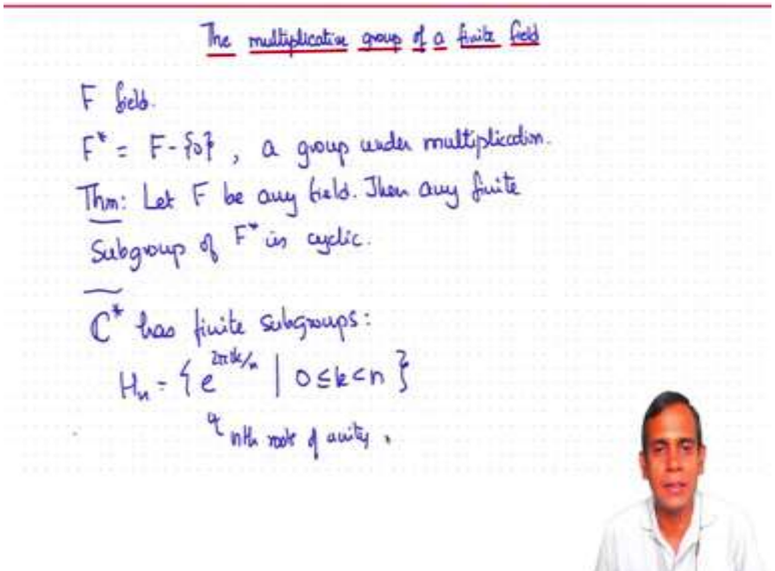
Algebra - II
Professor Amritanshu Prasad
Mathematics
The Institute of Mathematical Sciences
Multiplicative Group of a Finite Field

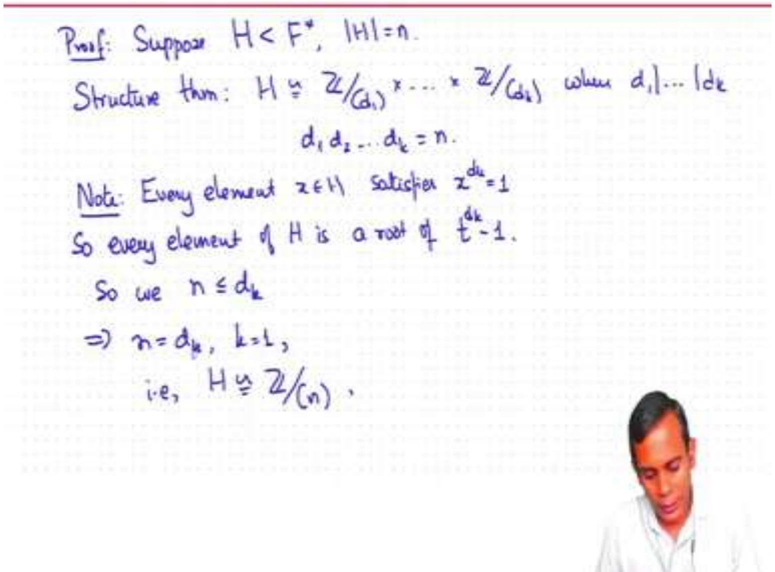
(Refer Slide Time: 00:15)



Suppose F is a field. Let F star denote the set all non-zero elements, and so F Star is a group under multiplication. It turns out that subgroups of this group, finite subgroups of this group, are all cyclic. Theorem let F be a field. Then any finite sub group of F star is cyclic. Before we go to the proof, let me just give you some examples.

So, if you take the complex numbers, then you look at C star, then every finite subgroup of C star consists of Hn equal to e to the 2 pi I k by n where 0 lies between k lies between 0 and strictly less than n. These are the nth roots of unity. In fact, when we prove this theorem will see that it is a very similar situation there, that if we have a finite subgroup of F star of order n then it consists precisely of nth roots of unity.

(Refer Slide Time: 02:27)

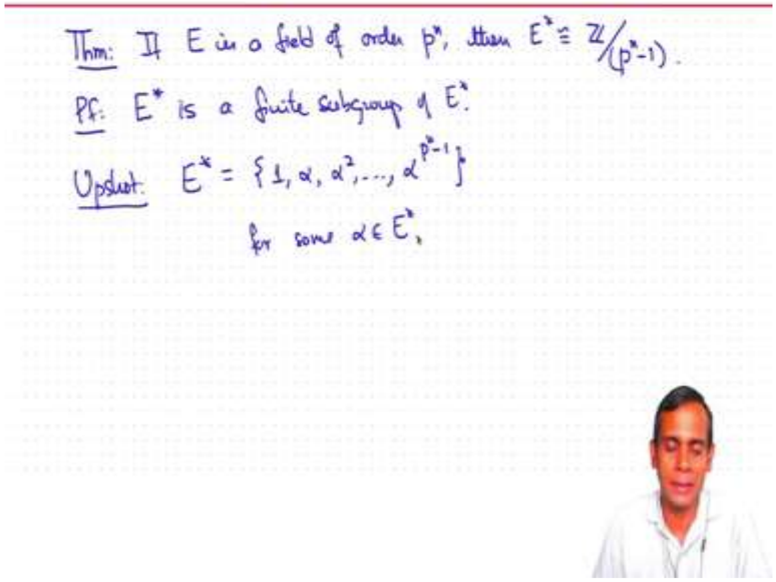


So, let us proof the theorem. Suppose H is a subgroup of F star and cardinality of H is equal to n then by the structure theorem for finite Abelian groups we have that H is isomorphic Z on d1, cross Z on d2 cross Z on dk where d1 divides d2 divides dk and the additional fact that the size of H is n it means that d1, d2 the product of these things is equal to n.

Now note that every element of H satisfies x to the power dk is equal to 1 because the order of each of these cyclic groups divides dk. And so what we have is that every element of H is a root of the polynomial t to the power dk minus 1. But this polynomial can have at most dk many roots because it is of degree dk. And so we have that n is less than or equal to dk.

So, this is only possible if n is equal to dk and in fact, k is equal to 1. I would just say n is equal to d1. So, i.e H is isomorphic to Z mod n. So, that concludes the proof of the theorem every finite subgroup of the multiplicative group of 80 feet is cyclic, in fact, which is of order n it is isomorphic Z mod n.

(Refer Slide Time: 05:06)



So, now let us look at finite fields, so the multiplicative group of finite field. So, theorem and this actually is an obvious corollary of this previous result if. So, if E is a finite field. If E is a field of order p to the n, then the multiplicative group of E is isomorphic to the cyclic group Z mod p to the n minus 1. Proof when E star is a finite subgroup of E star. It is yeah it is the full group and it is finite because E is finite, so E star is finite. And so the previous theorem applies, right.

So, E star has to be cyclic and it is order is p to the n minus 1. So, it is a cyclic group of order n minus 1. The upshot of this is that E star can be written as 1, alpha, alpha square, alpha to the power p to the n minus 1 you can pick an element alpha a non-zero element of the field such that every element of the field can be written as a power of that original element, okay. So, that is a very powerful property and we will see some applications of that in the next lecture.