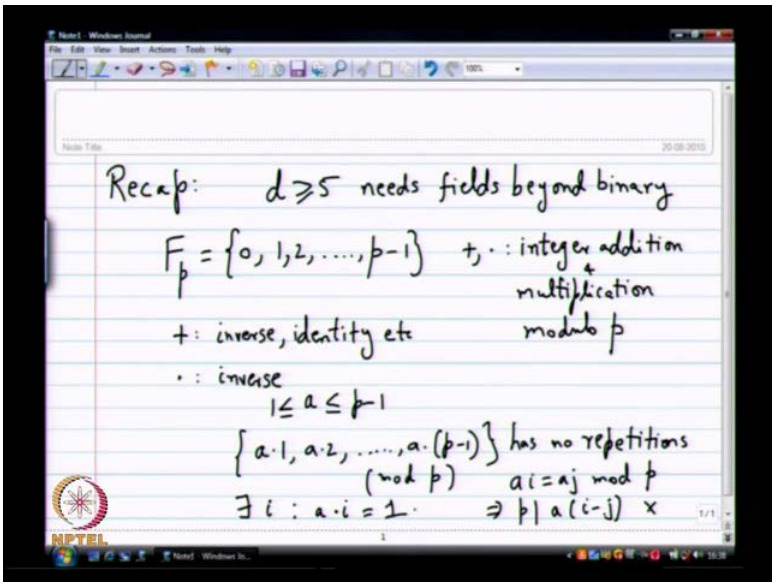
Coding Theory
Prof. Dr. Andrew Thangaraj
Department of Electronics and Communication Engineering
Indian Institute of Technology, Madras

Lecture - 9
Construction of Finite Fields

(Refer Slide Time: 00:19)



So, brief recap what we have been doing the last class. So, like I pointed out, if you want to get good codes with d greater than i equal to 5, you need to go beyond needs fields, beyond binary. So, that is the first observation and I just told you and you believed me I did not prove it or anything just said it is not very easy to design for d greater than i or equal to 5 and finite fields of size larger than 2 give you a very nice solution. That was the motivation, so we wanted to see if there are fields which are finite.

Then, they are larger than 2 first of all why are we interested in fields because we want to design linear codes which means we want to talk about linear combinations row space column space an all that. So, naturally we have a field you know I mean we have we want to look at vector space and a vector sub space. So, we need a field and that field has to be finite why we should we give finite, only then you can represent it bits, otherwise if it is in finite like real numbers and all that. Then this when you cannot represent it with bits very easily so finite fields make a lot of sense from that point of view so only finite field that we saw.

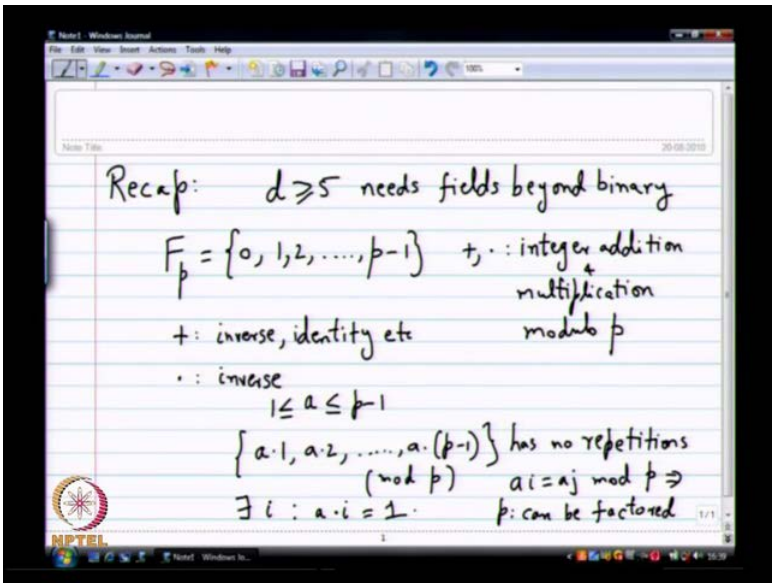
So, this is s p what is this s p contains the set 0, 1, 2 so on until p minus 1 and addition and multiplication are integer addition and multiplication modulo p k. So, I can give you some simple examples for how this works, but I am assuming here reasonably familiar what I mean by modulo p. So, when I do modulo p, I am going to divide by p and take the remainder, so I multiply two things, if it goes outside of this set what will I do divide by p and take the remainder and come back to the set.

So, that is how we do the field operations and it is easy to show what the things that are easy to show for addition properties are easy to show. So, you can show inverse and identity quite, I mean identity etcetera all this properties can be shown quite easily for the multiplication inverse is a little bit tricky and I had an argument towards the end of last class.

Basic idea is if you any a, which is between 1 and p minus 1 and then you look at the set a times one a times 2, so until a times p minus 1 there are no other repetitions. So, basically this set as no other petitions this modulo p of course remember it is all modulo p k. I am using the same dot as no other repetitions all of them are non zero, they lie between 1 and p minus 1 and there are no other repetition which means clearly there exists i such that a dot i equals 1. So, there are no quick argument for saying why this has to work why cannot there be repetitions for instance if a i equals a j mod p.

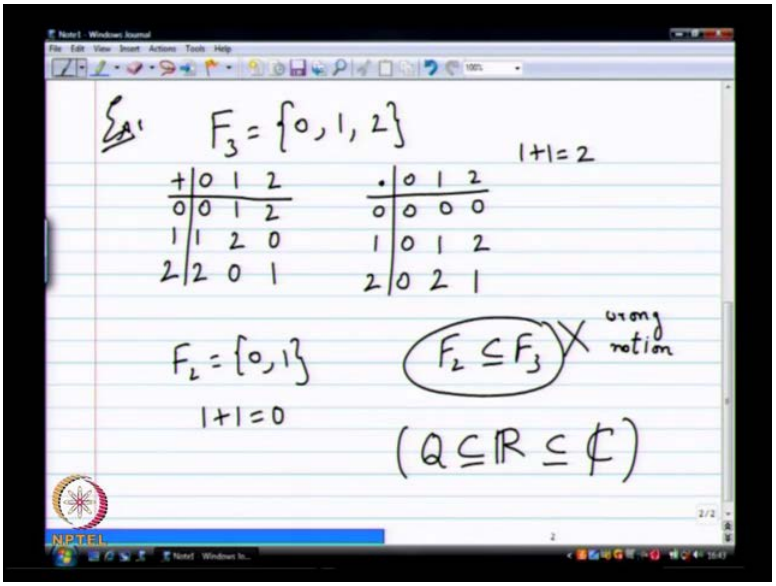
So, then you that some fact k, so either so you get this will implies p divides a into i minus j and that cannot happen in all means. Sometime like that, so though it is a quick end dirty argument, I guess is not correct. So, if this were to happen see re remember both i minus j and a are less than p and product has to be 0 modulo p which means only way it can happen if p is p factors since p is not it is factor this cannot happen.

(Refer Slide Time: 04:42)



So, this will implies p factors so let me just simply write that that way, so this implies p can be factor if you look at this cases carefully and make this argument rigorous, but like I said cannot study of infinite fields. We would not see too many proofs that we were rigorously write down, I will quickly give you an idea why it works. There are several books which you can look up which will do good job of writing down the proof preciously this s the way it works, so F p becomes a field.

(Refer Slide Time: 05:30)



So, you can see you can see few examples if you like of these, I do not thing added any example in the previous class, but you can see you can see a few example of instance F 3 contains three elements 0, 1 and 2. If you want to show how the addition operation works you can make an interesting looking table put 0, 1, 2, 0, 1, 2 here then show how the addition operation works. So, modulo to this is how the additional operation work then if you want to show how the dot operation work once again you have to do 0, 1, 2, 0, 1, 2.

So, anything multiplied by 0 will give you 0, you can show that in any field that is true if you have the additive identity you multiply any non zero number with the additive identity you will get 0. These things can be proved by using the axioms one, I guess it is this simply clear why you are calling it 0, you are calling it 0 because when you multiply everything becomes 0, so this is one this is 2, so 2 and this is 1.

So, all the properties are all the properties, that we were talking about works out this is how the addition operation looks. You can write similar fields similar tables for the other fields if you like F 5, F 7 just look at a little bit more complicated this is easiest one. So, other example that we saw was of course F 2 which was 0 1, so when you essentially see this see this fields that is some kind of inclusion I was saying you have to do the think about one field is containing another field. It is very tempting to say F 2 is contained in F 3, so I said that is true, but in real in actual nature it is not true.

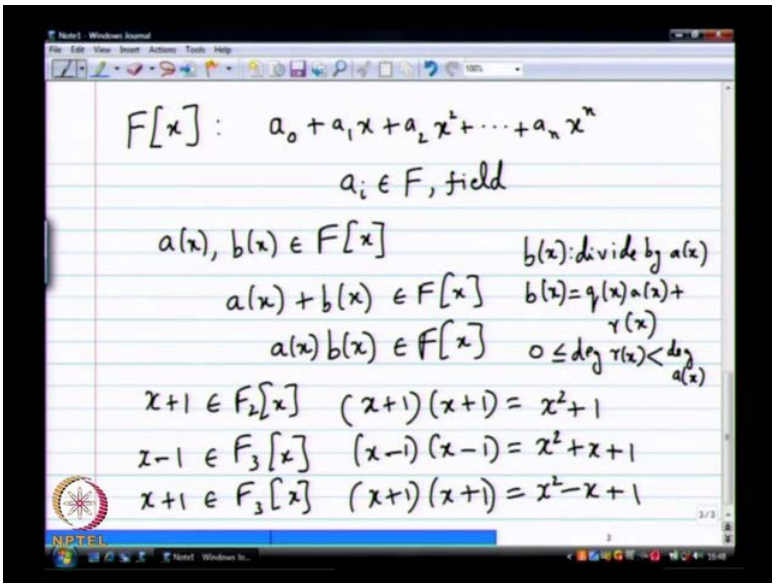
So, why is not true see the one in F 2 is very different from the one and F 3, so I wanted to think about that for a while and then I will tell you why that is true. So, you cannot think of F 2 as being subset of F 3 these is a wrong notion the set zero one of course you can imagine the integers of subset 0, 1 definitely is contained in the integers sub set 0, 1, 2 as long as you are thinking of integer addition all that is fine. When I say F 2, I assuming addition modulo 2, when I say F 3, I am assuming additional modulo 2, so the operations are different and that makes the elements also different for instance in F 2 what would happen to 1 plus some you get 0 in F 3 1 plus 1 is 2.

So, clearly the one has a very tricky different behavior 1 plus 1 becomes the additive identity of F 2 1 plus 1 clearly is not additive identity in F 3 1 plus 1 plus 1 would be what the additive identity so, you should not think as inclusion this if you think as inclusion. So, the in other fields that you might be familiar with, we always write q in contained in R, this is the rational numbers are contained in real and operations are all

similar the when rational numbers act exactly has they suppose to even within the real numbers.

We can also say the other inclusion you can also include the complexes and would be a valid field kind of inclusion because the operations are respect. So, this inclusion is dangerous, so it is it is wrong notion to have and you should know the difference that is a F p it turns out that there are also other finite fields F p is not only the finite fields. You can have F p power m for any m you can have F p power m we will see the construction soon enough in this lecture, but before that we need this idea of polynomials with coefficient from some filed.

(Refer Slide Time: 10:02)



So, I did introduce it in last class, but I want to go through it once again we will denote by F x polynomial of this kind, a 0 plus a 1 x plus a 2 x square, so unit a n x power m what all this a i belongs to f which is of course the field. So, this is set of polynomial in filed f, so once you have for instance a f x and b of x in the field you can do several operations with them the first operation which is the easiest of course addition. You can do this also belongs to F x, I am assuming in how to do addition, so you look at the light powers and simply add the coefficients, but here the additional should be in the in the fields.

So, do not simple day modulo p because it should be the additional operation in the field it could be some other operation. I do not know, now it is modulo p in most cases it will

be modulo some prime number, but in general, I mean in abstract way, you have to think of it as the additional operation being in the field. You can also do multiplication a of x times b of x this is also something which belongs to the set of polynomial with coefficients from f right and I am assuming you know how to do multiplication.

So, it is you have multiply by term by term it is very easy to define it is the same multiplication you have done for the polynomial all are long, but over again what will change the coefficient you have to multiply using the multiplication in the field f. Then when you add you should also add using multiplication in the field f, so various things can change drastically in this multiplication. I will give a simple example, suppose you look at x plus 1 as belonging to F 2 x what does x plus 1 multiplied by x plus 1 and try that and if I think x plus 1 belonging to let us say F 3 x what does x plus 1 time x plus 1. So, let us do a slightly different multiplication, sorry let us do a x minus 1 and x minus 1, sorry for this just bit of a difference just to make bit of more interesting what does x plus 1 times x plus 1, simply it is x square plus 1.

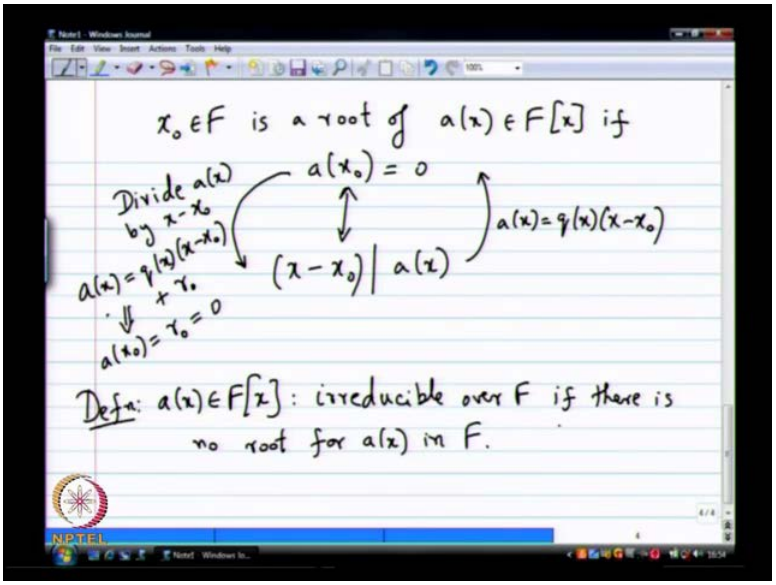
So, if you think x in one belongings to this and third example is if x plus 1 belongs to F 3 x, then what is x plus 1 into x plus 1, you get x square minus x plus 1, you can write it like that. I can write it like this x square plus 2 x plus 1, but what is 2 in F 3, it is minus 1, so you also write it has minus x. So, these are all just simply ways of writing it just to make answer look nice what about x minus 1 times x minus 1 x square plus x plus 1. I wanted the answer to look nice and nice form, if you see how multiplication changes character when you think of coefficient coming from different fields.

So, it is little bit strange then the third operation which is also very crucial is division with remainder arbitrary division are not possible in F X you cannot define a division which will divide any b of x by a of x. Then it will give you a some other element in F X itself it will be only rational you we would not worry about that we will only be worried about division with remainder in F X what is division with remainder.

You can divide b of x by divide b of x by a of x implies you do the long division when you do that long division, you will get two other polynomials q of x a of x plus r of x q of x is called coefficient r of x is called there remainder. What is the property, important property degree of r of x is between 0 and it is less then degree of a of x, so this is these are the various things about polynomials that you should be comfortable with the next

notion. I wrote about that notion also, but let me remind you once again is about rules of 0s when do you said x not in f is root is a root of a of x belonging to F X if a of x not is equal to 0.

(Refer Slide Time: 14:57)



So, you plug in x not instead of x evaluate that whole thing why can I evaluate it, I can evaluate it this valuation is meaningful because x not belongs to f and the coefficient of way x also belong to f s every multiplication is well defined. It can be done in the field f so far instance if a of x belongs to f to of x there is no meaning in putting x not from F 3 no compatibility, there is not much equation defined between those kind of elements. You have to restrict yourself to suitable fields that is important, so this is this is 0, there a question yesterday you said, it should be proper contain.

So, the question was what about this statement that if you have a equation with coefficient from rational fields then you can plug in the real number for x. You can do that, but then the rational are contained properly in the real where a operation are meaningful, but F 2 is not properly contained in F 3. So, the operation is different, I just showed you the example one is very different in F 2 then F 3. So, you cannot do such strange things even though I motivated them as integers suddenly when you think of one in F 2 it is not an integer any more it becomes some other entity.

So, you can notice those difference it is a bit abstract it is important to know the difference we use the same notation for multiple thing that is the problem. This is

equivalent to something else this this implies x minus x not divides a of x, so what do you mean by x minus x not divide a of x if you do the wrong division of a of x with x minus x not the remainder will be 0. So, this is true in any field and the proves is very easy how will you prove it who is going to prove it, so basically what you have to do is suppose a of x not 0 one way is very easy to prove x minus x not divides a of x a of x.

Then, what happens how do you prove this way if x minus of x is q of x times x minus x not, so you put a of x not this term is going to go to 0 and 0 multiplied by anything in any field is 0. I did not rigorously prove this things, but this are true, so believe me, so you have prove it, we can prove it, so this will show clearly a of x not is 0. The other way round how do you show that way to do it is you have take b of a of x and divide by x minus x not what will be the degree of remainder. It has to be degree 0, so it should be a constant right because last we strictness, then the degree of you are dividing by and that will be a constant.

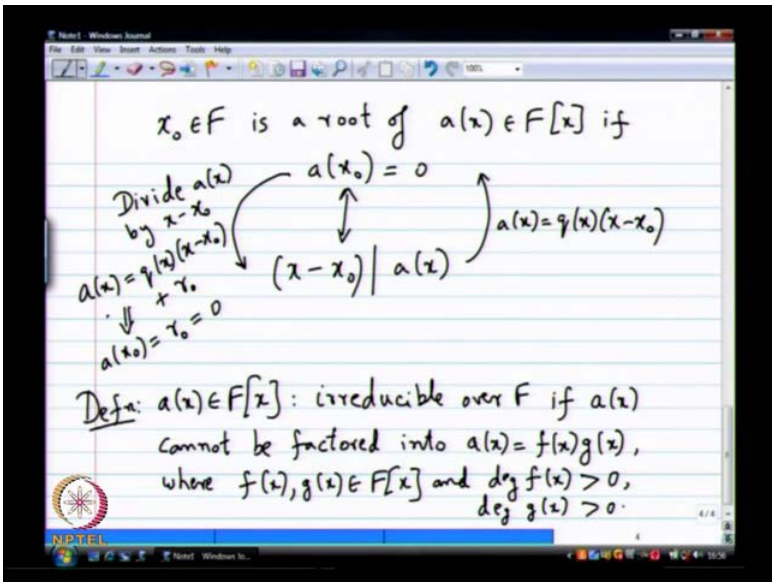
So, what do you getting a of x equals q of x times x minus x not plus some constants plus let us say r not, now what do I know about a of x not it is 0 it is going to go to 0. So, clearly r not has to be 0, this implies a of x not equal to r not put to 0 and you get this x minus x not dividing F. So, in case this are just mean, I am sure this you knew this in your gut, but if you have to prove it you have write it down right the careful proof has to be done and the divisional algorithm is the one that is gives you the proofs. So, this is this is the reality this quite important, not really five said if x not is rod, then this is true and I was said every a of x has a root of f that is definitely not true.

So, that is next definition he asked me the question, so I am going to the next question a of x in F X is said to be irreducible over f said to be this is the definition irreducible over f if what if there is no root for a of x in f. Then you say there is an irreducible polynomial, so that is the yes when you multiply that the actual still not have.

So, I know this is a this is slightly bad definition, so let me change itself there is no see this is this is not wrong this is not an if and only f you know if there is no root. It is a reducible there is no problem that is why I said it is a bad definition, but if it reducible it does not mean that there is no root that is not the only quotation, you can also have multiple it does not factor it is not reducible this is true, this is true or not actually. So, let us refresh, this is the very bad definitions let me not change this let me not change this.

So, let me change this, I am sorry, for that let us take it back and let me write the careful definition first.

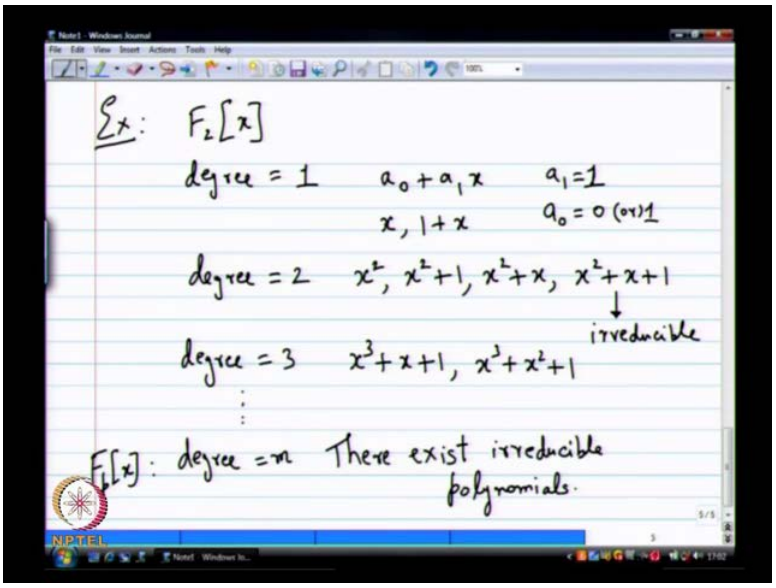
(Refer Slide Time: 20:55)



So, it is irreducible over f if it cannot be factored, so I have to say something about it, so let me say that, so as irreducible if let me just say a of x cannot to factored into a of x equals let us say some I do not f of x into g of x where thanks for pointing that out. So, both this case belong to F X and the degree of both of them is greater than 0, so you need that you cannot have a constant so you can always take out constants that is not a problem, but it should not able to out the factor. So, that is true, so one needs to be careful over an arbitrary field it cannot be factored only if this is true.

So, it is a big definition, but usually the way you check it for at least for smaller degrees is to see first if it has a root. Then you have to do some additional checks it is not as easy as it said so you have to do this very carefully. So, it seems like a complicated way to write it down, so let see some example it will be very clear, so why are we worried about irreducible polynomials.

(Refer Slide Time: 22:48)



So, if you notice if you look at F p how did we get F p we had prime numbers, so what is the property prime number they cannot to factored because they cannot be factored we got F p roughly. So, that is the reason why we got F p if you go and see the proof the main proof is with multiplicative inverse and that came because p cannot be factored. So, it turns out when you work with irreducible polynomials you can similarly, define F p power m. So, we will use irreducible polynomial to define F p power m and this are polynomial that cannot be factored. So, let us look at examples and the simplest example are degree 2 examples and over F 2.

So, we will mostly look at F 2 F x only we will look at some degree 2 degree two examples. So, I will look at F 2of x and let us say if I say degree equal to one so if I say polynomial of degree 1 first of all degree 0 does not make much sense. Let us do not worry about it degree 1 with coefficients from F to x.

Then, the form is what a zero plus a 1 x a 1 is 1 and then a 0 of 1, so you basically have just how many polynomials you have two polynomials of degree 1 in f to x what are the two polynomials x and one plus x. Both of them are irreducible right use x in on plus x, hopefully and then if you say degree 2 what happens. You have four different polynomials of degree 2 what are the four different polynomial x square x square plus one square plus x and x square plus x plus x square plus x plus four different polynomials.

It turns out three of them are reducible and one of them is not reducible, so for degree 2 checks are easy, so if at all a degree 2 polynomial can be factored into two polynomial of degree at least one only way it can happen is two degree 1 polynomials. So, you can easily plug in roots and check, so all you have to do is put an x equal to 0 and x equal to 1 and see if you get the 0 if both cases you do not get the 0. Then clearly it will be reduced this is one of the case where it is very easy also the factoring is also easy not too difficult than this case turns out this guy is irreducible.

Everything else is reducible, you can also find the factors very easily, but also another check is to see if roots is x equal to 0 is the root here x equals 0 is the root here x equals one is the root here. Then x equals 0 and one are roots so that something relevant to you. So, if you say degree equals three there are several, there are eight different degree 3 polynomials right and we can keep on writing them, but it turns out polynomial x cube plus x plus 1 and x cube plus x square plus 1 are the two that are irreducible. Anything else, I am quite sure with it say through there are some simple conditions for instance one has to definitely occur in an irreducible polynomial.

Otherwise, x can be definitely factor yes there are some rules and for binary there has to be only an odd number of terms and in fact for degree 3 also you can simply put an x equals 0 and x equals 1. I have only two its factors into two factors, one of them should have degree 1 both cannot have degree greater than 1.

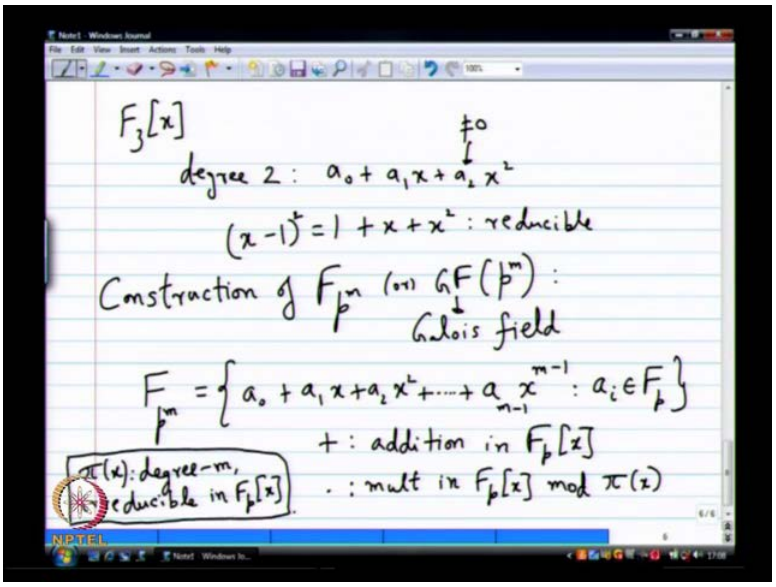
So, definitely there will be one root here, my previous equivalence root is the same as the degree 1 factor you have the root then that is the degree 1 factor that is the degree 1 factor and this is the root and that will that adds up. Hence, these are irreducible polynomials so what is what little bit non trivial can be proved with some effort, but not easy is for an arbitrary degree I say degree equals m there exist.

So, what is this gray symbol, I rule if you say what I say there exist the irreducible polynomial, so for every m there exist at least for one instance. Even in number you can exactly count there exist reducible polynomial for every m that is the good thing to know. So, till we know that there are prime numbers say many of them for every degree m there are a reducible polynomial.

That is the first non trivial result we may not really prove that in class, but it is true yeah its actually for any fields, but I have written it down there, this is true for any F p x. So,

there are algorithms to find this irreducible polynomials you can look it up computation software like mat lab there are many methods to find a mat lab may not have it, but mathematical or something definitely have this software. All irreducible polynomial for any F p you can look it up, so these are irreducible polynomials, from now on I will assume that I can always find irreducible polynomial of degree m and F p x.

(Refer Slide Time: 29:26)



So, lets us see few more interesting points here, so I moved to F 3 x degree 1 is a boring case we would not see it. Let us go to degree 2 how many polynomials are there for degree 2 three x 18 different polynomials because see it has to be a 0 a 1 x plus a 2 x this cannot be 0's. In this case there are two possibilities here times three here times three here 18 different possibilities, so you can go through this there are several but for instance this polynomial one plus x plus x square is reducible. So, it is not irreducible easy to see one of the roots what equals one x equals one is the root this is we saw just before is same as its one x minus 1 know, so always thinking in the binary feels.

So, x minus one square is one plus x plus x square if you see this, it is not a multiplication, so it is clearly reducible, so this is another indication that F 2 and F 3 is not a proper containment, it is something else. Strange things can happen when you think of one and F 2 it is very different from one and F 3, one needs to be careful about all. So, we are ready to see the construction f to power m its surprise you or not, so have an I will just give you the construction which show the that is feel that is later on.

We will see some properties yes this is a construction of F p power nits also denoted like I said g F p power n Galois field after French mathematician Galoi what is the construction goes like this this. Basically, set of all polynomials of degree m minus 1 or lesser, I am not saying these things to non zero a belongs to F p. So, this is the set all right what does the set contain, I have not defined the addition and multiplication this is the crucial part of definition of the field. Let us us look at the field once again and the set first and make sure that we are comfortable with that what the set contains.

It contains polynomials with coefficients from F p a of degree less than or equal to m minus one how many such polynomials will I have each coefficient can take one of p possible values. So, clearly p to the power m, so F p power m is not made a mistake this F p power so the crucial part is addition and multiplication so addition will be what just regular addition n F x. There is no problem there, so you see all the properties are satisfied, closure is satisfied divide any two polynomials of degree less than or equal to m minus 1, definitely get the polynomial of degree less than or equal to m minus 1.

There is zero polynomial which acts as the 0 and every element has also has an inverse if we do minus of that you get the inverse and it is also a in the same field that is no problem multiplication. You will need an irreducible polynomial in case multiplication is polynomial multiplication it is basically multiplication in F p x modulo some phi effects. Here, this phi effects is the I should say what phi effects is we should have phi effects which is a degree m irreducible polynomial in F p x.

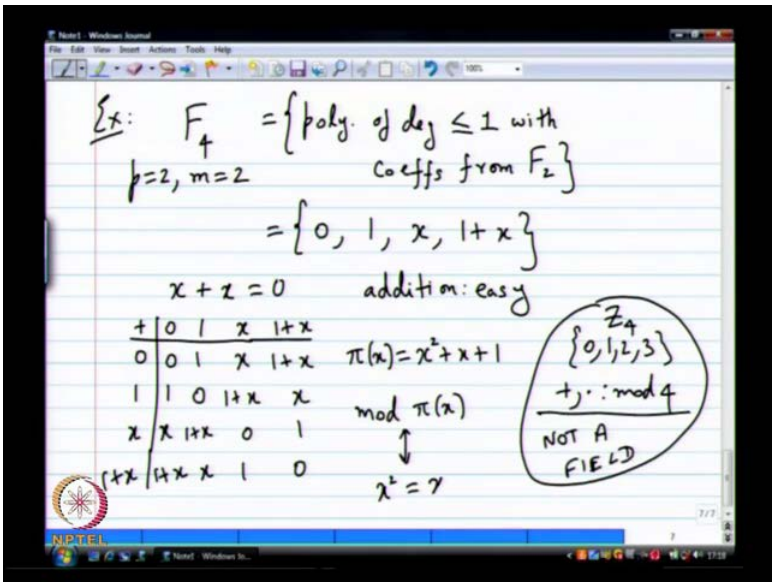
This is crucial just like we had p before we need a phi x which is irreducible degree m polynomial. That can be many yes what terms, you have only one field surprising results will come to an end, so you pick any one degree m if it is polynomial F p x and use that to define your multiplications. So, how will I multiply, now if I have two elements from F P power n, I will first multiply their polynomials and F p x.

So, I will get, so I will get maximum degree what it can go up to 2 m minus 2, so it can go up to that. Then what will I do, I will divide that and do a long division of that with pi x and take that reminder. Now, what will be the reminder degree less than or equal to m minus one because pi of x has degree m, so that is the idea in saying multiplication x modulo p x. So, clearly closure is obvious, it has no problem, only non trivial thing is the inverse and inverse the same proof I did before will go through problem.

So, you can go back and check that proof you take any one polynomial in this multiplied by all the other polynomials. You have F p also done F P power n is simply F p x once you have the addition and multiplication reminder multiplication and division with remainder you are done, I can do very easy computer implementation.

So, that is the focus of this course at least the way you see here you should be able to write the program to implement it whether you do it or not that is my goal is the focus from which I am teaching. If you want know the theory behind this you have to read some text books, so you asked me some questions, I answered to my best of the ability there are books which has all these written down very clearly. So, let us see some examples before I tell you some more interesting things about these fields here.

(Refer Slide Time: 37:53)



Few examples what about F 4 a without knowing anything about anything else you can write down easily the elements of F 4. It is very easy what were the elements of F 4 what does the elements of four again go back and look at sea p power n 4 is what 2 square p is 2 and m is 2 and so that a first step, yes recognized. These two and m is 2 and F 4 x contains what polynomials of degree less than or equal to m minus 1 with coefficients from F 2 x. So, this contain polynomials of degree less than or equal to m minus one and what is m minus 1 with coefficients from F 2 x.

So, this is just a small set how many do you have F 4 different elements clearly and what are the 0 1 x 1 plus, so those are the four elements in this and you can make an addition

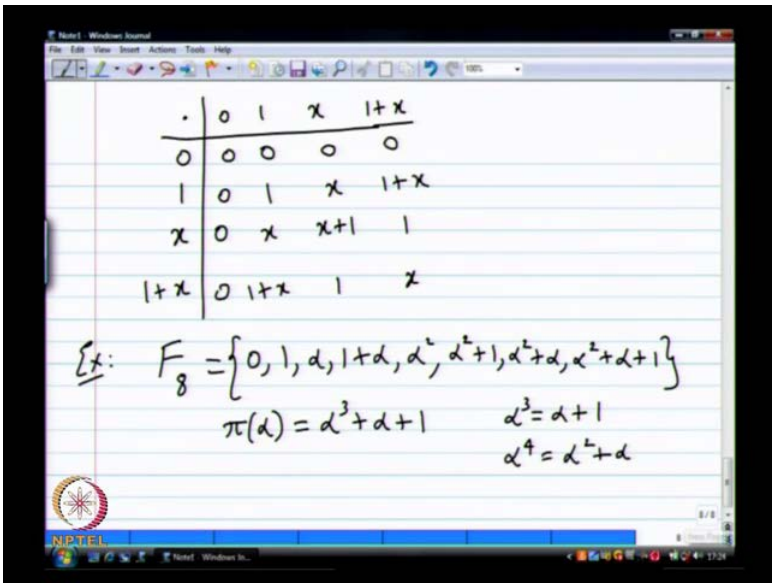
table addition is very trivial you know how to add. So, add any two you will get something else which is in this list only I am slightly non trivial addition is x plus x what will be x plus x 0.

So, in fact the moment you have three equals to irrespective of what ms you will add to elements what will you get repeatedly added elements what will you get you will always get 0 any will be 0 because you have 2 times less than and 2 0. So, that is the idea so that addition is trivial, so we will just leave it alone easy to see what the addition is you can make a table if you like. I made a table, so that you can make if you like so table very easy with the table.

So, let us make the table we will do that 0 1 x and 1 plus x 0 1 x and plus x, you can go ahead and fill out this table so not very hard that is the table you get I am sorry, I am not writing F 4 of x no. This is F 4, so thanks for pointing aloud F naught F 4 of x definitely F 4, I hope I did not write F 4 of x there as F e power n F 4 of x also exist, but that is not this if this is F 4, sorry for the mistake thanks for pointing aloud. Yes, definitely for this the question is F 2 is 0, 1 F 3 is 0, 1, 2 should not F 4 be 0, 1, 2, 3 that is not correct that is not correct that is not defined that will not be a field, why will that not be a field for instance two does not have a inverse in that do mod four.

So, question was this a field 0, 2, 3, 1 addition and multiplication mod four it is not the field it is this guy not the field. So, what is x square minus x minus 1, but the same as x plus 1, so x square equals x plus 1. So, that is the magic mantra to you once you use that your multiplication will be very clear when I do modulo when I multiply two polynomials modulo p of x all. I am using this additional rule that x square equals x plus 1, so once you use that you can easily use the multiplication table. So, mod p of x mod pi of x is equivalent to having the condition x square equals x plus 1.

(Refer Slide Time: 44:52)



So, once you do that the multiplication becomes very easy to write now in my head, but to write it down you will see this is what this has been. So, next example we are going to see F 8 and here I am going to make a switch in the notation that make everything more complicated.

Then, you will see everything will be very more much more complicated what is the switch in the notation instead of x. I am going to use alpha Latin letters the moment you go to Greek letters suddenly everything will become much more complicated. It is very common to write finite field's alpha instead of x. So, x owns like variable you might want you can use actually I want to write F 4 x also I want to think of polynomial else the coefficients from F 4, F 4 also has x.

Then, the notation becomes really nasty that is only reason why they do it suddenly because of alpha everybody thinks you have much more difficult problem than what you have it before same thing is before I want to shift it to alpha. So, what is f eight to have eight different elements each of them are polynomials in alpha of degree what less than or equal to 2 and coefficients from F 2 0 or one you write it down it is not very hard 0 1.

So, this is f 8, I am not going to label the table for the addition is I am not going to label the table for multiplication, but we will do some multiplications by hand just to check how things are worked. So, for doing multiplication I need to define a five of alpha which is of degree three, so I told you that there are two different choices you can make

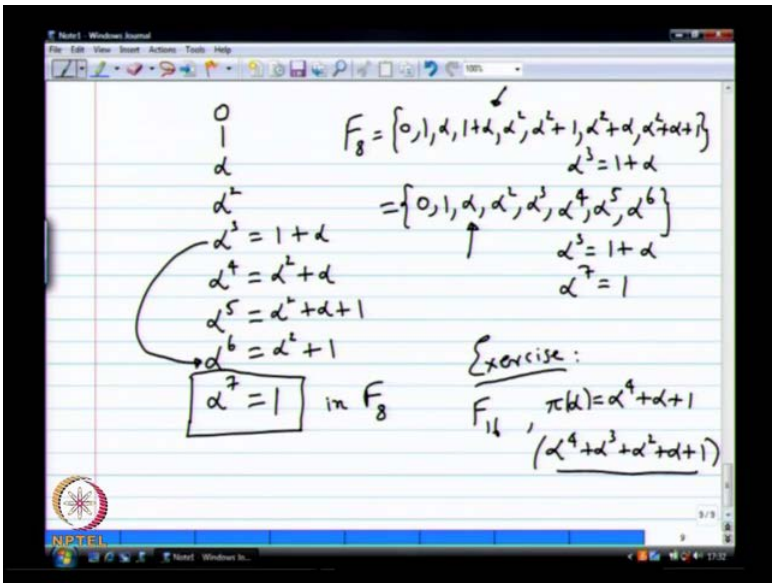
five of alpha for degree three, so we will take alpha power three plus alpha plus one you can also pick the other.

I commented briefly you do not really get a new field those things, we would not prove, but it is anyone is good enough and we will pick nicer looking one I think alpha three plus alpha plus one is nice. So, you can do any multiplication, but what is the rule that you keep in mind when you do multiplication strictly is alpha power 3 is alpha plus 1 that is the only rule you have to remember, but remember in the multiplication you will also get alpha power 4. So, what you will do for alpha power 4, so it is basically alpha times alpha power 3 and alpha power and alpha plus 1. So, basically alpha power 4 is same as Alpha Square plus alpha, so you use these two rules any multiplication becomes very trivial just write down this two rules always.

Remember, then any multiplication you do whenever you will get alpha power three replace it by alpha plus 1. Whenever you get alpha power 4 replace it by alpha square plus alpha that is how you operate a f 8, so in reality it is a much simpler field than the real field. So, you will learn about real field all the complexity you will daily get scared, so scary field somehow we have comport able with the real field than this abstract field. It is just of 8 elements what can really go around along with eight elements, so it will be nothing real numbers vary on one has how many elements uncountable infinite number of elements this is much somehow scary, but people get more scared of this the real field.

If the name real is most unreal of all should not have been called real, I do not know why they call it if you read the actual definition of real field you will agree with me. So, this is not real at all it exists in some bodies imagination, so, I wanted you to do a certain specific type of multiplication it is interesting. You will see a nice little pattern emerge about these fields which is also universally true which once again we would not prove, but we will accept that fact.

(Refer Slide Time: 50:27)



So, I want the multiplication, I want you to do in F 8 it is the following, I wanted you to find you have 0, you have one you have alpha you have alpha square in the field and then I have alpha for 3 being equal to 1 plus alpha. Then I have alpha 4 which is alpha square plus alpha, what I want you to fill out is alpha for 5 alpha of 6 alpha for 7 we will stop. Everybody converge any answer, so alpha for 5 is what, so it is basically alpha for 3 plus alpha square and then alpha part three you have to be replaced by alpha plus 1. So, essentially you will get alpha square plus alpha plus 1, and then alpha part 6 you have to multiply alpha part by 5 by alpha you will get alpha square plus 1.

In fact there is a curious way to go from here to here directly how will do that, basically square at one plus alpha square at is simply one plus alpha square to goes to see when alpha part seven is what alpha no adds one a. It is one again then what will happen alpha for eight alpha after that it will repeat the same think will repeat again and again. So, what you have seen is has alpha part seven equals one and f eight alright that is the first think that is obvious from this table from this calculation.

There is another slightly more settled thing if you look really carefully, you will notice what I am saying what this that others settle thing yeah all the elements of f eight are simply being generated as powers of this one alpha. So, that is the others settled think here. So, I wrote previously F 8 as this how did the F 8 see a road the F 8 as this guy. I

wrote f 8, I wrote F 8 as this know, so any where the cutting in pasting is not really working out quite well because the size.

So, I am not able to adjust for anyway, so let me right it again I wrote F 8 as 0 1 alpha 1 plus alpha square the alpha square plus 1 alpha square plus alpha square plus alpha plus 1. Then I wrote down the rules alpha part 3 equals the rule alpha part 3 equals 1 plus alpha was able to figure out the feel based on that terms out the same F 8 is the exact same as 0 1 alpha square alpha part 3 alpha part 4 alpha part 5 alpha part 6. Then I have to remember two rules know also part three is one plus alpha and then alpha part 7 is 1 so what is so nice about having two different ways of writing F 8.

If have to do additional multiplication by hand in first notation and top notation this in the top notation and this notation. This is easy which operation easy and which operation is difficult you can do by hand addition is very easy, but multiplication is little bit more difficult, it is not difficult clearly, but it is little bit more difficult. You have to do long division, do some rules remembers something in this notation what is very easy multiplication is very tribunal, but what is difficult addition is not very obvious alpha of 5 alpha of 4.

If you work a lot, get the answer if you do not want to use the other notation in fact you will you will end up going other notation get do the addition. So, when you implement finite fields this table is very critical how you go from what is known as the polynomial notation to what is known as the power notation for f 8. At least, we have seen, but we wonder if this is true for any f power amp consolidated does true consol there is one element of F p power amp which will generate all the elements as consecutive power. So, is those things are true you will see them later, now just want to look at the two things conveyance as self that multiplication is easy one notation why addition is easy in the are the notation.

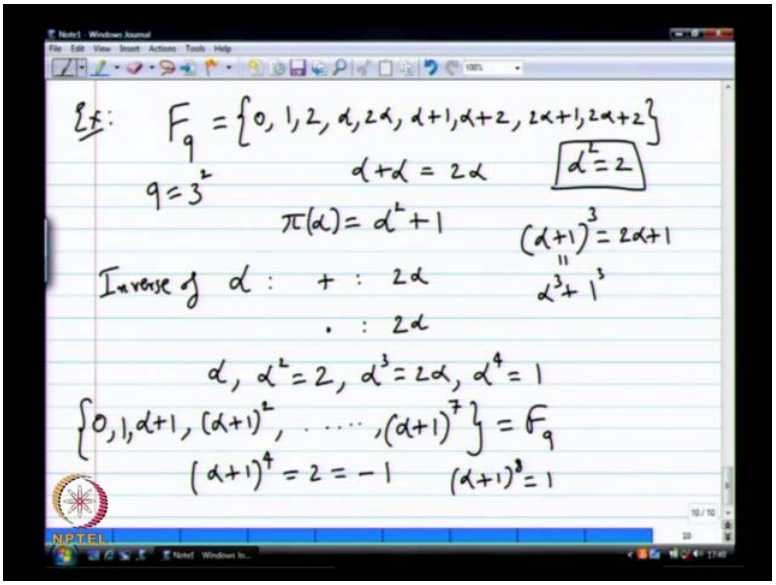
So, that is f 8, so an exercise for you is to try the same think for f 16 so f 16, you pick phi of alpha to d alpha for 4 plus alpha plus 1 case this is a reducible to check that you need to do a lot of work what is the work you to do the check this is reducible check. You have to do that is, so every take first of all leaner factors, so alpha equals to 0 is not a route alpha equal to one is not route. So, the no leaner factor can, then you to look for factors of degree 2 is possible it is possible that it is factor degree 2, you will see they

will be no factor of degree 2 for instance alpha square plus alpha plus 1 will not divide this then you can be show.

You have check it owned work, so once you check that you have done they will does not divide that this will be a reducible other reducible polynomial. In fact, there are three reducible polynomial of degree 4 other one as other one as basically the mirror image of this what is the mirror image of this alpha for 4 plus alpha for 3 plus 1 and then they other polynomial that say reducible a alpha for 4 plus alpha for 3 alpha square plus alpha plus 1.

All this gets are also a reducible and take any one and try, but you will get the surprising answer for this once do not try this do not try this too early try just this alpha for four alpha for one. You will work, try this and try making this equivalence to do different notation its good exercise it is first time, you do it you may not believe me should not believe me should try. It is equivalent case had me come back that ask come to that, so this is alpha little bit special that is why you got this equal if you take any other elements all its power own generate all the even if F P it is not true. So, let see let see few more computations as to get feet wet this in case an F 8, F 8 let us write something.

(Refer Slide Time: 58:48)



Lets write something F 8 is little bit weird because all elements will be good, let us some other field, so will take, so let us see another example just likely more entering will try. What can we try what is the next you can try tell something F 9 at seems like the next

simplex thinking you try let try F9 let us try F 9 is going to be nine elements 0 1 2 and then alpha 2 alpha what else alpha plus 1 alpha plus 2 2 alpha plus 1 2 alpha plus 2 to again all 9. You are remember 9 is 3 power 2, so I have to look for all polynomial with confidents from F 3 of degree less than or equal 2 1, so all in all problems, so addition I will skip, so addition you know it is going to work.

So, little bit non trivial, so when compared t to F 2, so F 8, F 4 addition little bit non trivial so for assistance alpha plus alpha plus what two alpha it does not bold is 0 that is what meanwhile says little bit not trivial. So, if add three times what will happen that you go to 0 an element add a three times will go up to 0, but 2 times go to 0, but beyond that thus nothing but say about addition its hope fully addition as clarity.

So, multiplication you need you need irreducible polynomial of degree what two coefficient from three case terms out one choice which is weird choice is alpha square plus 1. So, it is reducible in F 3 in F 2 its clearly not reducible, but F 3 is reducible, you can check that, so if put in 0, you get the you get one you put and one you get two you put and 2, you get 2, so it this every reducible in F 3. So, if you know go ahead and do the multiplication, you will get lets straight something just row of fun what is the inverse of alpha what is the multiplication inverse of false added inverse.

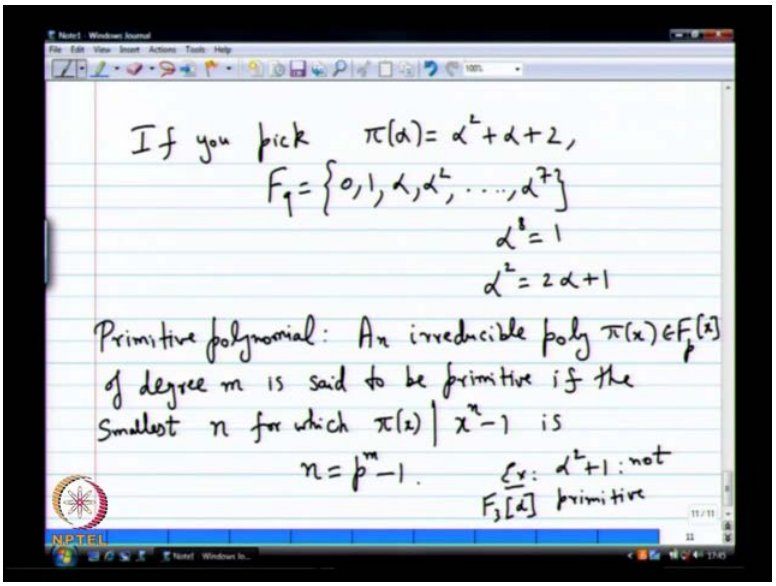
This is very easy added inverse this is what minus also two also what about multiplicity inverse try do not want to intelligently get to the answer at least by f you think will you get to the answer two alpha is an try what about multiplicity inverse of alpha plus 1 get that easily. So, what does can be finally easily let us stop here is multiplicity inverse is little bit boring live it like here live it like here case. Other thing we try to before was to look at power of alpha, so look at what happens you need power as alpha itself inbuilt. So, look at what efforts happening you get alpha then what is alpha square equals what is alpha part 3, 2 alpha what is alpha for 4, 1.

So, how is this, so just it makes everything go away in this, so alpha power 3, 8 which just now wrote down is 2 alpha, so its 2 alpha plus 1 it is very easy if you want to do alpha plus 1 power 4, you can do that you see its 2 minus 1 and this. So, even for f 9 when I pick Alpha Square plus 1 as my pie of alpha, I am not getting to be my magic element which creates all the elements power, but alpha plus 1 is a magic element. That

is good enough if I have a table going from the notation on the top to this notation, I can do both addition and multiplication easily.

So, it can happen, so as it turns out instead of alpha square plus one if you pick if you pick pie of alpha to d Alpha Square plus alpha plus 2 for instance is this valid irreducible polynomial. It is it is a valid irreducible polynomial, there is no problem in that, so if you were to pick pie of alpha to be a alpha square plus alpha plus 2. It will turn out what will alpha itself will end up generating the entire F net alpha F 9 will be equal to 0 1 alpha square so on till alpha power 7 alpha powers 8 will be 1 and Alpha Square will be 2 alphas. So, I will write down the general fact soon enough, but this these are things to keep in mind.

(Refer Slide Time: 01:07:10)



So, what we have shown by example, now we have proven the example we have not really proved it, but what we have proved the example is feels of form F p power m seems to have two different ways of representation. One is the simple polynomial representation of F p which is very useful for addition the other is this power representation is called the power representation. It seems to be one element which is able to generate all the elements by its powers and these through this statement are in general true for any F p power 3.

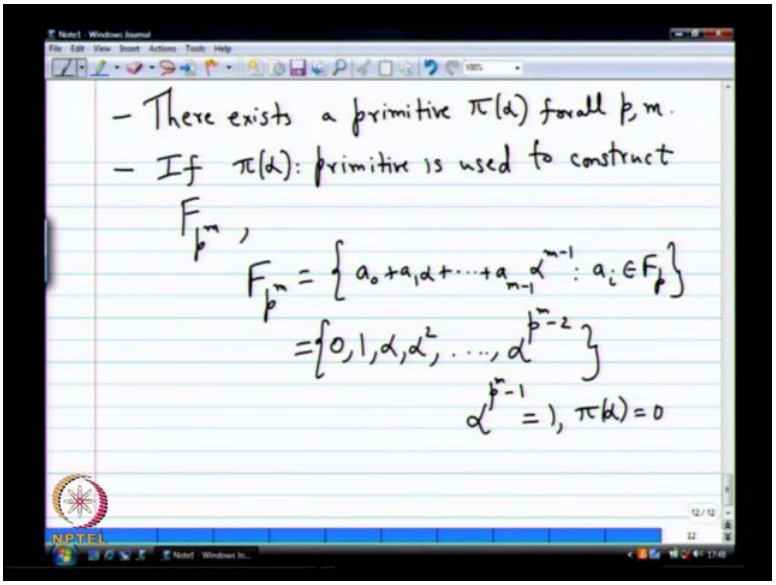
So, what you have to do for that is you have picked a pie of alpha smartly and that choice is what is called is a primitive polynomial. So, what is a primitive polynomial an

irreducible polynomial say pie of x of degree m the set to be primitive if the smallest n for which pie of x divides x to the power n minus 1 is n equals. So, I should say where this p F X comes from say F p x n equals p to the power m minus 1, it seems like a crazy definition is a bit of crazy definition.

If you see all the motivation that seems to come from other areas will just take it as a definition and you can back go back to our examples with F 9 this pie of alpha square plus 1 will divide for what n it will divide x power n alpha power n minus 1. Use one of your formulas a square minus b square is a minus b into a plus b, use one of that you will see for n equals 4 that will divide and 3 square is 9 and you want the smallest for it 4. It will divide will be to be 9, 8, so for four itself it divides, so that pie of alpha did not qualify as primitive on the other hand this pie of alpha square plus 2 will be primitive. So, that is the example alpha square plus one is not primitive of course in F 3 F 3 alpha, so this example for F 3 alpha does not spend too much time digesting this definition.

It is not so crucial, what is very crucial is if you pick pie of alpha as a primitive polynomial first of all there exist primitive polynomial for every p and every m that is the first point what are the two points that are important to remember. There exists pi alpha for all p m, so there is primitive polynomial not only visible it is also primitive that there exists primitive polynomial this also can be looked up in mathematics etc. They can many primitive, so there exist at least one primitive pie of alpha for all p m and then the next thing that is true is if you use if pie of alpha primitive is used in to construct F p m.

(Refer Slide Time: 01:11:59)



Then, F p m will be a 0 plus a 1 alpha plus 1 till a m minus 1 alpha power m minus 1 a i belonging to F p and it will also be equal to the set 0 1 alpha square so on till alpha power p to the power n minus 2 alpha power p to the power m minus 1. This will be equal to 1, pi of alpha will be equal to 0 0 1 1, some of these powers will be equal to 2, I mean for instance there will be some i, such that alpha power i is equal to 2. If p is greater than 2 if p is for instance 7 there will be some i, for which alpha power i equals to 2 and there will be another j for which alpha power j is 3 etcetera.

These are the elements, all the elements are generated, so this is true for I have written it for p power m this is also true for F p, we never really saw F p. So, for even for F p, this is true does not really apply in this, of course it applies you have to think of F p has been generated with a degree polynomial degree 1 which is always primitive. Then you can write it down, so for even for F p this is true that is always a primitive element. So, it will be difficult for all kinds of result we are talking about I will stop here digest this pick up from here in next week.