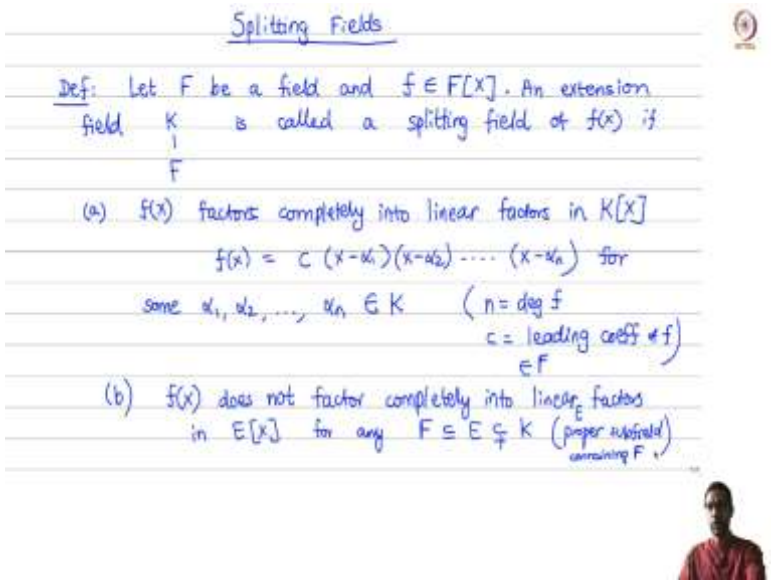
Algebra II
Professor – S. Viswanath
The Institute of Mathematical Sciences
Existence of Splitting Fields, Bound on Degree

(Refer Slide Time: 00:19)



Let us talk about Splitting Fields. So here is a definition, let F be a field and let small f denote a polynomial in the ring F of x. An extension field K of F. So, let us denote it in the usual way K is an extension field of F is called a splitting field of this polynomial f of x, if two conditions are satisfied. So, let us write them both out, number one, this polynomial f of x factors completely into linear factors.

So, this polynomial should do linear factors in the polynomial ring Kx, in other words, I can write fx as a product of x minus alpha 1, alpha 2, alpha 3 and so on till x minus alpha n. And of course, if you assume that the polynomial is not monic, that there is some leading coefficient, then that leading coefficient also comes out in front.

So, we will typically assume that we are talking about monic polynomials or ones where the leading coefficient is 0 is 1, sorry. So fx is such a product for some elements alpha 1, alpha 2, alpha n, in the extension field K. And as I said, so well here, what is n? n is the degree of the polynomial f, and C is just a leading coefficient.

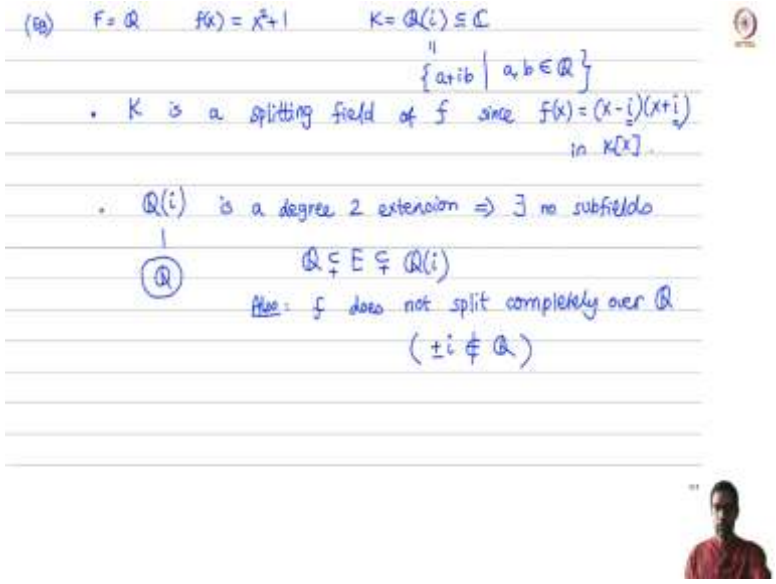
So that is in fact, an element of the ground field F. So, this is the leading coefficient of F, coefficient of the highest term x power n, this is of course, an element of F. So, the condition one is really that it should factor completely into linear factors. In other words, there are n

roots for this polynomial in the extension field K. Secondly, this property does not hold for any smaller sub field.

So, in some sense, K is the smallest. Let us write that out precisely f of x does not factor, does not factor completely into linear factors in let us say, Eof x, where, for any subfield, what is E? E is a subfield which contains F, but it is a proper subfield. So, this is a proper, so by this, I just mean E is a proper sub field of K which contains F, proper sub field containing F.

So, these are the two properties that you need for a field K or an extension K to be called a splitting field.

(Refer Slide Time: 04:09)



So now let us give some examples. So here are some easy examples of splitting fields of polynomials. If I take my field to be the rational numbers, and my polynomial to be x square plus 1, then the splitting field turns out to be something that we have seen before in the earlier lecture. So, this is the the field of Gaussian integers, or rather the the field of, you know, rational numbers with the Gaussian rationals if you wish.

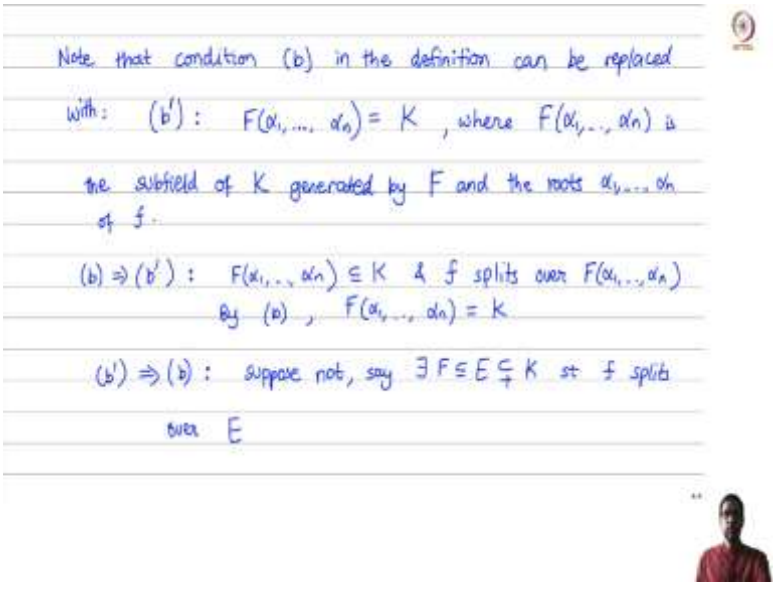
So, it is it is all, so we know what this is. This is a set of all a plus ib, a and b running over the rational numbers. And why is this field a splitting field in this case? So, we need to check the two conditions. So, I claim, that K is in fact, a splitting field, K is a splitting field of this polynomial f, field of f, because, well, first property, f should split into linear factors over K, and that is satisfied because this polynomial splits as x minus i into x plus i.

And the i that now appears here is after all an element of this field, so you can think of this as the factorization of f of x in the ring K of x, where K is now the field Q of i. Secondly, second property, which we need is that they should somehow be the smallest that this property should not hold for any intermediate subfield, or a proper subfield. But recall, again, from what you have seen before, that the extension Q of i over Q is of degree 2. This is the degree 2 extension, which means that you really cannot have any subfield.

So there exists no subfields E, which are strictly between Q and Qi, strict intermediate subfield does not exist, because 2 is a 2 is really a prime number. And you have seen this property of degrees of extensions are multiplicative. So, when you have a degree 2 extension, it does not admit any any subfields. So, there cannot be ease which are strictly between Q and Qi and of course, for equal to Q itself this you know, the polynomial f does not split over Q.

Also, we need to check that Q itself is not going to work and that is clear here observed that f does not split completely over Q, because what are the two roots plus and minus i they are not in Q. So, you cannot factorise it completely into linear factors over Q. So, what does that mean? It this this extension K also satisfies the second property that you need, the only proper subfield of Q i is Q itself, and the polynomial f does not split completely over Q. So, that proves that K is the splitting field.

(Refer Slide Time: 07:33)



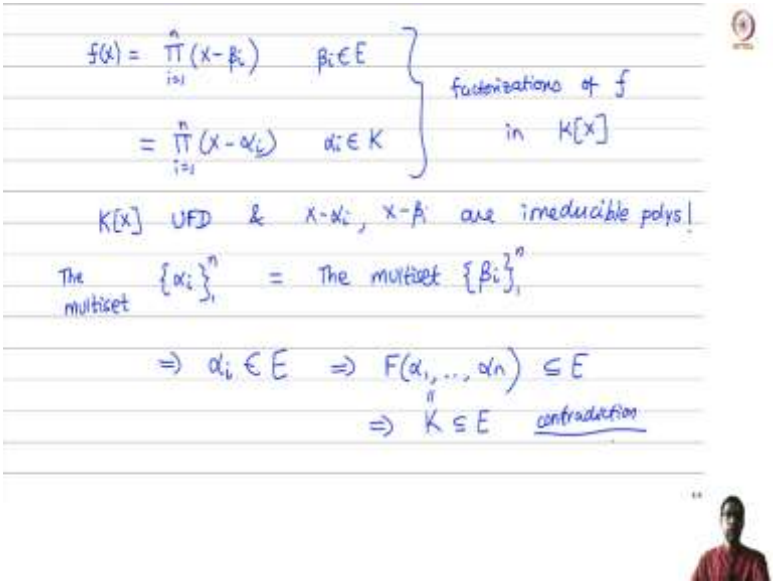
Note that condition two or condition b in the definition can be replaced with an equivalent condition. So, let us call that b dash, this is now called condition b dash, which is the following that F of alpha 1, alpha 2, alpha n equals K where, what is F of alpha 1 through

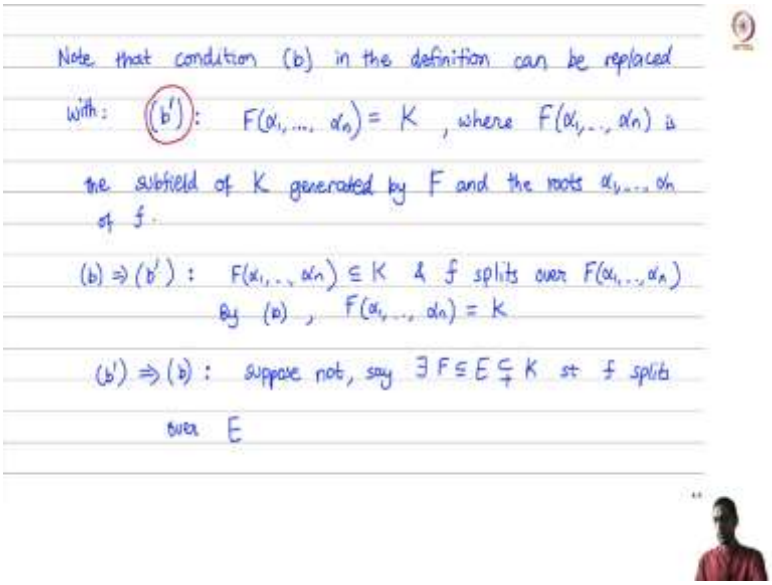
alpha n this is just a, is the subfield of K generated by by F and the roots alpha 1 through alpha n of smaller f. And it is easy to see that you can replace b with b dash, meaning they are equivalent.

For example, if you chose to keep b as your definition, then b dash follows naturally because of the following reason, b says that there are no intermediate subfields, there are no proper sub fields over which the polynomial f splits completely. Now, if you assume that then b dash follows because of the following that f of alpha 1 through alpha n will in fact be a subfield of K over which, this is a subfield of K and the polynomial f certainly splits over this subfield.

So, by the hypothesis of b, this this cannot happen unless this sub field is the whole field. Now, similarly if you chose to keep b dash as your definition, then b follows as we will see in just a second. So, let us proceed by contradiction. Suppose b is false, suppose not, so what does that mean? Say there exists an intermediate subfield. So, let us say E which is a proper subfield of K and E containing F, such that f splits over E.

(Refer Slide Time: 10:17)





Now what does f splitting over E mean? Well, it just says the following that you can write f of x, again, so let me ignore the the leading coefficient of f, I am just going to assume it is leading coefficient is 1, that it is a monic polynomial. So, let me write f as the product of x minus beta i, beta i is coming from the intermediate subfield. And so, this is of course, because we have assumed now that f splits over E.

Now observe that this is on the other hand, we also know that x is the product of x minus alpha i's. And now the alpha i's are coming from the ambient field K. Now, these two different factorizations, so these are both factorizations. You can think of these both as factorizations of f in the ring Kx. Because E is, after all a sub of K, I can think of the first expression also as being a factorization over K of x.

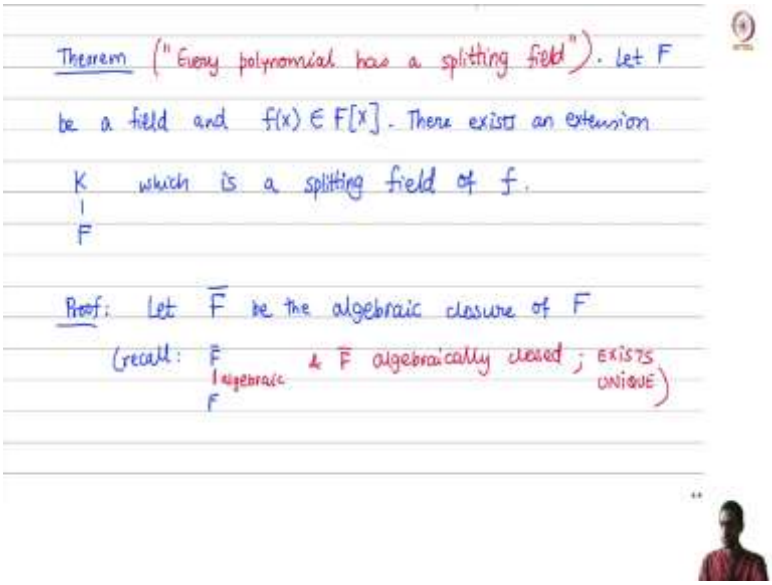
So now I have two different factorizations in the ring K of x, but that is K of x is a unique factorization domain. And each of these x minus alpha i's or x minus beta i's, they are all just linear polynomial. So, they are definitely irreducible polynomials. And if you have two different factorizations, then that, you know, the only possibility is that they really coincide with each other.

So, K of x is a UFD, Unique Factorization Domain and all the terms here are just linear x minus alpha, x minus beta etc, are definitely irreducible polynomials. So, what does that mean? This means that these two factorizations are the same. In other words, if I take well, alpha i 1 to n, well, there are potentially repetitions here. So, let me call this the multi set. By which I mean you also keep track of how many times each alpha i appears, the multi set of alpha i's must coincide with the multi set of beta i's.

In particular, what does that mean? This means that all the roots are actually in the smaller sub field inside E, because each alpha i is the same as some beta j. And the betas of course are in E. So, all the alphas are in E. And what does that mean? It means that the subfield generated by F and the alphas is also contained in E, because F is of course, already in E and all the alphas are now E according to this, but what does that mean?

Well, we assumed according to b dash, that K is the same as this sub field. So, we conclude that K is a sub of E, and that is now a contradiction, because to begin with K was, or rather E was a proper subfield of K. So, this is just to say that, you know, sometimes it is more convenient to use this characterization b dash, rather than b itself, but they are really the same thing. So, let us move on.

(Refer Slide Time: 13:50)



So here is our main theorem in some sense. One of our main theorems in this really says that every polynomial has a splitting field. So, every polynomial has a splitting field. That is in words, but let me make that bit more formal. So, let F be a field and let f of x be polynomial, and there exists an extension K of F, which is a splitting field of f. I mean, I could have just said there exists K which is a splitting field of f, because being an extension is of course part of the definition. I will just state it for more clarity.

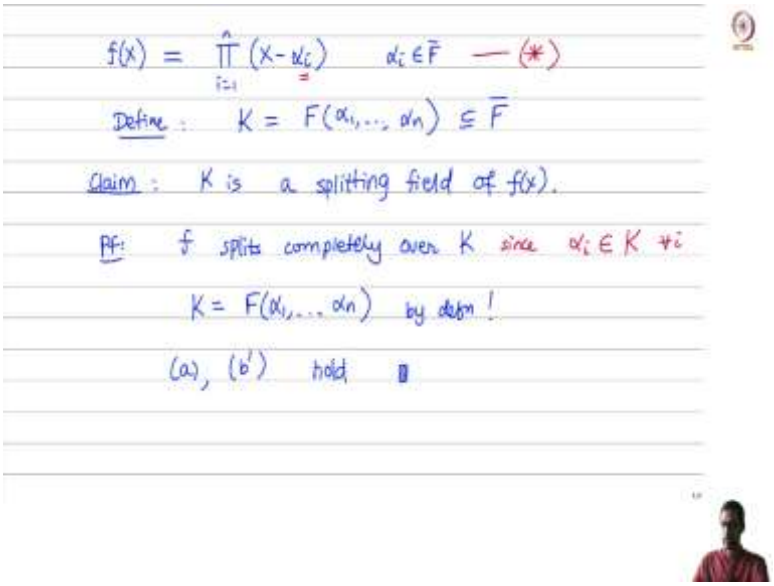
So here is the proof. How does one construct a splitting field? So well, we need to remember to do two things. One, we need to find a field over which f splits completely into linear factors. And that field is, well, one such field is definitely already available to us something that you have seen before. And this is the algebraic closure.

So let, let us begin with that as our first approximation, let F bar be the algebraic closure, of the field F. So, recall that such a thing exists. So, what is the algebraic closure? It is an extension of F, which has two properties, number one, that this this extension is an algebraic extension. And F bar is algebraically closed, which means that any polynomial with coefficients in F bar will have all its roots in F bar.

Example, classic example being the field of complex numbers itself. And F bar algebraically closed. That is the definition of the algebraic closure. And recall, the two main facts that given any field F, there exists an algebraic closure. And it is essentially unique, and by essentially, I mean, abstractly, there could be many algebraic closures, but any two algebraic closures are isomorphic to each other by an isomorphism, which is identity on the field F. So, recall this from what you have seen before.

Now, F bar already gives us a first approximation to what we want to a splitting field.

(Refer Slide Time: 16:58)



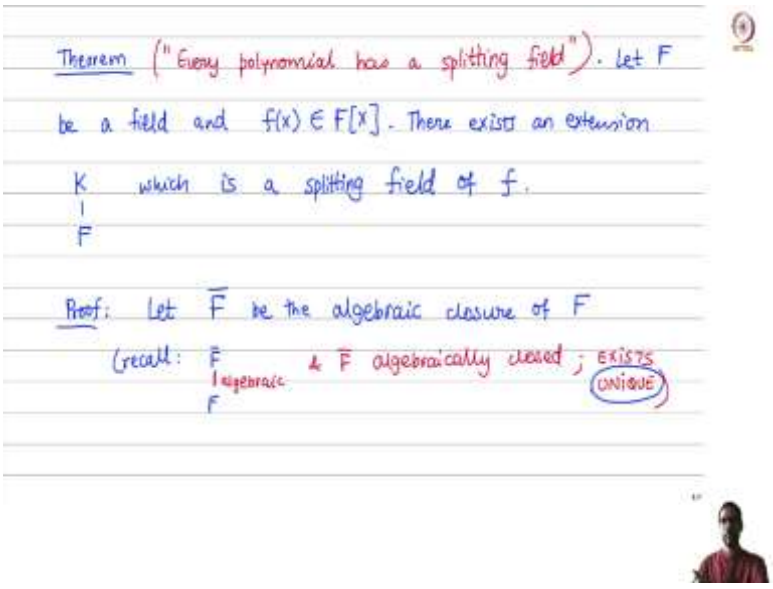
So, let us just take this polynomial F, we know for sure, it splits over F bar. So, we can write it as a product of linear factors, alpha i, i equals 1 to n, where alpha is coming from the algebraic closure. Now define the splitting field, then, remember, we have our property b dash, so it sort of tells us what we should do in order to construct the splitting field. Inside the algebraic closure, we just take the subfield which is generated by F, and these end roots of this polynomial small f.

So, we have a candidate now, which is, you know, inside the chosen algebraic closure. And now it is just a question of checking the properties claim K is a splitting field of this polynomial fx. Proof, well, number one, it is obvious that f splits over K, splits completely over K is clear, because because well, this expression here that that we wrote out, this star holds, I mean, it splits completely.

Now the point is that the alpha i's that we have, they are, by definition elements of K. Since the alpha i's are all elements of K. So that is the first property. And secondly, let us check axiom b dash instead of b. Well, because that is really how we we constructed K and so, observe that K is by definition the subfield of itself which is generated by F and the alpha 1 through alpha n.

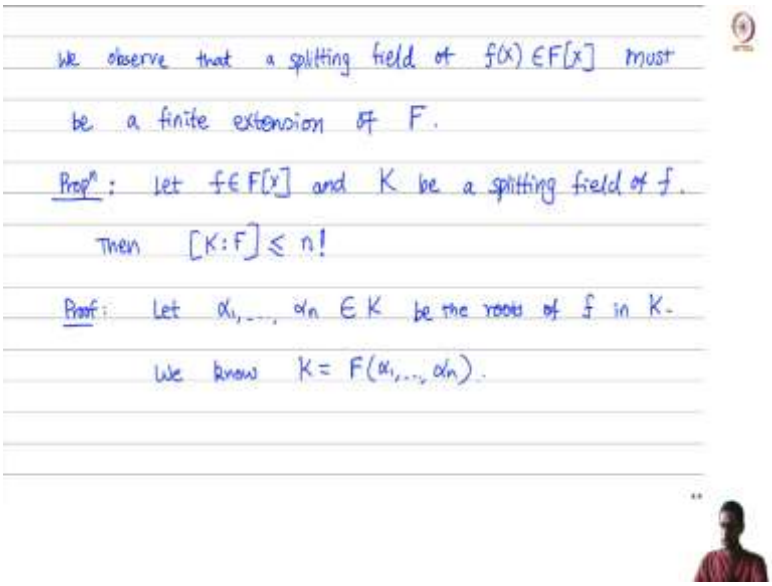
So, this more or less by definition, follows follows quickly from from the way we defined it. So, which implies that we have checked the axioms a and the axiom B dashed hold. So, we are done. So, that proves that K is a splitting field.

(Refer Slide Time: 19:19)



Now, analogous to what I just said about algebraic closures that not just they exist, but they are unique, meaning essentially unique there exists isomorphism between any two algebraic closures, which restricts to an identity on F. Now, we will show the same same result is true for splitting fields as well. If you fix a polynomial small f, the splitting field is essentially unique, there is really only one splitting field up to an isomorphism which is identity on the base field.

(Refer Slide Time: 19:55)

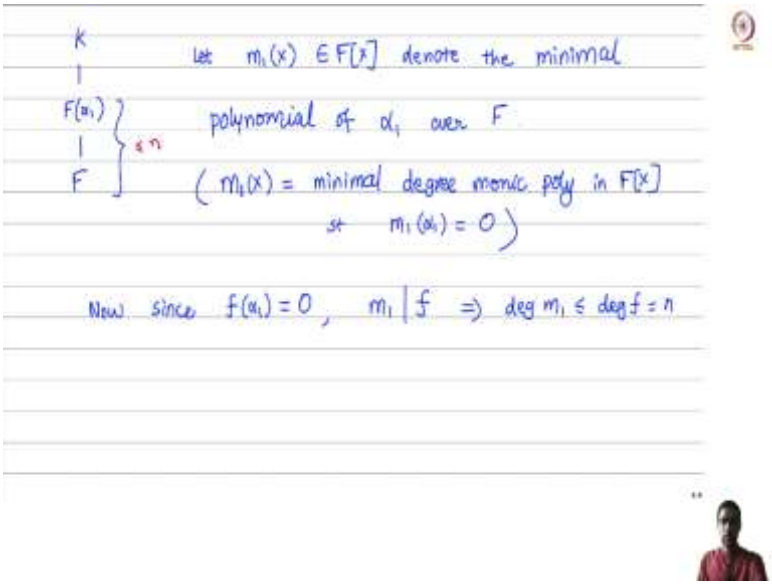


But before we do that, let us prove some other simpler properties of the splitting field. So, we observed before proving the uniqueness that the splitting field is, splitting field is necessarily a finite extension. Splitting field of the polynomial fx is or must be a finite extension of the field F.

In fact, here is a more quantitative proposition, it says, let f be a polynomial, and K be its splitting field, a splitting field, we still have not shown uniqueness, be a splitting field of f, then then not only is K a finite extension of F, we also have a bound on the degree of the extension. It is it is finite on the degrees at most n factorial.

So, let us prove this, proof is rather easy. Now what do we know? We know that K is a splitting field. So, let us write out the roots, that alpha 1 to alpha n in K be the roots of this polynomial f in the field K. We know the following. We know that K is just F of alpha 1, alpha 2, alpha n. So, let us sort of go in go in stages.

(Refer Slide Time: 21:58)

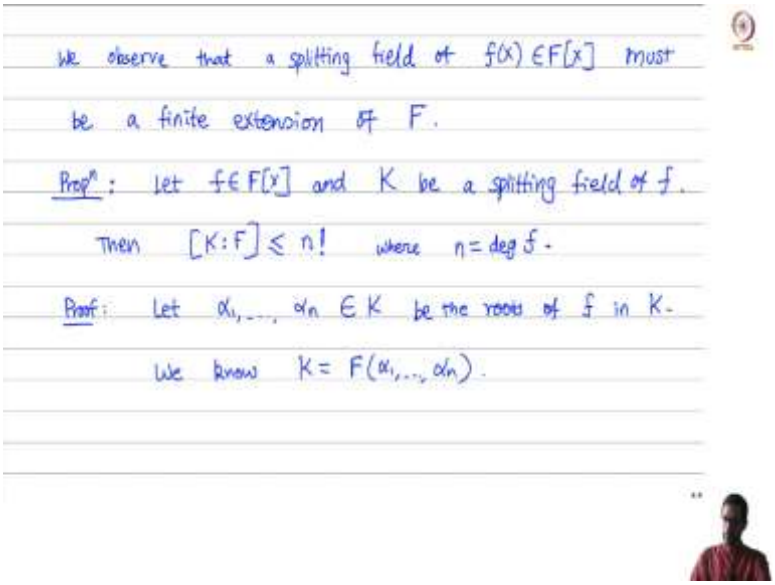


So, let us take the very first one of the alphas, so considered alpha 1. So, let us say look at just the first fellow, alpha 1 alone and look at the extension. So, adjoin alpha 1 to F, and look at the field F, adjoined alpha 1, think of it as an extension of F. So, in some sense, all of this is really inside K. So, I should probably just say, this is really a subfield of K as well.

Now, let us, let us do the following. So, we will eventually show as K is finite by building it up as a tower of extensions. So, let us look at this very first guy, F alpha 1 over F. So, let m1 of x in Fx, denote the minimal polynomial, by which I mean the minimal degree irreducible polynomial satisfied by alpha 1, denote the minimal polynomial of alpha 1 over the field F. So, I can also assume it as monic.

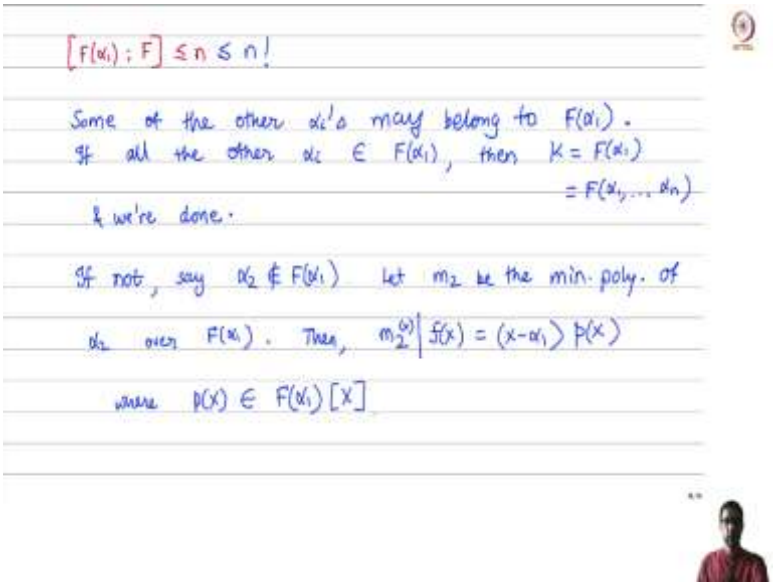
So, what is m1x, recall, this just means m1x is the minimal degree monic polynomial in Fx satisfied by alpha such that m1 of alpha 1 is 0. Now, since f of alpha 1 is 0, what this means is that m1 must divide f, because the minimal polynomial certainly divides any other polynomial, which annihilates alpha 1. So, in particular, this means that the degree of m1 is at most the degree of f, and the degree of f is what I am calling n by the way.

(Refer Slide Time: 24:08)



So, I should probably have said that in the definition, where n sorry equals the degree of the polynomial f. So, at the very first step the first extension has degree that is at most n. So that is the first observation, this degree is at the most n. Now, let us see where we are, where does this leave us?

(Refer Slide Time: 24:39)



We have at least gotten one of the roots in play F of alpha 1over F. But when I construct this extension F alpha 1, many of the other root's alpha 2, alpha 3, some number of the other roots, may already be part of this extension.

For example, maybe alpha 2 is equal to alpha 1, or maybe alpha 2 is minus alpha 1 or some polynomial in alpha 1, say alpha 1 square plus 2alpha 1 plus 3 or something like that. So, some number of the other roots may already be part of this extension, F alpha 1. Now, if all the other roots are part of F alpha 1, then you are done because F alpha 1 itself is the full extension K. But suppose now.

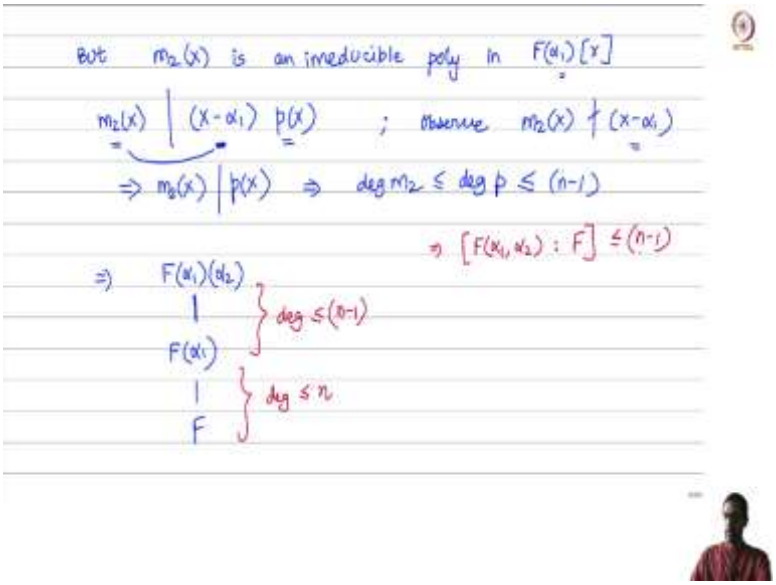
So, let us write out what I just said. So, some of the other alpha i's may already belong to F alpha 1. Now, if all of them belong, then you are done, if all the other alpha i belong to this extension, when that just means that K is just F alpha 1 itself, because K remember is F of alpha 1, alpha 2, alpha n. And we are done. Why are we done? Because we have shown that the extension size is at most n and n is definitely smaller than or equal to n factorial.

Now, if not suppose, if not, at least one of the other alphas is not part of F alpha 1, let us say alpha 2 is not part of F alpha 1, say alpha 2 does not belong to the extension F alpha 1, then we sort of repeat the argument. So, let m2 now denote be the minimal polynomial abbreviated to mean poly of alpha 2 over the extension F alpha 1.

So, then again, by the same reasoning as before, m2 is the min poly for alpha 2, F is a polynomial, which you know F such that F alpha 2 is 0, so, m2 must divide f. But what is f now? So, let us just look at f of x, f of x looks like this, we know for sure that, alpha 1 is the first root that we wrote out. So, it is x minus alpha 1 into some polynomial P of x.

So, let me, let me factorise f like this x minus alpha 1 into P of x, where P of x is a polynomial with coefficients in the field F alpha 1. So, of course, when you go to K, P of x will be the product of the other factors x minus alpha 2, alpha 3 and so on. But, you know, because alpha 1 belongs to the field F alpha 1, I can pull out that factor alone and think of the remaining factors as being some polynomial in F alpha 1 of x. So, m2, this polynomial m2 of x must divide x minus alpha 1 into P of x. So, this is just the factorization in this polynomial.

(Refer Slide Time: 28:16)



But now observe that but m2 is an irreducible polynomial because it is the minimal polynomial in this ring F of alpha 1 of x. And this first factor, so here is an irreducible polynomial, which divides a product of two polynomials x minus alpha 1 into Px. So clearly m2 of x does not divide the first factor, because, well, the first factor is just a linear factor.

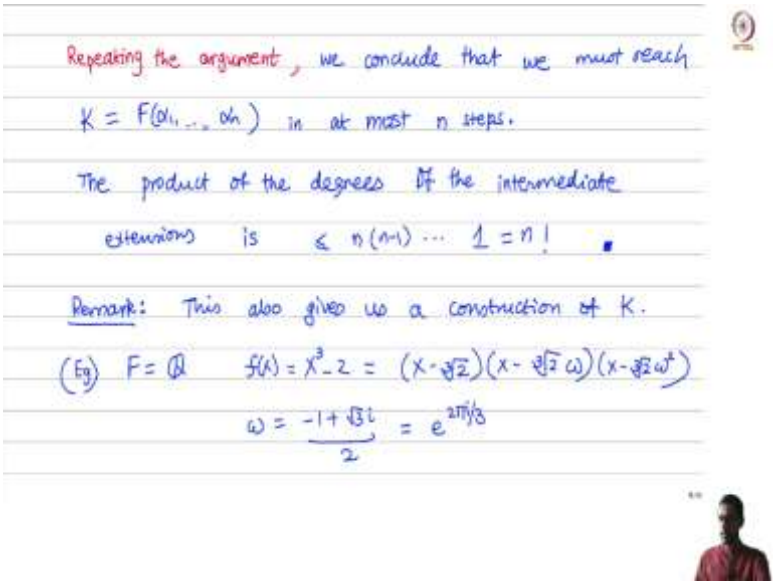
So, observe m2 cannot divide the first factor in fact, it is relatively prime to the first factor, because, you can just think of the this as being an irreducible polynomial of degree one in this this field F alpha 1 of x in this ring F alpha 1 of x. So now, what does this mean again? I mean, you can think in terms of the fact fact that m2 of x is a prime element of the ring F alpha 1 of x or in terms of the unique factorization, the fact that this is the UFD and so on.

So, the point is these two are relatively prime to each other. So, therefore, m2 of x has to divide the other term which is P of x. So, what does that mean? That means that the degree of m2 is at most the degree of P and the degree of P is at most n minus 1 because, the fact the factor x minus alpha 1 has already been pulled out of F, what is the meaning is of degree at most n minus 1.

So, what does this mean? This tells you then that when you look at the extension, so I had F alpha 1. And now I adjoined another element alpha 2 to it, to form a further extension, this new extension that I have formed has this has degree, at most, n minus 1, because it is at most the degree of P, and this we had already seen has degree at most n. So, this means F of, so, by

the way F alpha 1 adjoined alpha 2 is just what we call F adjoint alpha 1, alpha 2. And it is the same thing really. So, this degree is at most n minus 1.

(Refer Slide Time: 30:52)



And now, it is clear what we need to do, if you repeat the same argument repeating the argument, maybe some of the other alphas are now already part of F alpha 1, alpha 2, but if not, you can adjoin that additional alpha and the minimal polynomial of the new alpha that you are joined will be at most n minus 2 for the same reason, because you now pull out both at x minus alpha 1 and x minus alpha 2.

So, repeating their argument, here is what we conclude, we conclude that we must reach K, which is the entire splitting field in at most n steps, because you cannot join one at each each step and in you may not need n steps in some of the intermediate steps, some of the other alphas may automatically be part of this.

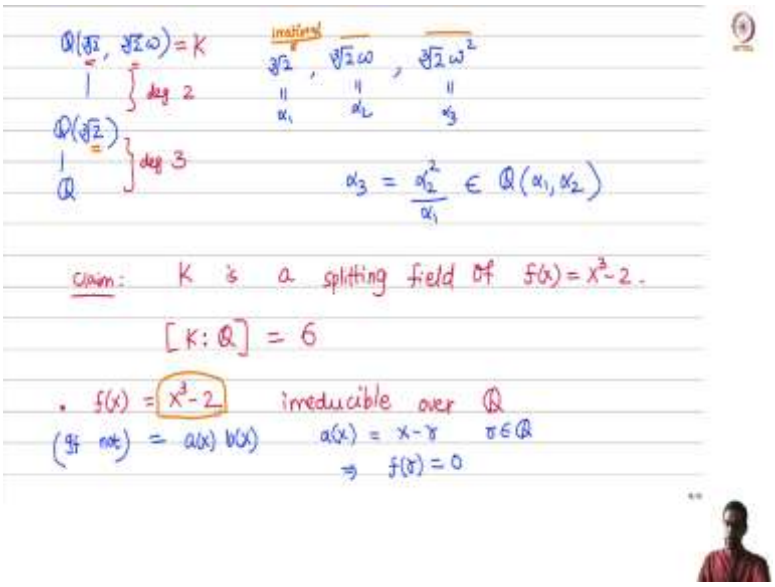
So, but, the worst case is that you need n steps, and at each step the degree that you get is n at most, at most n minus 1, at most n minus 2 and so on. So, the product of the degrees involved therefore, is degrees of the intermediate extensions is at most n into n minus 1 and so on till 1, which is n factorial. So, that is the, that is the end of the proof.

In fact, thing to note here remark is that we actually have also seen, I mean, in the course of the proof, sort of a way to construct the splitting field if you will. So, remark this also gives us a constructive way of, also gives us construction of F of K, this particular field. What do

you do? At each step you adjoin one at a time. And then you see how many of the other roots still have not fallen into the extension at that point and then you adjoin that root.

So, for example, if I took the field F to be Q, and my polynomial f of x to be x cubed minus 2, which we know factorises like this x cube, x minus cube root 2 x minus cube root of 2 omega and omega square. So, this is over the complex numbers, where omega is a cube root of unity. So, let us write it as minus 1 plus root 3i by 2 is the cube root of unity.

(Refer Slide Time: 34:02)



Then, here is what we can do to construct the splitting field step by step in some sense which is that you first adjoined the first root. So, I can I can say, I have Q of cube root 2. Now, at this stage, what I find is that the other two roots, which are cube root of 2 omega and cube root of 2 omega square, they are, in fact they are complex, they have a non-zero imaginary part and they are not part of this extension at this point.

Q of cube root of 2 is certainly part of the real numbers. There are no, everything here has imaginary part 0. Now, what we can do is say, fine, I have two more left. So, let me adjoin one of them. So, I can try and adjoin, push this down. So, I look at now adjoining Q cube root of 2 with cube root of 2 omega.

Now the point is when I adjoined this additional guy then turns out that the third fellow is automatically part of this extension. Why is that? So, let us just give these fellows names again, cube root of 2 is alpha 1, this is alpha 2, and let us say this is the third root alpha 3. Observe that, how do I get alpha 3? Alpha 3 is just nothing but alpha 2 square divided by

alpha 1. So that is exactly the the relationship among these three. So that just means that alpha 3 is actually some polynomial combination of, well, I mean, it is in the field. So, I am also allowed to divide if you wish, so it is, it is some combination of alpha 1 and alpha 2 here.

So, this is certainly in the field generated by, this over Q. In the field generated by alpha 1 and alpha 2. So you do not need to do one further step of extension here, you will not need to go one more step. So, this is this is sort of a constructive way of just understanding what splitting fields are. And in this case, so this is the thing that we obtained at the end here.

Let us call that K. Let us call that K here. So, this K is in fact, the splitting field. So, claim, K is exactly the splitting field. K is the splitting field of, well, it is a splitting field of this polynomial fx. So, it is clear that it is a splitting field, because number one, it splits, the polynomial splits over this field certainly, and the roots of this polynomial generate this this field K, more or less by definition. In fact, the first two roots are enough to generate the whole thing. So that is easy.

But the second part of the claim is that here K, Q is, in fact, well, it is actually 6. So, we claim that the, in this case, the degree of this extension is 6. And that is something that one needs to verify. It requires a little, little proof. So, let us just do that quickly. So, I claim that this very first extension has degree 3. And the thing on top has degree 2. So, we just need to verify these two things, and that will show that it is 6.

So why does the first extension have degree 3? Because if I take this polynomial f of x equals x cubed minus 2. So here are some facts. This is actually irreducible over cube This is an irreducible polynomial. So that is fact one. Why is this irreducible over Q? Well, it is a cubic polynomial. If it were not irreducible, then it would factor into, there will be at least two factors, you will have to write it as some a of x into b of x.

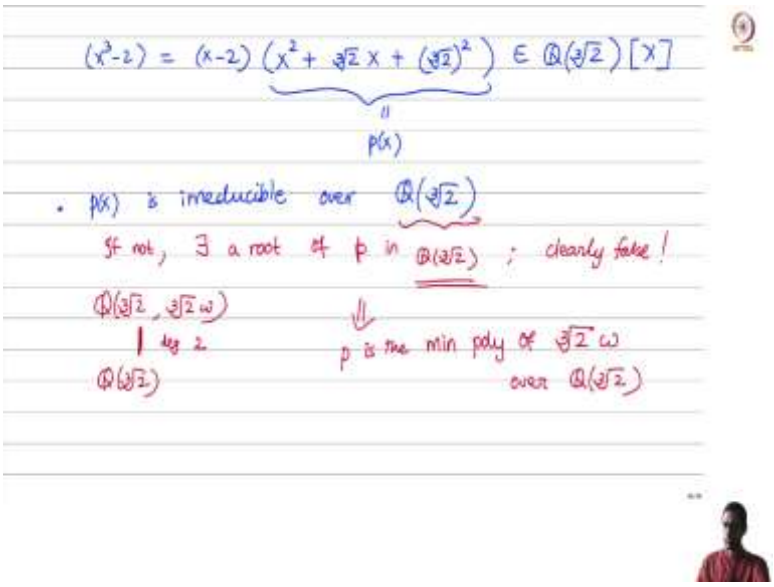
So, I am just giving you a quick proof of why it is, it is irreducible, if not f can be written as a product ax, bx, and since the total degree is 3, at least one of them is a linear polynomial, one of them has to be degree 1, the other is degree 2. So, what does this mean? This means that a of x therefore let, let me assume a of x is a linear polynomial, it looked like some x minus some gamma, where gamma is a element of Q.

In other words, there is a root gamma. In other words, gamma is the root of this polynomial. So, which means then, that f of gamma is actually 0, because a of gamma 0 and so f gamma

is 0. So, a cubic polynomial, which is if it is not irreducible over Q, it must have a root in Q. And one can easily check that none of these three fellows is in Q. I mean, it is clear that this is irrational. Maybe one has to give a short proof of that. But since cube root of 2 is irrational, it is not in Q, and these two, these two are clearly not in Q, they have some imaginary part.

So, you cannot have any any of the roots be in Q, which means that this polynomial must be irreducible over Q. So that shows that the first element you adjoined, which is cube root of 2, it is minimal polynomial has degree 3, it is minimal polynomial is exactly this. Therefore, by what you have seen before, when you adjoin a single element, the degree of the extension is just the degree of its minimal polynomial. So that is degree 3.

(Refer Slide Time: 40:00)



Now for the second guy, we need to check that it is it is a degree 2 extension. And again, there it is just a question of figuring out what the minimum polynomial looks like. So, observe x cubed minus 2 is, can be factorised as follows x minus 2 into x squared plus cube root of 2x plus cube root of 2 the whole square. This is just the factorization and this is a factorization with coefficients coming from the field Q cube root of 2.

Now, this polynomial here, so this polynomial, so let us call it P of x, so observe P of x is an irreducible quadratic polynomial. So, it is it is irreducible over this field Q cube root of 2. Again, why? Same reason, if it is reducible, then it must have a root in the field Q cube root of 2. So again, reason if, if not, and there exists a root of P in this field Q cube root of 2.

But clearly that is, that cannot happen because the roots of P are the other two roots, cube root of 2 omega and omega square and they are, they all have imaginary parts. So, the other two roots do not, clearly do not belong to this this sub field Q cube root 2. So that is clearly false. So, what that means again is if I take this Q cube root 2 and I adjoin this additional element cube root of 2 omega to it, this cube root of 2 omega satisfies the polynomial P and that polynomial hs degree 2 and it is irreducible.

That means that the degree of the extension is also the same as the degree of its minimal polynomial. So, this means that P is exactly the minimal polynomial of cube root of 2 omega over the field Q of cube root of 2. So, the degree of the extension is 2 and well that is all we needed to prove, and the total extension has degree 6. So, we are done.