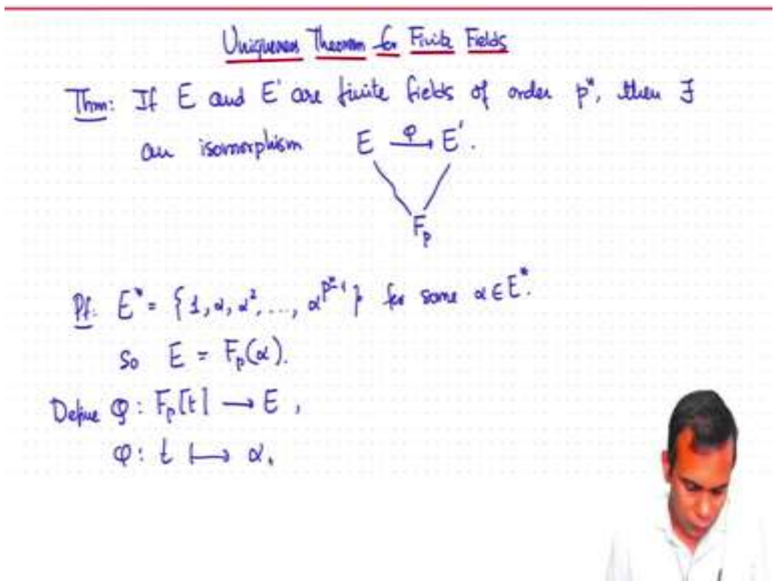
Algebra - II
Professor Amritanshu Prasad
Mathematics
The Institute of Mathematical Sciences
Uniqueness Theorem for Finite Field

(Refer Slide Time: 00:15)



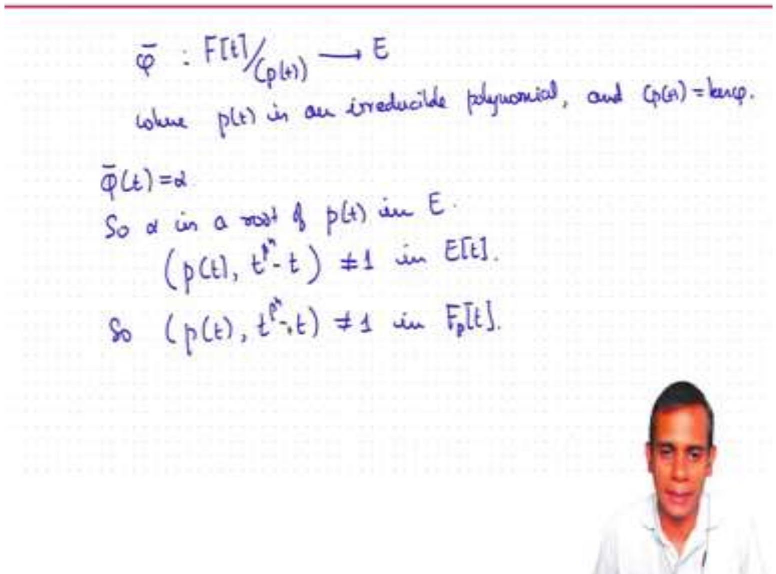
In this lecture, we will show that up to the isomorphic there is only one field of any given finite order. For this, we will use the fact that the multiplicative group of a finite field is cyclic. So, suppose e. So, theorem if E and E prime are finite fields of order P to the n, then there exists an Isomorphism E onto the E prime.

And what is more, this is sort of a trivial observation, but I just want to say it here is that this Isomorphism will map to the copy of FP which is obtained by taking one and adding it to itself. How many of the times it lacked by identity on F? So, there is an isomorphism of field extensions E over FP to E prime over F.

Now, the proof of this is as follows. We will express E as coefficient of FPT modulo irreducible polynomial. So, what we do is we know that E star is the group generated by some element alpha. Some non-zero element Alpha generates this group, and what this means is that E is the group generated by Alpha, the field extension of F P generated by Alpha.

That is the smallest field containing F.P and Alpha is all of E. Now that means that we can construct a homomorphism fee from FP to E As we did in the first lecture of this course, which is just takes fee of t goes to Alpha, then what we have is that this fee gives rise to an isomorphism.

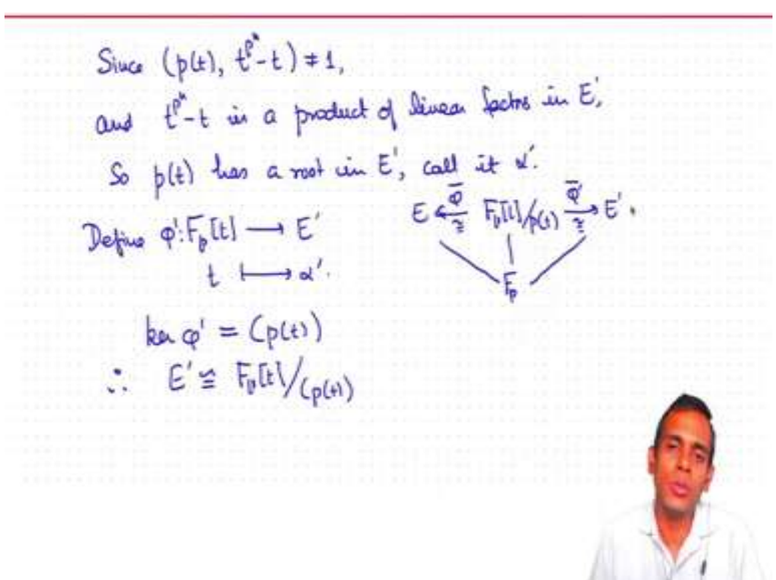
(Refer Slide Time: 03:19)



So we have Ft mod Pt to E, P bar where, Pt, is an irreducible polynomial and Pt generates kernel of Q. So, E is isomorphic to Ft mod Pt. Now, this suppose we write. So, what we know is that fee bat of t is Alpha. And so Alpha is root of Pt in E this means that the GCD of Pt and t to the P to the n minus t Alpha is also root of P to the n minus t because the elements of E are precisely all the roots of t to the p to the n minus t. This is not equal to one in E t.

But we have seen that this GCD does not actually depend on which polynomial rate we are computing it over, if the GCD is not one in Et, it is also not one in FPt. Because both is polynomials are FPt and. And so the GCD must also lie in FPt, okay.

(Refer Slide Time: 05:52)



Now let us move to the field E prime. So, since Pt and t to the P to the n minus t is not equal to one and t to the P to the n minus t split into linear factors in E prime. Is a product of linear factor? This means that Pt has a root if in fact one of those linear factors must also divide Pt. So, Pt has a root E prime call it Alpha prime. And now you define FPt to let us call this fee prime to E prime by taking t to alpha prime.

Now this homorphism must have kernal containing Pt because Alpha Prime is the root of Pt. But this Pt is a maximal ideal. I mean, the kernal cannot be all of FPt because this map is obviously non zero alpha prime, is not it? And so this kernel P prime has to be equal to Pt. And therefore, E prime is also isomorphic to FPt mod Pt.

And so what we have is FPt mod Pt this over FP is isomorphic to E on the one hand via fee bar and isomorphic to E prime on the other hand, via E prime bar which means that E and E prime has isomorphic via fee prime bar circle, fee bar inverse and that proves the theorem. But the thing is that up to isomorphism, there is only one finite field of any given order.