can write down all other things, so it is a cyclic group of order 7. So, this also tells us that X power 8 minus X actually splits completely in F 8; splits completely in F 8, it is X into X minus 1 into X minus alpha into X minus alpha minus 1 and so on.

So, the last will be X minus alpha squared minus alpha right, so there will be these 8 terms. One corresponding to each of these elements X minus 0, X minus 1, X minus alpha, X minus alpha minus 1, X minus alpha squared and so on all the way after this.

This is a factorization remember this factorization only holds in F 8 X not in F 2 X, because remember alpha squared all these elements are not in F 2 X. So, how do you actually find the factorization in F 2 X this is where we have to use the theorem.

The structure theorem said, the irreducible factors of alpha X power 8 minus X you take q to be 8 are the irreducible polynomials in F 2 whose degree divides r, here 8 is 2 power 3, so r is 3, q is 8 ok. So, I will just write I will erase this, but here we are looking at r equal to 3.

(Refer Slide Time: 10:27)

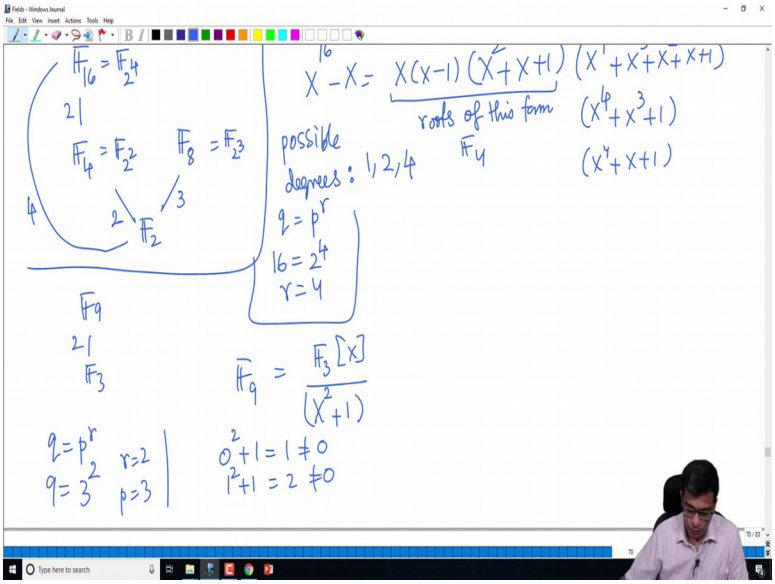



So, we are looking at irreducible polynomial whose degree divides 3, so possible degrees are 1 and 3 the only numbers are divide 2 or 3 or 1 and 3. So; in fact, the factorization turns out to be X times X minus 1 will always be there that corresponds to the 2 factors that already exist in F 2 X.

But, the other ones will be the polynomial that we went modulo, so it will be X cubed plus X plus 1 and you can also check that it is X cubed plus X squared plus 1 ok. So, check this works this is the irreducible factorization, only irreducible factors are those of degree dividing r, so in this case r is 3.

So, r must divide degree must divide 3, so; that means, only 1 and 3 are possible. So, I will just do one more example couple of more examples illustrating this, so let us look at F sixteen, so this is degree 4 polynomial that we have to take and this has order 4.

(Refer Slide Time: 11:37)



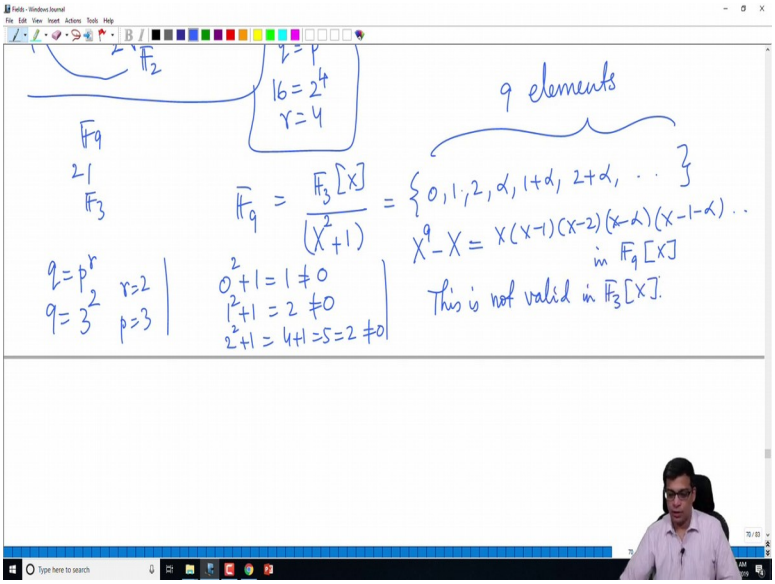

So, if you take F 16 things get a little more interesting, because this is F 2 power 4 this does contain F 2 squared right. Because, one of the statements of the structure theorem is that F ok, so maybe I will just refer to that. So, F p power r contains F p power k if and only if k divides r, so in our situation F 2 power 4 contains F 2 power 2, but it does not contain F 2 power 3 ok.

So, this is a field about, this is a field of this, but there is a tower like this ok. So, in this if you take X power 16 minus X, how do you factor this here possible degrees are because here r equal to, so 16 equals 2 power 4, so r equal to 4 right. So, possible degrees are things that divide 4; that means, 1, 2, 4.

And a simple calculation will tell you that the factorization we are looking for is there will be degree 2 terms, degree one polynomials there is a degree 2 polynomial remember that captures F 4 the roots of these. So far what I have written the degree 4 part roots here of this form the F 4 that is contained in F 16.

But then you will have some other terms and those other terms will be all degree 4, because it cannot be degree 3 there is only degree 1 degree 2. So, the remaining things are all degree 4 and I have computed this; this is what it looks like. So, I will write it down and you can check this, X 4 X cubed plus 1, X 4 plus X plus 1 ok, so this is a factorization again illustrating the last part of the structure theorem.

(Refer Slide Time: 13:55)




So, now one more example, let us look at F 9, so here q is 9; that means, 9 is 3 squared, so r is 2 and p is 3. So, F 9 is a degree 2 extension of F 3, so also I should finish this put numbers here. So, this is a degree 3 extension F 8 of F 2, this is a degree 2 extension this is another degree 2 extension and this is a degree 4 extension as we know also confirmed by the multiplicativity of degrees ok.

So, here we can actually write down all the elements and if you look at one, so F 9 in fact, can be computed as F 3 X. Here we have to take F start with F 3 and X cubed plus X plus 1 is the polynomial which is irreducible.

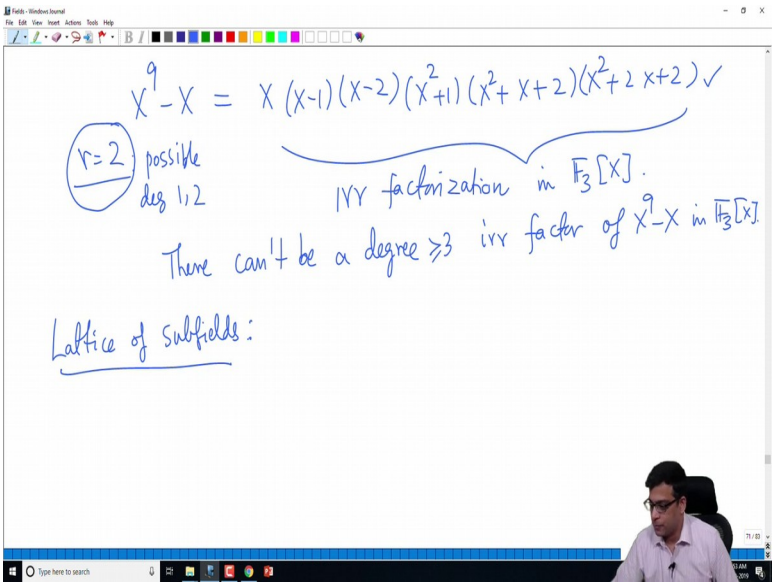
See to even for a degree 3 polynomial the trick of finding roots will tell us it is irreducible or not, because if a degree 3 polynomial is not irreducible it factors as a product of 2 smaller degree polynomials. One of them must be degree 1 at least, because you cannot have all degree 2s right because then it will add up to at least 4.

So, a polynomial of degree 3 is irreducible if it has no roots and F 3 has 3 elements 0, 1 and 2, 0 cubed plus 0 plus 1 is not 0, 1 cubed plus 1 plus 1 is actually 0. So, I should take here 2 right, because sorry actually I am sorry I have to take X squared plus 1 maybe I should take this that is one possibility. I wrote it wrongly X squared plus 1 I claim is a irreducible polynomial, because yes.

So, what are the roots possible roots 0 squared plus 1 is 1 which is not 0, 1 squared plus 1 is 2 which is non 0, and if you do 2 squared 2 is minus 1 actually. So, 2 squared plus 1 is 4 plus 1 which is 5 which is 2 which is non 0. So, this will for example, give you a polynomial which is irreducible and you can factor that and write that as a field of degree order 9 and it is elements can be written as 0, 1, 2 alpha. Here, 1 comma alpha will be basis, so it will be alpha square will be 2, so 1 plus alpha 2 plus alpha and so on.

So, I will not write all the 9 elements; there will be 9 elements. The interesting thing is how to factor X power 9 minus X; X power 9 minus X in F 9 will be X, X minus 1, X minus 2 and so on. X minus alpha, X minus 1 minus alpha and so on, in F 9 X. Because elements of F 9 are roots of X power 9 minus X there are 9 of them. So, it completely splits whereas, this is not the factorization in this is not valid in F 3 X ok.

(Refer Slide Time: 17:35)



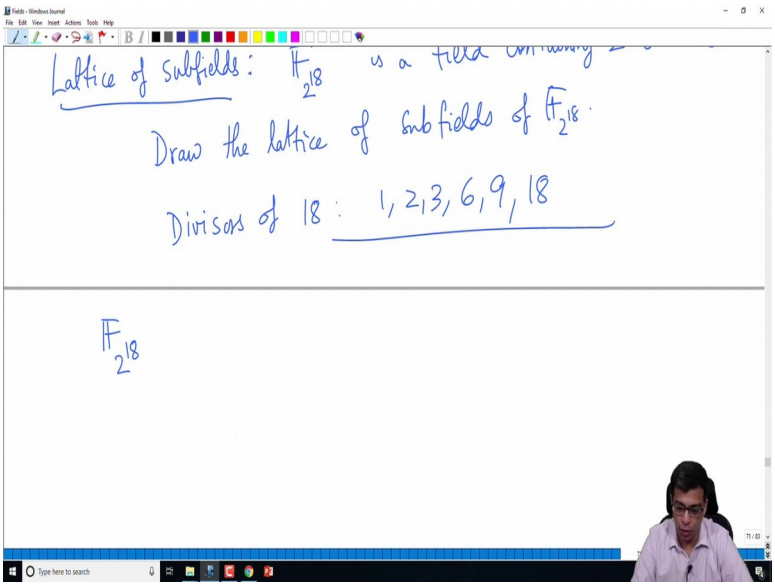

So, what is the correct factorization? Here remember the irreducible factors must have degrees dividing r which is 2, so here possible degrees are 1 and 2. So, we have X, X minus 1, X minus 2 these are linear factors coming from F 3 itself and the remaining things are all degree 1.

One of them is the one we started with there will be another sorry remaining ones are degree 2 it will be X squared plus X plus 2 and X squared plus 2 X plus 2 one can check that these are all irreducible. So, this is the irreducible factorization in F 3 X, the only possible irreducible factors of X power 9 minus X have degree 3.

We know that because by the structure theorem the factors of X power 9 minus X have degrees which divide 2 in this situation. So, there cannot in particular be, so as a separate consequence there cannot be a degree 4 factor irreducible factor or degree greater than or equal to 3 factor of X power 9 X power X minus 9 in F 3 X. This is another way of saying this, every factor is either degree 1 or 2, so this is the factorization.

So, this illustrates mainly the last part of the structure theorem which is proved maybe somewhat quickly and I hope the examples illustrated that statement. Now, I am going to do one more example to illustrate the subfields of a given finite field. So, tower of fields or it is called lattice of subfields ok, so let me illustrate this by drawing some lattices.

(Refer Slide Time: 19:47)

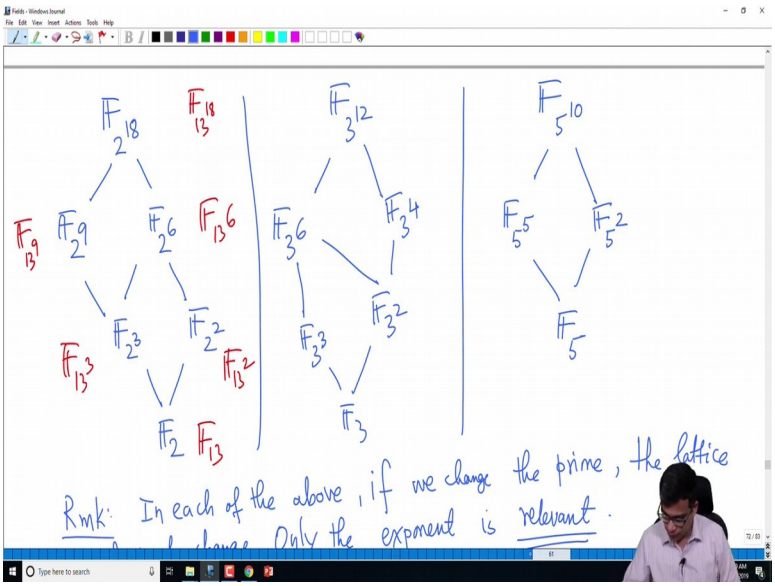



So, for example, if you take F 2 power 18 ok, so this is a field containing 2 power 18 elements, so right this is a large huge number right it is a very big field. Draw the lattice of subfields of this, so I am going to appeal to the structure theorem, the part of the structure theorem with said F subfield of p power r contains of field of p power k.

Remember p must be same clearly you cannot contain a different p because they are all above Z mod p Z. So, p must be same, but exponents also have a relation r must be divisible by k, so here we are taking 2 power 18. So, we are looking for 2 power k where k divides 18, so what are the numbers that divide 18. So, I am going to draw here, so let me start with this, so F 2 power 18 at the bottom we have to have F 2.

But what are the divisors of 18, so let me write that here we are interested in divisors of remember the divisors of the exponent or what we are looking for divisors of 18 are 1, 2, 3, 9, 6, 9, 18 right. So, all fields F 2 power 1, F 2 power 2, F 2 power 3, F 2 power 6, F 2 power 9, F 2 power 18 or going to appear in this lattice.

(Refer Slide Time: 21:31)




So, let us do F 2 power 9 here, because 9 divides eighteen this is a valid subfield of that. Whereas, if you do F 2 power 6 that is a valid of field, but 9 and 6 are not comparable, because 6 does not divide 9. On the other hand 3 divides both 9 and 6, so that is F 2 F 2 cube will be in both of them. Whereas, F 2 squared will be in this, but not in this hence not in this right, it will be in F 2 power 18 this is the fields that we considered already F 8, F 4 and of course, these are both in F 2.

So, this is a lattice of fields right 2 power 16, 9, 6, 3, 2, 2 ok, what about I will look at some other examples 3 power 12. So, what is, what are the divisors of 12? Divisors of 12 are 1, 2, 3, 4, 6 and 12 ok. So, you have F 3 power 6 here, also 3 squared we will be contained here also, so let me write like this 3 cubed will be contained here because 3 divides 6.

And there will be another subfield 3 squared 2 divide 6, 3 divide 6, but 2 and 3 are not comparable. On the other hand you will have 4 here and 4 will be contained in this, but this will these this side of the lattice is not comparable to this and at the bottom we have F 3 right, so I hope this makes sense to you. So, 3 power 3 is contained in 3 power 6, but

3 power 3 is not contained in 3 power 4, 3 squared is contained in 3 power 6 as well as 3 power 4, but not in 3 power 3 and everything is about 12.

And I am just randomly choosing primes here; if 2 is replaced by any other prime that lattice does not change because only the exponents are relevant here the prime itself is not relevant. So, for example, if you take F, F 5 power 10 and has factors 1, 2, 5 and 10.

So, here I get F 5 power 5, F 5 power 2 and there is no other factor, so this is just F 5. So, important remark in each of the above, if we replaced the prime if we change the prime, the lattice does not change, only the exponent is relevant.

So, what I am saying is that here 18 is the relevant number, so if you instead of 2 you have 3 or any other prime 13 power 18 everything will go through it will be F 13 power 9 here. Here it will be F 13 power 6, here it will be F 13 power 3, here it will be F 13 power 2, and here it will be F 13, what the prime is irrelevant.

Because the crucial statement of as long as of course, you keep the prime same if you equal to thirteen here and 2 here prime is the same. Whereas, if you change 18 the whole thing changes, in the crucial structure theorem statement a field of order p power r contains a field of p power k if and only if k divides r. As long as p is the same r and k are the only relevant numbers, so here we can without changing anything replace 2 by a different prime, here replace 3 by a different prime, replace 5 by a different prime.

Then, exponent is a crucial thing to determine completely the lattice ok, so this is our, some of the examples I wanted to do to illustrate the structure theorem. The especially the last 2 parts which were important in understanding the lattice of subfields or the irreducible factorization of the polynomial X power q minus X.

So, I am going to stop the video here, and this completes the course I will just do one or two more videos solving some exercises on fields. But, let me the main part of the course stops here; in this course we have studied rings and fields. This is really a very, it is supposed to be a first course, we covered some standard topics that are covered in a first course.

It goes without saying that there are so many, there are lots of topics that I have not touched on in ring theory as well as in field theory, for example. I did not talk about

primitive extensions, Galois Theory and so on. So, these are all covered in a second course in field theory in rings also we did not talk about factorization of rings and Euclidean domains and so on.

These are some of the topics that we have not covered, but my goal in this course in this 8 week course was just to give you an introduction to the theory of rings and fields and illustrate how one solves problems in these topics. So, I hope you enjoyed the course and you should solve all the exercises that I have been giving in the class.

And ask questions in the discussion forum to understand the material better and carefully watch the videos if you have any questions. And remember again I will stress this fact this is only a first course, if you really want to understand ring theory and field theory better there are courses that you can take as follow ups to this.

Let me stop the video here; in this video we did examples to illustrate the structure theorem for finite fields. And this completes the main part of the course, in the next one or two videos we will do some exercises.

Thank you.