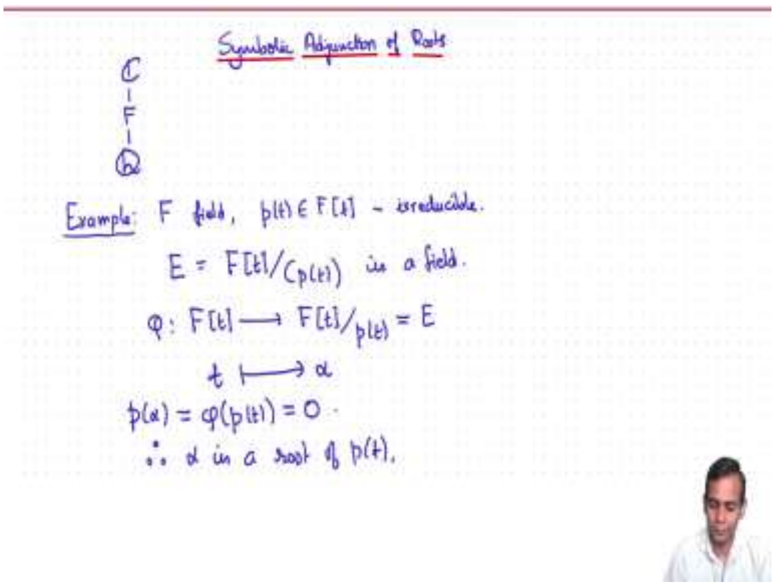
Algebra-II
Professor Amritanshu Prasad
Mathematics
Indian Institute of Sciences
Symbolic Adjunction

(Refer Slide Time: 00:14)



Until now we have been looking at field extensions. Mostly we have been looking at the rational numbers sitting inside complex numbers or inside real numbers, and we have been looking at fields that lie above the rational numbers. These have been most of our concrete examples. However, we often need to look at more abstract situations such as when we construct finite fields, or when we study field extensions of the field of rational functions over a field.

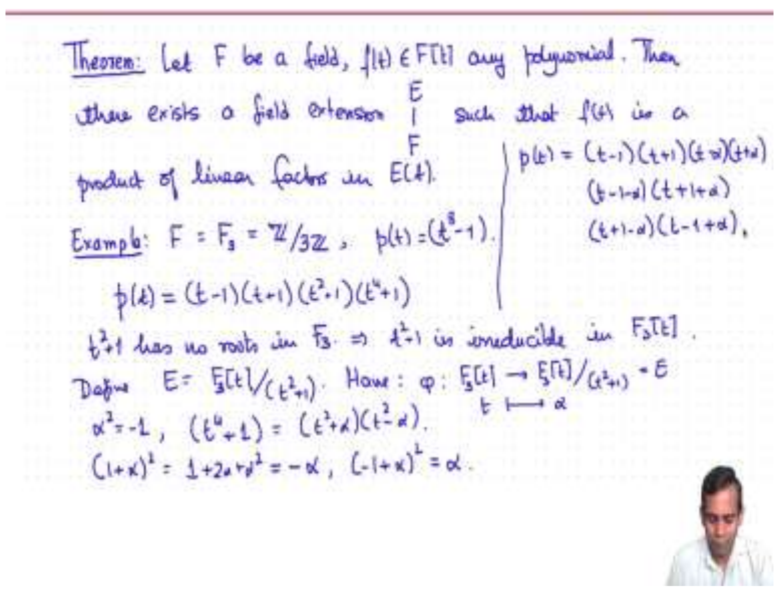
But then, we do not have this device of complex numbers or real numbers to fall back on. So, we can construct fields in a somewhat more abstract way. The simplest example is when you have a field and an irreducible polynomial. So let us take F to be any field and Pt to be an irreducible polynomial in the variable t, and coefficient in F.

Then you can construct an extension E to be Ft mod, Pt. Now, remember that if Pt is irreducible, if it is an irreducible element of a principle ideal domain, then it generates a maximal idea, because if there were a larger ideal, then it could be generated by a element that divides Pt. And so, if Pt is irreducible, it would generate a maximal ideal. And, since the ideal generated by Pt is a maximal ideal, Ft mod Pt is a field. And so, this is a field.

And now, in this field, let us, let us see. So we have Ft, and this maps surjectively on to Ft mod Pt, which is equal to E. So, in here we have the element t. And, we can look at its image in here, which we will call alpha. Then, what we have is that p alpha is well, it is the image of Pt. So, let us call this map phi. It is the image of Pt. And, that must be zero, since Pt goes to zero under, under the map phi.

Therefore, alpha is a root of Pt. So, in the simplest example, what we have done is we have started with the field and an irreducible polynomial with coefficients in that field. And then, we have constructed a field extension, where that polynomial has a root. This kind of a construction can be carried out in a much more general setting. And, this is going to be the main theorem of this lecture, which I shall now state.

(Refer Slide Time: 03:06)



The theorem is that suppose you have a field F and let Pt be any, Ft be any polynomial in Ft, okay. Then there exists the field extension E over F such that Ft is a product of linear factors in Et. We know of course, that when we take field contained in the complex numbers, the complex numbers will always serve the purpose of the field E. But in more general situations, we actually need to construct this field extension E over F.

Let us look at a couple of examples before we go to the proof. So, just to, so to reinforce the, the abstraction that may be involved here, let us start with F being the field with 3 elements, which is just integers mod 3. Since three is a prime, that is a field. And, let us take Pt to be the polynomial, a t to the power 8 minus 1, okay, then Pt. Let us try to factorize it as much as I can.

So, it has a factor t minus 1. t minus 1 into t plus 1 is t squared minus 1, t squared minus 1, into t squared plus 1 is t to the power 4 minus one. t to the power 4 minus 1 into t to the power 4 plus 1 is t to the power 8 minus 1. Okay, now, you can easily check that t squared plus 1 has no roots in F3. So in fact, t squared plus 1 is irreducible, in F3T. So, you can define E equal to Ft mod t squared plus 1. So, let alpha be the image of t in E.

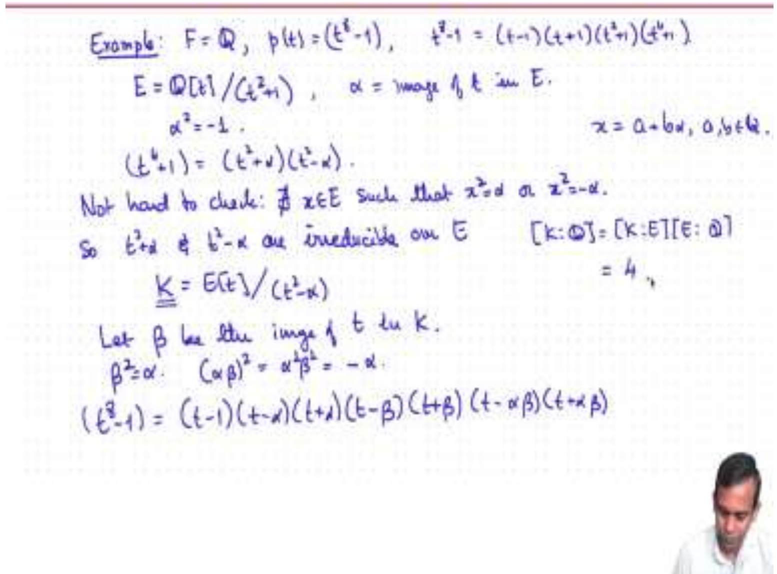
So, we have a map phi from Ft to Ft, let us write F3 here, mod t squared plus 1, which is E. And, so, we will take T and call its image alpha. Then what we have is that alpha squared equals minus 1 because alpha squared plus 1is zero by design. And so, what we have is that T to the power 4 plus alpha is is, no plus 1, this factor here, this last factor here, is equal to t squared plus alpha into t squared minus alpha.

Now, if you just study this a little bit, you will see that you take 1 plus alpha the whole squared, then this is 1 plus 2 alpha plus alpha squared. But, alpha squared is minus 1. So, this is equal to 2 alpha. But 2 alpha is equal to minus alpha because 2 is equal to minus 1 in F3. So, 1 plus alpha squared is equal to minus alpha and minus 1 plus alpha squared similarly you can compute to show that this is equal to alpha.

So, we have elements whose roots, which are square roots of alpha and minus alpha. So, this polynomial for the t squared plus alpha and t squared minus alpha further factorize. So, what we have is, let me just write it over here. This thing Pt becomes t minus 1 into t plus 1, and then t squared plus 1, we already adjoined its two step, plus alpha and minus alpha into t minus alpha into t plus alpha. And then, we have to, 4 more factors corresponding to t to the 4 plus 1.

So, t to the 4 plus 1is t squared plus alpha and t squared minus alpha. And, t squared plus alpha has 2 roots, namely the square roots of minus alpha, which means that we will take t minus 1 minus alpha into t plus 1 plus alpha. And then, we have a factors corresponding to this, which is t plus 1 minus alpha, into t minus 1 plus alpha. So, Pt factorizes into 8 linear factors over the field extension, E, which is just F3t mod t squared plus 1.

(Refer Slide Time: 09:01)



Let us look at another example with the same polynomial. But, instead of starting with F3, we will start with Q. F is Q and let us take the same, Pt equals t to the power 8 minus one. And, once again, we have this factorization just copied from last time; t to power 8 minus 1 is t minus 1 into E plus 1into t squared plus 1 into t to the power 4 plus 1.

And these, these polynomials t squared plus 1 and t to the power 4 plus 1 are irreducible over Q, okay. You should think about t squared plus 1 is obviously irreducible over Q because it has no roots and quadratic polynomials are irreducible if it has no roots. This t to the 4 plus 1, you need to show that has no quadratic factors either. But, we do not really need to do that right now. Let us just do what we did last time.

So, first defined E to be Qt mod t squared plus 1. So, this is a quadratic extension of Q. And, taking alpha to be image of t in E, we have alpha squared equals minus 1. And so again, we can write t to the power 4 plus 1is equal to t squared plus alpha into t squared minus alpha, okay. It is not hard to check that t squared, that there does not exist any element x in E, such that x squared equals alpha, or x squared equals minus alpha.

You have to do this, a general element of E is going to be of the form a plus b alpha, where a and b are in Q, rational numbers. And so, you just write down the equation x squared equals alpha.

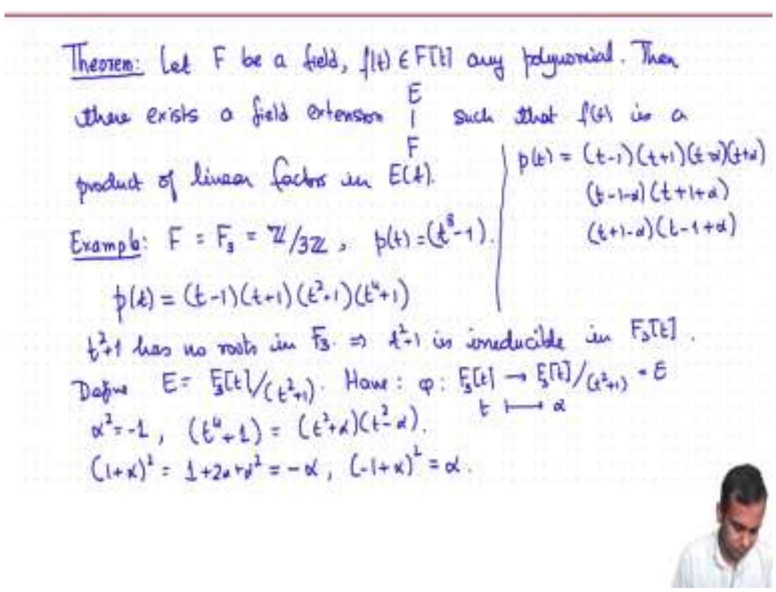
And, what you will get is a quadratic equation involving a and b. And using that, you will be able to show that such a and b rational do not exist, okay. I will leave that as an exercise to you.

What that means is that t squared plus alpha and t squared minus alpha have no roots, and therefore each of them is irreducible. So, we could take one of them, and let us just define, so t squared plus alpha and t squared minus alpha are irreducible. And so, you take K to be Et mod t squared. These are the reducible over E. So, I can take t squared Et mod t squared minus alpha, that is going to be a field because this is an irreducible polynomial.

A let beta be the image of t in K. Then, what we have is that beta squared equals alpha. And, what we also have is that alpha times beta squared is alpha squared beta squared, where, but alpha squared is minus 1. So this is minus alpha. So, alp..beta is a square root of alpha and alpha beta is the square root of minus alpha. Of course, minus beta is another square root of alpha and minus alpha beta is another square root of minus alpha.

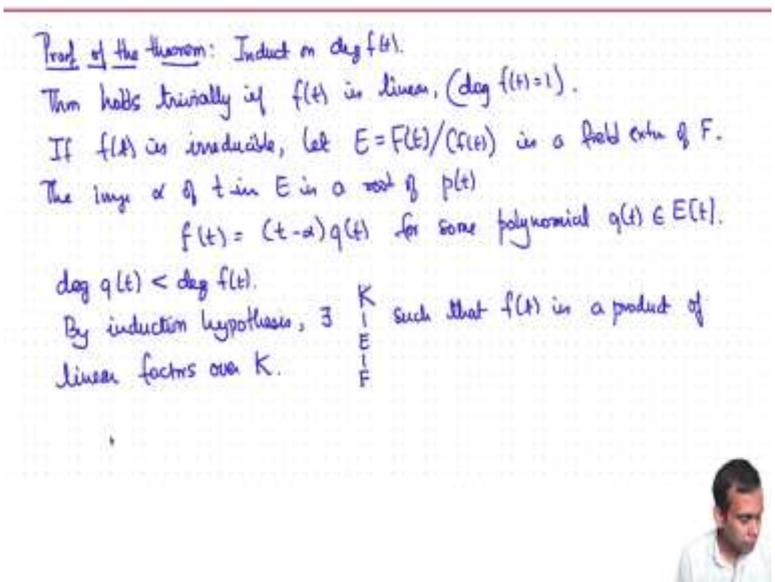
And so, what we get is that t to the 8 minus 1is equal to t minus 1 into t minus alpha into t plus alpha into t minus beta into t plus beta into t minus alpha beta into t plus alpha beta. And, this is a linear factorization of t to the power 8 minus 1in this larger field K. Now, the degree of K over Q is the degree of K over T times the degree of E over Q. And, that is 2 into 2. So, that is 4.

(Refer Slide Time: 13:52)



I hope these examples have given you a feel for what we are doing here. And, now we are ready to prove the general theorem. So, proof of the theorem. Well, before we go to the proof of the theorem, let us just go back and take a look at the statement of the theorem. So, the theorem says that if F is any field and little ft is any polynomial with coefficients in the field F, then there exists an extension E or F, such that the polynomial little ft is a product of linear factors, okay. So, you have a complete factorization of the polynomial in the field.

(Refer Slide Time: 14:38)

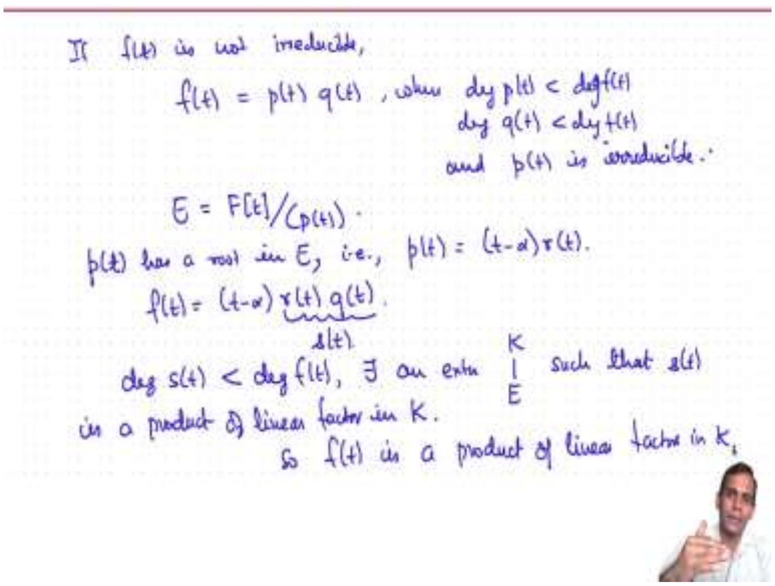


And, so, the proof of the theorem is by induction on the degree of F. If F is linear then this is trivially true, right. So, theorem holds trivially if Ft is linear or degree is equal to 1, okay. Now, if Ft is irreducible, then just take as a first approximation, let us take E to be Ft mod. The ideal generated by little ft. And, this is a field. It is an extension of F. And, and, now, Pt has a root in, as we have seen, the image of t in E.

So, the image alpha of t in E is a root of Pt. That means that Pt can be written as t minus alpha times Qt for some polynomial Qt in Et. Now, we are working with E because this root is in E. So, we apply the factor theorem in the field Et. The factor theorem says that if you have a polynomial which vanishes at some point, then, then the binomial is divisible by x minus t minus that point. Okay, so um, so, so, this is a form of Pt.

And so, let us try now Ft, ah yeah, sorry, this is Ft. And now, what we can do is, we have degree of Qt is strictly less than the degree of Ft. So, by the induction hypothesis, there exists an extension K over E, such that Ft is a product of linear factors over, maybe I cannot call it K, I started with a field K, so, let us call this, oh no, I started with the field F, so, this is fine, Linear factors over K. And so, Ft split is, is, is a product of linear factors in a field K which is an extension of F; because E itself is an extension. Now, suppose Ft is not irreducible.

(Refer Slide Time: 18:23)



Then you can write Ft as Pt times Qt where degree of Pt is less than degree of Ft and degree of Qt is less than degree of Ft and Pt is irreducible. Just take an irreducible factor of Ft. Then again, you define E to be Ft mod the ideal generated by Pt. And so, Pt has a root in E. And, so, we can write Pt equals t minus alpha times rt. So, what we have is Ft equals t minus alpha times rt times Qt. Let us call this St. So, what we have is the degree of St is strictly less than the degree of Ft.

And, working over E, what we have is there exists an extension K over E such that St is a product of linear factors in K. Well, St is a product of linear factors in K and Ft is t minus alpha times St. So, also Ft is a product of linear factors in K. So, what we have shown is that you start with any polynomial over any field; you can always find an extension in which that polynomial is a product of linear factors.