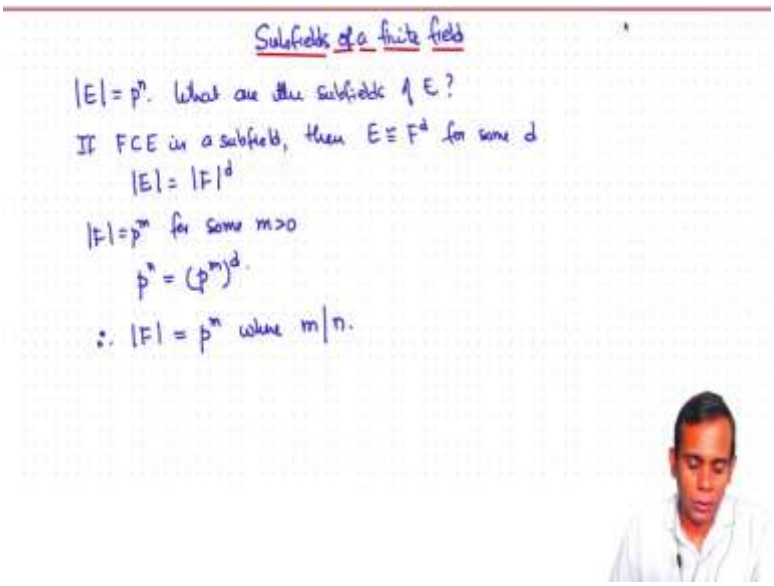
Algebra – II
Professor Amritanshu Prasad
Mathematics,
The Institute of Mathematical Sciences
Lec15
Subfields of a Finite Field

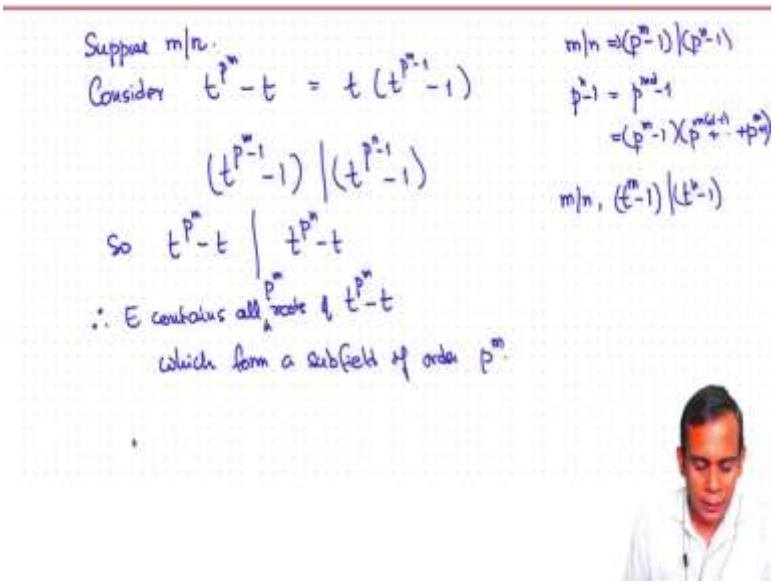
(Refer Slide Time: 00:15)



Suppose E is a field of order p to the n, we ask what are the subfields of E. Firstly there is a fairly simple calculation that we can do to figure out the order of the subfield of E, if F is a subfield of E, then E is a vector space over there. So E is as a vector space is isomorphic to F to the power d for some integer d. Now that means that the cardinality of E is going to be the cardinality of F to the power d, now E has characteristic p implies that F also has characteristic p, just because if you take the one the unit of E it is also the unit of F.

So if you ask how many times you have to add it to itself before you get 0, the answer is the same, whether you are working E or n. So what we have is also that, the order of F is p to the m for some m some positive integer m, and so what we have is p to the power n is p to the power m to the power d and therefore the order of F is p to the power m where m divides n. So, if E has a subfield then it is order must be p to the power m where m is a factor of n. Now we ask suppose m is a factor of n, then can I find a subfield of E with this order.

(Refer Slide Time: 02:19)



So now suppose m is a factor of n, then let us look at the polynomial t to the power p to the power m minus t, so this is t into t to the power p to the power m minus 1 minus 1. Now note that m divides n this implies that p to the power m minus 1 divides p to the power n minus 1. Why is that? suppose n is m times t, then p to the n minus 1 is p to the md minus 1 which, I can write as p to the m minus 1 into p to the m d m times d minus 1 plus t to the m times d minus 2 plus dot dot a geometric series p to the power m plus 1.

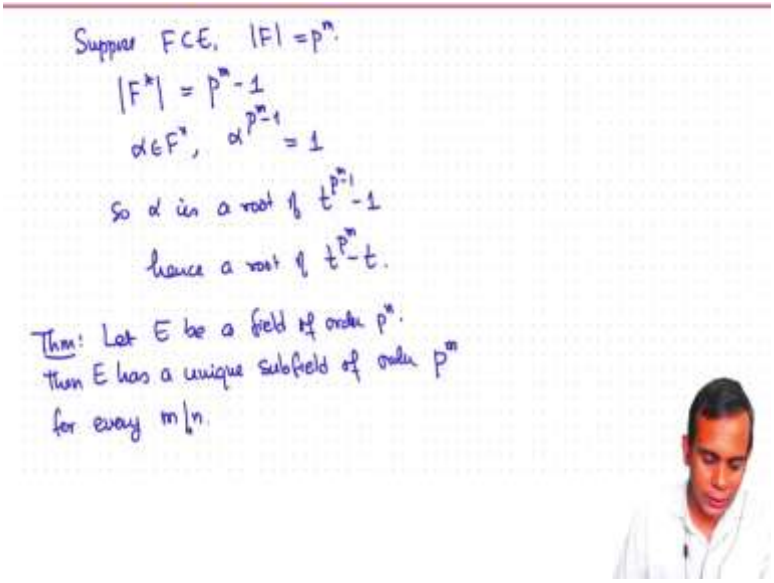
So we have this factorization and therefore p to the m minus 1 divides p to the power n minus 1, and so p to the power m minus 1 divides p to the power n minus 1, so this is t times t to the power, and now we have another result, that if m divides n, then t to the power m minus 1 divides t to the power n minus 1.

It the same proof instead of p you use t, this works in polynomials and so since p to the power m minus 1 divides to the power p to the power n minus 1, what we have is, t to the power p to the power m minus 1 minus 1 divides t to the power p to the power n minus 1 minus 1 and so t to the power p to the m minus t divides t to the power p to the n minus t, because that again t into this thing which divides t to the power p to the m minus 1 minus 1.

If m divides n then t to the power p to the m minus t divides t to the power of p to the n minus t, now all the roots of this polynomial are the elements of E, in fact the elements of E are precisely the roots of this polynomial and therefore all the roots of this polynomial also are in E.

Therefore E contains all the roots of t to the power p to the m minus t, and how many are there well we just saw in the last lecture that there are precisely p to the m of them because they are all distinct by the derivative criterion. So, all p to the m roots which form we also saw in the last lecture a subfield of order p to the power n, therefore indeed if m divides n, then E has a subfield of order p to the n.

(Refer Slide Time: 05:50)

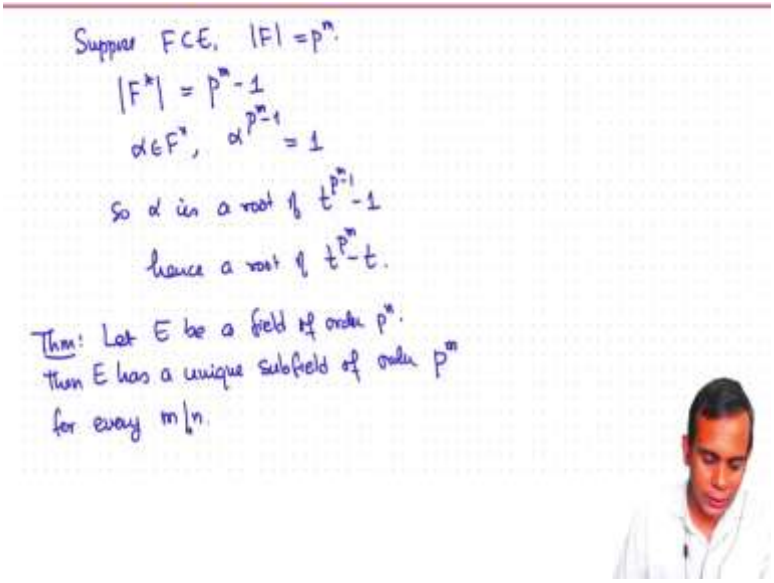


And, another fact is that suppose F is a subfield and the order of F is p to the m, then you look at the multiplicative group F star and this has order p to the m minus 1. So if you take any element alpha in F star then alpha to the power p to the power m minus 1 is equal to 1, because its order must divide the order of the group, and so alpha is a root of t to the power E to the power m minus 1 minus 1 ie of if hence lies in the field that we constructed earlier.

So hence also root of t to the power p to the minus t, are this now the roots of this include 0 and the roots of this polynomial, and so what we see is that the only field of order p to the m consists of roots of the polynomial t to the power p to the m minus t, and so what we have is the theorem that E has a unique subfield of order p to the m for every m dividing n.

So maybe I should say here that, suppose E is a field of order p to the m, let E be a field of order p to the n, then E has a unique subfield of order p to the m, for every m divided n, so we know exactly what the subfields of a finite field are.

(Refer Slide Time: 08:27)



Let me show you illustrate with a picture some fields of even order. The smallest field of even order is a field of order 2, and this is contained in a field of order 4, it also contained in a field of order 8. But this field of order 8 does not contain a field of order 4 because 8 is p cubed and 4 is p squared and 2 is not a factor of 3.

This field of order 4 is contained in the field of order 16 because 2 squared is so this is 2 squared and this 2 to the power 4 and 2 divides 4, but it also contained in a field of order 64 here, which is, this is 2 cubed, this is 2 squared, this is 2 to the power 6. So 6 divides 2 and 3, so F64 contains F4 and F8, going in this direction we have F20 sorry 2 to the power 9 and 2 to the power 9 is 512.

And you can extend this diagram a bit more F16 contains F256 which is 2 power, so this is 2 power 1, this is 2 power 2, this is 2 power 4, and this is 2 power 8, and you can put here F4096, and here there is a rather large field F262144, and some huge field over here, of course these are not all the fields, there are more fields that even just containing F2 with nothing in between a field of order 2 to the power p for every prime p contains F2.

Now in this example, a field of order 262144 contains how many subfields, so it contains this this this this this this, so it contains exactly six subfields, including itself. So what does this reflect? this reflects that this is F2 to the power 18 and 18 has six divisors, the divisors of 18 are 1, 2, 3, 6, 9 and then finally 18 1, 2, 3, 4, 5, 6. So the number of a subfield of a field of order p to the n is equal to the number of divisors of n.