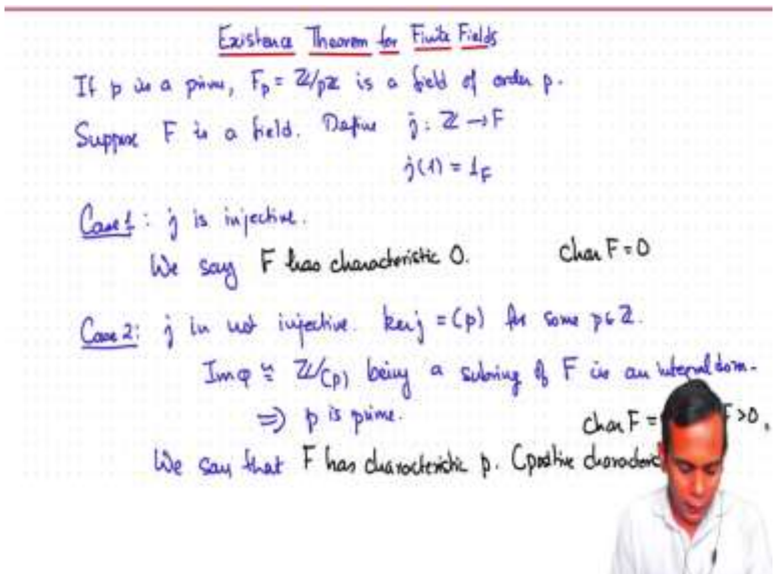
Algebra – II

Professor Amritanshu Prasad
Mathematics,
The Institute of Mathematical Sciences

Lec14

Existence Theorem for Finite Fields

(Refer Slide Time: 00:15)



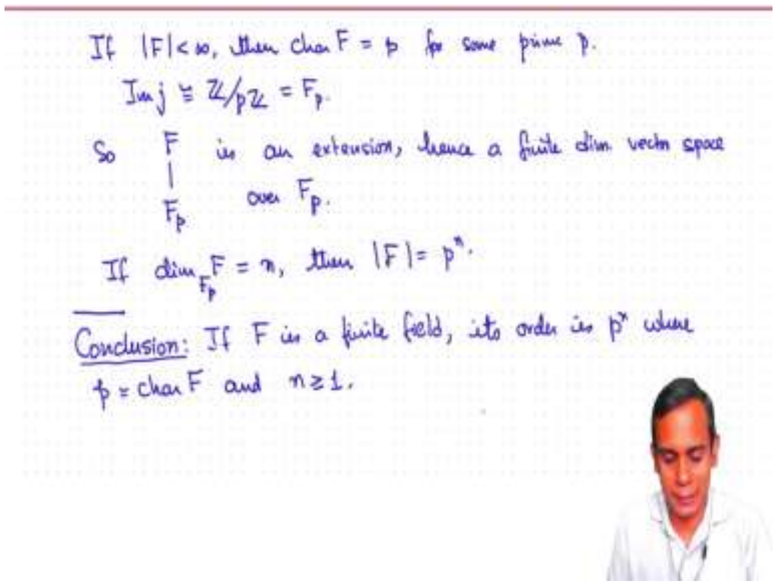
What are the possible cardinalities for finite fields? So firstly, if p is a prime number then you can look at the finite field z mod pz, we know that that is a field. So, it is a field of order p, what other orders can see finite fields have? So, to understand this firstly, suppose F is a field, then you define a ring homomorphism j from Z to F by setting j of 1 is equal to the unit of F.

The two cases, the first case is that j is injected, injective in this case we say that F has characteristic zero, you may prefer to say that F has characteristic infinity, but actually we just the common terminology is that F has characteristic 0. You can keep adding 1 to itself, and in in in the field F and you will never get 0, you can keep adding 1 to itself and get different elements of the field F.

But in the finite case of course j cannot be injective; in that case the kernel of j is an ideal. So, kernel of j is a proper ideal offset, so it is it is generated by some element p. But the image of Phi is therefore isomorphic to Z mod p and this being a sub ring of a field is an integral domain. The sub ring of an integral domain is an integral.

Being a sub ring of F is an integral domain which implies that p is prime and so in this case we say that F has characteristic. And if F has characteristic p for some prime number p, we say that the characteristic of F is positive. So, this is called the positive characteristic case. We will also use some notation, here we will say char F is 0 and here we will say char F is p and we will also say char F is positive, as opposed to 0.

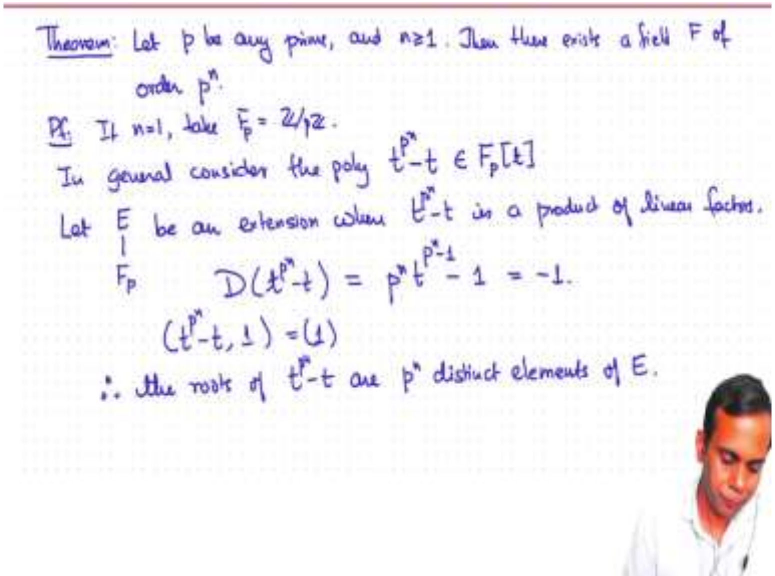
(Refer Slide Time: 03:54)



Now a finite field obviously must fall into case two. So, for any finite field the characteristic is a prime number p, and in that case if F is finite, then char F is p for some prime p. And image of j is is going to be isomorphic to Z mod pZ which we have called Fp. So, F is an extension of Fp, so F is a field extension of the field Z mod pZ and therefore it is a finite dimensional, since its finite itself, hence a finite dimensional vector space over Fp.

So that means that, if if if the dimension of F over Fp is n, then the cardinality of F has to be p to the power n. So, the conclusion is that if F is a finite field, it is order is p to the power n where p is the characteristic of F and n is some positive integer. That raises the question, that if I have a prime number p and a positive integer n, can i always find a field with p to the power n many elements? And the answer to that turns out to be yes.

(Refer Slide Time: 06:10)



That is our theorem. let p be any prime and in any positive integer. Then there exists a field F of order p to the n, that means a field with p to the n many elements, and the proof is, uses what we had before about showing that every polynomial, if you have a field and you have a polynomial over that field then you can find an extension where this polynomial is a product of linear factors.

Now to start with if n is 1 then we can just take F equals Z mod pZ and (())(07:16), so, in general the polynomial you consider is t to the power p to the n minus t. So, this is a polynomial in, so we are calling this field Fp so this is a polynomial in Fpt, its coefficients are in Z mod pZ, and let e be an extension, where t to the power pn minus t is a product of linear factors.

Now, note that if i take the derivative of this D of tp to the n minus t, that turns out to be p to the n tp to the n minus 1 and minus 1 which is actually just minus 1. So surely the gcd of tp to the n minus t comma 1 is 1. So by the derivative criterion for a polynomial having distinct roots, therefore the roots of tp to the n minus t are p to the n distinct elements of E, and now it only remains to show that these distinct elements actually form a sub feed of E.

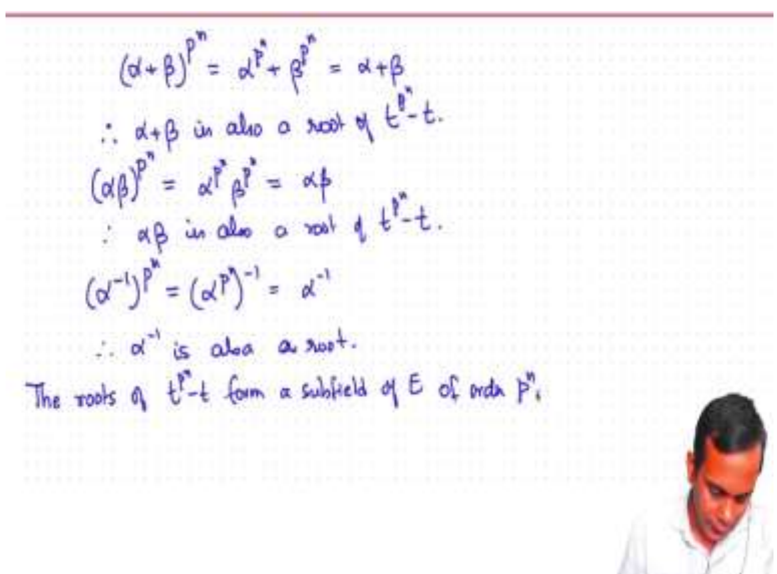
So, the claim is, that the roots of tp to the n minus t form a sub field of E. We need to just check that if alpha and beta are roots, then alpha plus beta is a root. So, if alpha and beta roots, then we have alpha p to the n plus beta p to the n, alpha p to the n is equal to alpha and beta p to the n is equal to beta.

Now there is a very useful trick in characteristic p which is that alpha plus beta to the power p is just equal to alpha to the p plus beta to the power p in a field of characteristic p, this is because if you just write down the binomial expansion you have alpha plus beta to the power p is sum k goes from 0 to p, p choose k, alpha to the k, beta to the k minus 1, but this p choose k is just going to be divisible by p unless k equals 0 or 1.

The integer p to the k or p, so in positive characteristic what happens is in characteristic p, what happens is all these terms die out, leaving only the first term and the last term. So this becomes alpha raised to p plus beta raised to p, and now you can apply the same equation again and again and so you can get alpha plus beta raised to p square.

Well that is alpha plus beta raised to p, then that raised to p, which is alpha to the p plus beta raised to p to the power p which is alpha raised to p square plus beta raised to p square, and continuing in this way what you can show is that, alpha plus beta raised to the power p to the n is equal to alpha raised to the power p to the n plus beta raised to the power p to the n for all alpha beta and all n greater than 0.

(Refer Slide Time: 12:06)



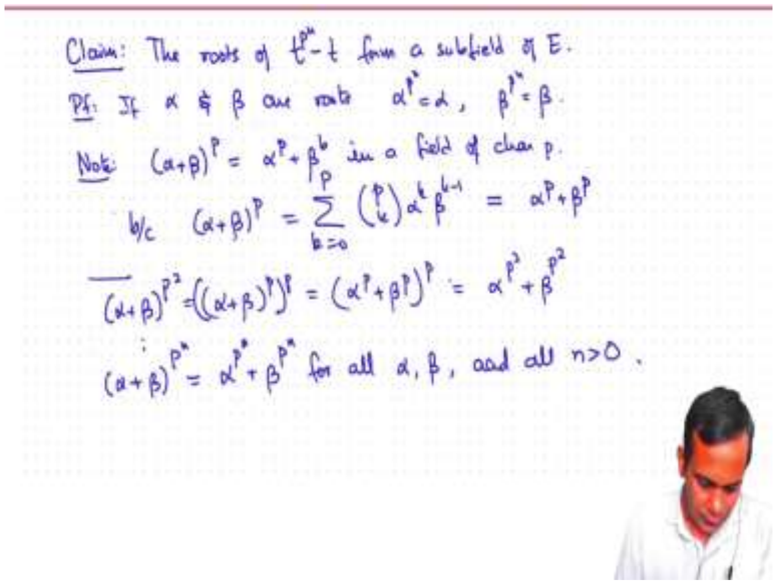
So using this, what we see is, that if we have alpha plus beta raised to the power of p to the n well, we just saw that is alpha to the power p to the n plus beta to the power p to the n, but since alpha is a solution of t to the p to the n minus t alpha to the p to the n is just alpha and beta to the p to the n is just beta.

So what we get is alpha plus beta to the power p to the n is again equal to alpha plus beta, which means that alpha plus beta is also a root of the polynomial t to the power p to the n minus t. so what we have shown is that if alpha and beta are roots, then alpha plus beta is the root. It is very easy to show that if alpha and beta are roots, then alpha beta is also a root.

So you write alpha beta to the power p to the n is alpha to the power of p to the n, beta to the power p to the n, just because multiplication is commutative but alpha to the power p to the n is alpha, and beta to the power p to the n is beta, so alpha beta to the power p to the n is alpha beta, alpha beta is also root. So what of course 0 and 1 are also roots so what we have is that the roots of the polynomial t to the power p to the n minus t form a sub ring of F, but there is also this simple fact that the inverse of an l of a root is again a root.

Alpha inverse to the power p to the n then that is the same as alpha to the power p to the n inverse, but that is alpha inverse. So alpha inverse is also a root, therefore the roots of the polynomial t to the power p to the n minus t form a sub field of E and we have seen because of the derivative criterion for repeated groups that this polynomial actually has p to the n distinct roots, so they form a subfield of E of order p to the n.

(Refer Slide Time: 14:44)



And, so the conclusion is that, yes for any prime p and any integer n greater than equal to 1 there exists a field F of order p to the n, you just start with Fp, you take the polynomial t to the power p to the power n minus t, find a field in which it factorizes into linear factors and look at the subfield consisting of its roots and that is going to be a field of order p to the n.