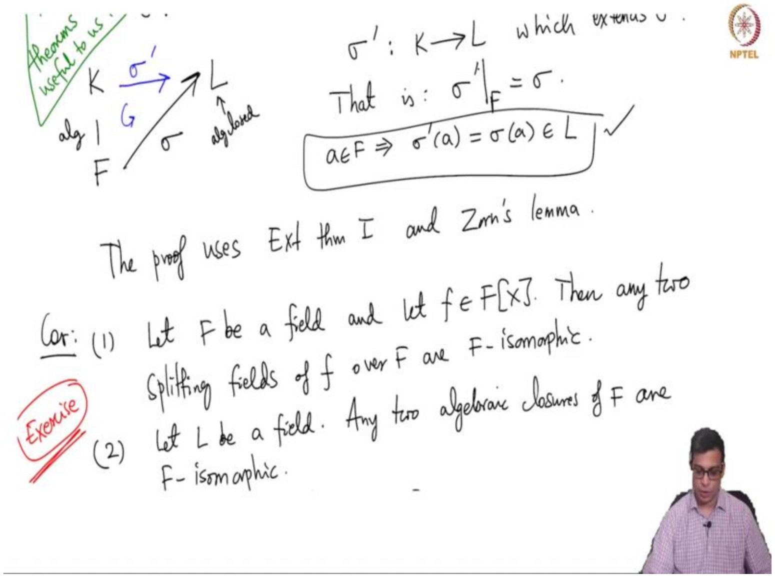
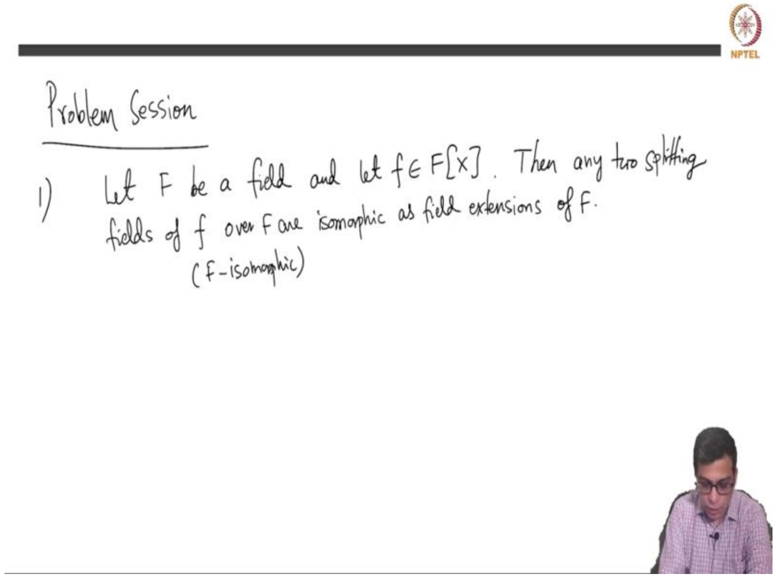
Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 08
Problem Session I

(Refer Slide Time: 00:15)



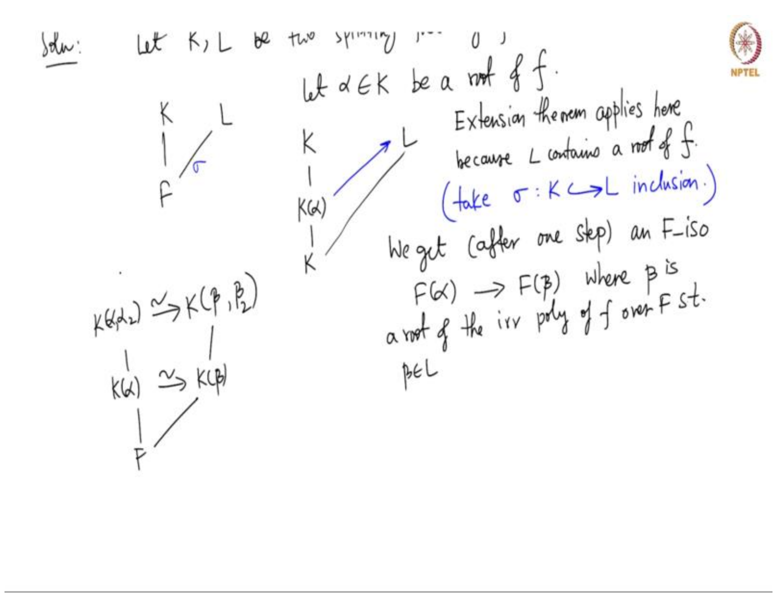
Welcome back. In the course so far, we reviewed the required material from groups, rings, fields and I am ready to start Galva Theory. But before that let me do a couple of problem sessions so that you understand how to solve problems and also recall some important concepts from field theory. So, I will mostly stick to field theory problems. So, let me start with the problem that I gave at the end of the last video, this exercise that I have written here. So, you recall that we proved a couple of extension theorems and we talked about algebraically closed fields. So, the first exercise today.

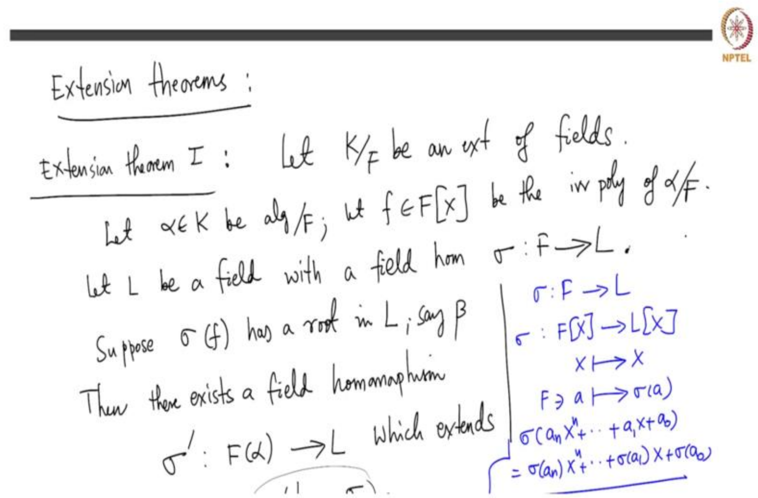
(Refer Slide Time: 00:56)



So, today our problem sessions, so the first problem is let F be a field and let small f be a polynomial over that field, then any 2 splitting fields of f over F are isomorphic. So, I am not going to isomorphic as S field extensions of F not just abstractly isomorphic S fields but as field extensions of F that is they are F isomorphic

(Refer Slide Time: 01:50)





So, I am not going to do the full details of this because it is essentially an immediate consequence of the extension theorems that we proved. So, let me set it up and I need some details you can provide yourselves. So, let and K and L be 2 splitting fields of small f or big F. So, here what we have is this. They are both extensions of F. So, by definition a splitting field is an extension of F where the polynomial splits completely and those extensions are generated by the roots. So, now let alpha be in K, be a root of F. It has all the roots so it has, let us take 1 of them. So, what we have is actually a picture like this.

Now if you recall what the first action extension theorem says, first action, first extension theorem applies here and gives a map like this which extends the map from K to L because the reason it extends here is because L contains a root of f. If you go back to the first extension theorem, you have some arbitrary field extension on algebraic element in the bigger field. You have an irreducible polynomial.

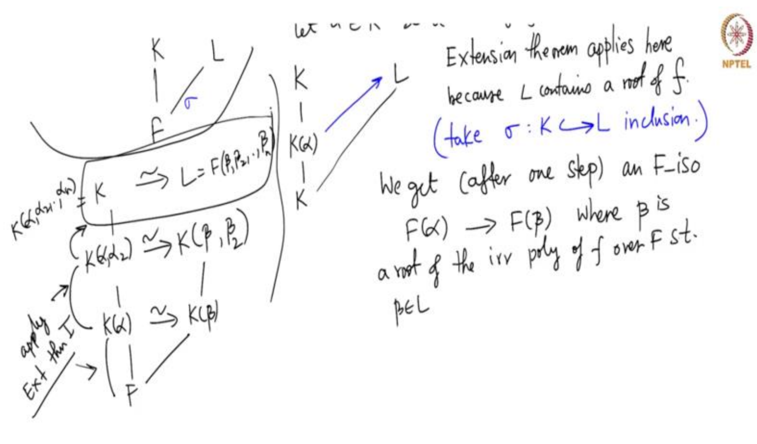
So, the given polynomial in our problem may not be reducible but we can take the irreducible polynomial of alpha which will be a root of f. So, those are details that you can fill in. And in general, we actually worked with an arbitrary field L and the homomorphism such that sigma f has a root in beta. So, here I am going to take sigma to be identity. So take, I mean sigma to be the inclusion. So, sigma is just this, sigma exists already because it f is a subfield of f.

So, with that, what you have is an extension. So, you can extend it and then if you go back to the proof or rather the explanation that I gave without really proving it in detail is that this extension here takes f alpha to f beta. So, f prime is the image in general. But f prime is f here.

So, f alpha, so we get basically after 1 step, an isomorphism, an F isomorphism f alpha to f beta where beta is a root of the irreducible polynomial of f over capital F such that beta is in L. So, remember F may not be reducible. So, f may have factor as irreducible factors like this and this may be the irreducible polynomial of alpha over f let us say. Then because f splits completely in L, so it has f1. So, f1 also has a root and you apply technically you apply the extension theorem to f1 alpha and capital L.

So. then what you get is K alpha as isomorphic to K beta over F and then you keep going. So, K alpha, alpha 1, this alpha can be thought of as alpha 1. So, then you get an isomorphism from K beta, beta comma beta 2. So, this is an extension and then you keep going. And you keep going. So, I am a bit fast here. But ultimately what you can do is this is isomorphism from this to this because K is nothing but K alpha, alpha 2, alpha n. L is nothing but f beta, beta 2, beta n.

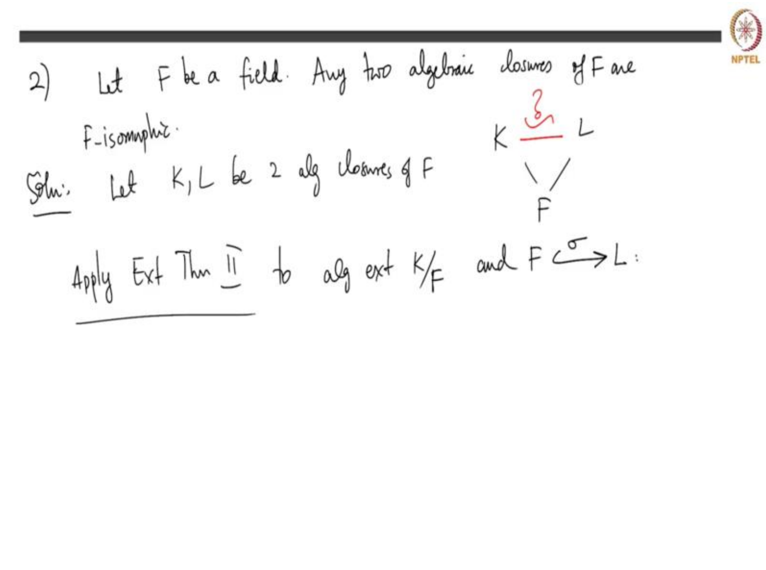
(Refer Slide Time: 06:40)

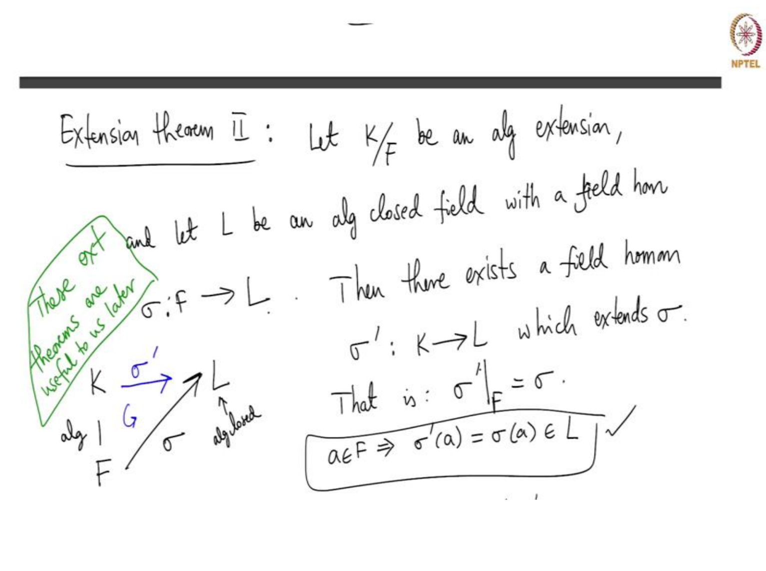


So, you can also check that these roots, number of roots are the same as part of this process. First you show that this is an isomorphism then you apply extension theorem again. So, apply extension theorem to this, extension theorem again to this. Here, we applied it and gotten this isomorphism, apply it again, apply it again and so on to get this. So, this is the statement that any

2 splitting fields are isomorphic. So, I am just going over this fast because this is something that you can think about. You will understand more if you actually think and supply all the missing details.

(Refer Slide Time: 07:16)

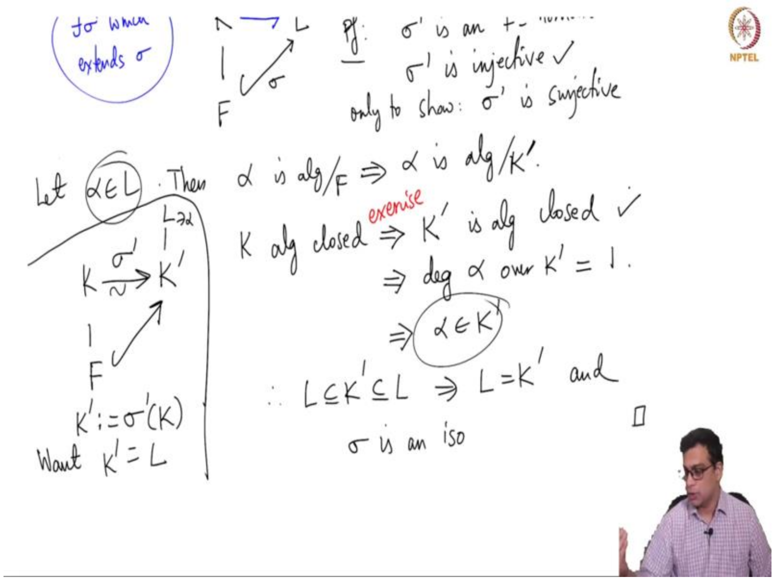




So, now let me do the second problem that I gave last time which is also an immediate consequence of the extension theorem. So, let f be any field, any 2 algebraic closures of f are F isomorphic. So, what I am saying is that, so again I will, I would not go to details. But let maybe not the full details I mean. Let K and L be 2 algebraic closures of F. So, we have K and L and they are both algebraic closures of F. Our goal is to show that there is an isomorphism over the field f so that means, that means there is an isomorphic which fixes f point wise, that is important for us. So, this is also easy.

Because apply now, extension theorem 2. And if you recall what is extension theorem 2 say, if you have any algebraic extension and a algebraically closed field L of F, then there exists a map from K to L which extends sigma. So, here of course sigma is inclusion map. So, basically apply this to algebraic extension K over F and the inclusion of F in L. So, this is sigma.

(Refer Slide Time: 08:57)



So, then by the extension theorem, it gives us a map. This remember is the map, is the inclusion map. So, it is not an arbitrary I mean, it is actually an inclusion of F in L. F sits inside L as a subfield then by the extension theorem there is a map like this, sigma prime I think I called. So, there exists sigma prime which extends sigma. So, that is the conclusion of the extension theorem.

Now I claim sigma prime is the desired isomorphism, F isomorphism. The proof is clear. First of all sigma prime is an F homomorphism because it extends the sigma and sigma is an inclusion of F in L. So, any element of F goes to itself. So, sigma prime fixes capital F. This is, sigma prime is injecting or 1, 1 in other words. This is because any field homomorphism is so, so it is an injective map only to show sigma prime is surjective. If it a surjective map from K to L, it is also an injective map so it is an isomorphism.

And this is clear because let us take any arbitrary element alpha in L. So, what we have is, of course alpha is algebraic over F because remember, algebraic closure is an algebraically closed field which is an algebraic extension of the Bayes field. So, L is algebraic over F. So, that means alpha is algebraic over F that means alpha is algebraic over K. So, let me just set up some more notation here.

So, we have F, K, sigma prime. Let us say it goes to K prime which is in L, just sticking to the notation that I normally do. I will denote it like this. So, K prime is the image of sigma prime. So, K prime is equal to sigma prime of K. So, we want K prime equals L. So, that is my goal but apriori maybe K prime is a smaller field than L. It is simply the image of the map sigma prime that exists by the extension theorem.

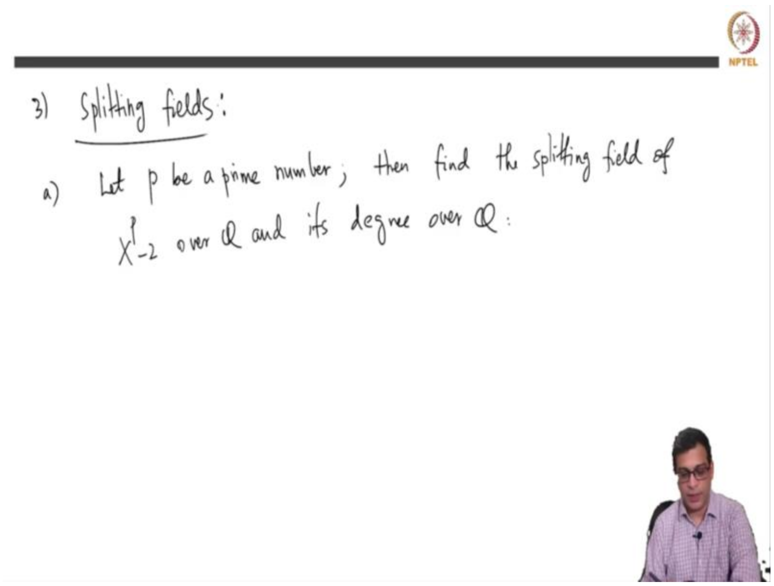
So, I am picking alpha here, alpha is algebraic over rather alpha is algebraic over F. So, I should really say alpha as an element is algebraic over K prime because if alpha is algebraic over F, it is it has it satisfies the polynomial ()((12:04)) in capital F. That polynomial belongs to capital X, K prime x also. So, alpha is algebraic over K prime. Now we use another set of implications, so K is algebraically closed. So, so far we have used that L is algebraic over F because that is we have also used L is algebraically closed in order to apply the extension theorem.

Now we are using L is algebraic over F here. We have also already used that K is algebraic over F in order to use extension theorem. Now we are going to use K is algebraically closed. So, both facts for L namely that it is algebraically closed and it is algebra over F are used for L as well as for K. So, you remove any of those properties, this proof will not work. So, K is algebraically closed implies K prime is algebraically closed. This is a fairly easy exercise. Algebraic closure is preserved by a field isomorphism.

Remember sigma prime is an isomorphism onto K prime. So, if every polynomial non-constant polynomial in K has a root, then every non-constant polynomial K prime has a root, so that is easy. K prime is algebraically closed and that means degree of alpha over K prime is 1 because that is the meaning of algebraically closed field. So, alpha is algebraic over K prime, so it satisfies a polynomial of K prime. Take the irreducible polynomial of alpha over K prime. But the only reducible polynomial of K prime, over K prime are linear polynomial. So, that means degree of K prime, degree of alpha over K prime is 1 that means alpha is in K prime.

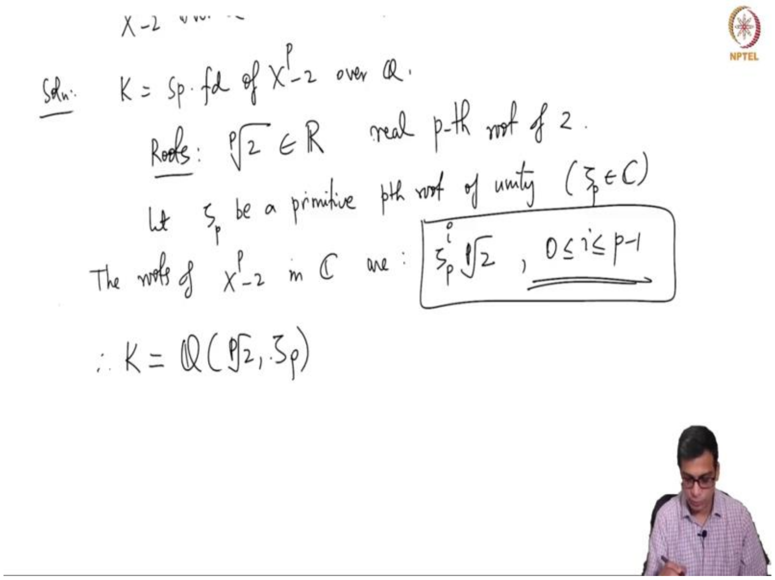
So, we have taken an arbitrary alpha in L and concluded that it is in K. So, that means L is in K prime, K prime is of course in L. So, that means L equals K prime and sigma is an isomorphism, so that completes the solution. So, this is the proof that any two algebraically algebraic closures are F isomorphic. So, the proof is not that important. We have done it so that you understand how to go about using extension theorem and the statements will be used later. So, typically we often talk about these splitting fields of an polynomial or the algebraic closure of a field just to when there is no danger of confusing the two fields. As far as f extensions are concerned they are isomorphic.

(Refer Slide Time: 14:50)



So, now let me do a third exercise, third exercise on splitting fields. So, I am going to just give you a few examples of how to compute splitting fields. Again these are things that you may have studied in you in your algebra field theory course but I want to do, just do and hands on examples so that you are comfortable with the kind of calculations that we will do later. So, let me start with some simple example, so let p be a prime number, then find the splitting field of X power p minus 2 over Q and its degree. So, find the splitting field and its degree over Q. So, this is the problem.

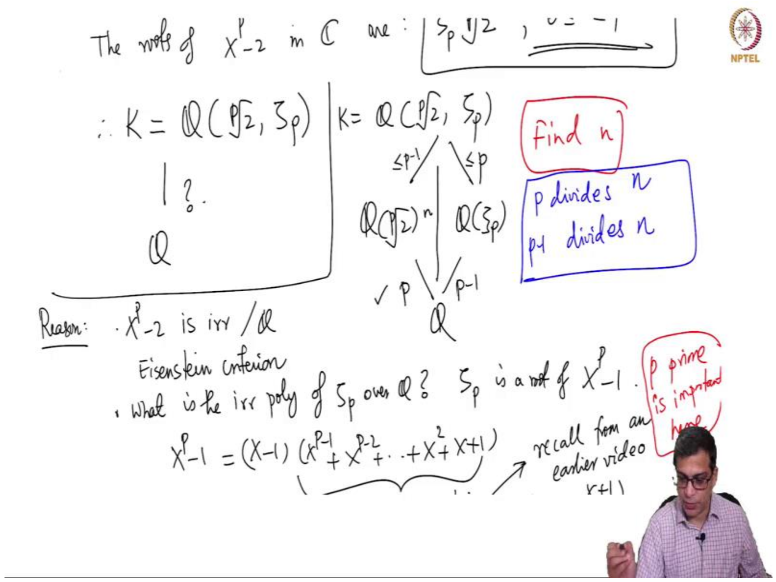
(Refer Slide Time: 15:53)



The first point I want to emphasize is what is a splitting field? So, let, we will denote the K by K, denote the splitting field by K. So, I am going to shorten it like this. So, think about this for a minute. What are the roots of this polynomial? Roots if you think about it, first of all you can take the pth root of 2, take the real pth root of 2. P is a positive numbers so there is a real pth root of 2 in R, so real number. And let zeta P be a primitive, pth root of unity. So, this is of course in complex numbers, it is typically not. In fact P is a prime numbers so it, unless it is 2 it will not be in real numbers. So, let it be the a primitive. There could be several primitive pth roots.

So, let it be a primitive pth root of unity. So, then the roots of X power p minus 2 in C are. So, remember there is a God given algebraically closed field that contains Q. So, we can always take root there and then generate the splitting field by taking the roots, the field generated by those. So, the roots of X power p minus 2 you will see R. You can easily prove this. There you have, so these are the p roots which has p roots it is a degree p polynomial. So, it will have p roots there given by zeta power pi times p root 2 pth root of 2. So, you get pth root of 2 for I equal to 0, then zeta p pth root of 2, zeta p square pth root of 2 and so on. So, the splitting field is Q adjoined, clearly if you think about this, I can just take this.

(Refer Slide Time: 18:02)



Because once I have these 2, I have all the other roots because I can take powers of this and remember these two must be included if either you remove any of them, it will not be a splitting field because if you only put pth root of 2 you cannot get other roots. If you only put the pth root of unity, you would not get pth root of 2. So, now what is the degree of this? So, now in order to find this, I am going to use the multiplicative property of the field ex degree of the field extensions and carefully break up this extension like this.

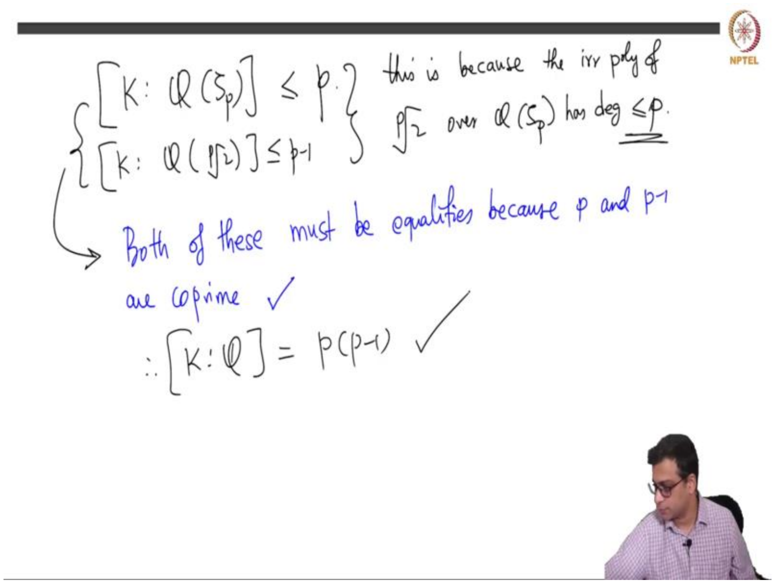
So, now the first point I want to emphasize is there are 2 subfields here, so these are both subfields and we do know what are the extension degrees here. I claim that this is p and this is p minus 1. Why is this? The reason for this and this is first point is x power p minus 2 is irreducible, is over Q, irreducible over Q. This is simply by Eisenstein criteria. Remember x power p minus 2 is a polynomial that pth root of 2 satisfies and x power p minus 2 is irreducible, so this degree must be p. So, that is ok.

On the other hand what is the irreducible polynomial of this? This is the primitive extension as it is called that means it is generated by a single element. We will talk about primitive extensions in detail later. So, the degree of this extension will be simply the degree of the irreducible polynomial of zeta p. But what is that? So, zeta p certainly satisfies, this polynomial. So, zeta p is a root. Let me write it more precisely. It is a root of this, but of course that is not irreducible right because x power p minus 1 does factor like this.

But this is irreducible right so recall from the recall from an earlier video. It does not look like you can apply Eisenstein here, directly certainly you cannot apply, but do the change of variable x to x plus 1 then you can apply. And then here is where the fact that p is prime is important. It is not going to be true if p is not prime. So, p is prime is important here. That is the only place where we use p prime. So, that means this is p minus 1 because irreducible polynomial is zeta p over Q has degree p minus 1. So, this is p minus 1 that means whatever this number is. So, we are interested in finding this number n. So, the question is find n.

So, what we know is that p divides n and also p minus 1 divides n. P divides n and p minus 1 divides n because whatever I mean, n is equal to p times this number, n is also equal to p minus 1 times this number. But of course there are lots of numbers that p and p minus 1 divide. But I claim that it must be p times p minus 1 because now let us look at what can be the degree of, let us say this.

(Refer Slide Time: 22:05)

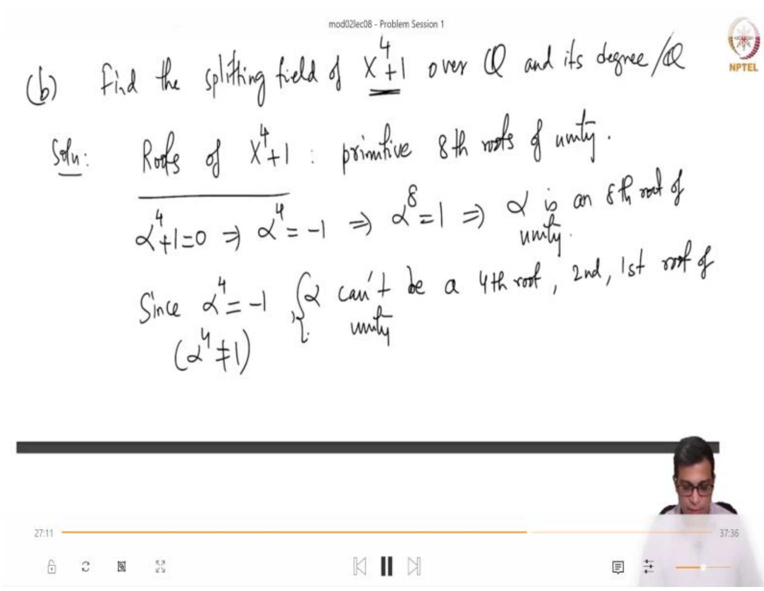


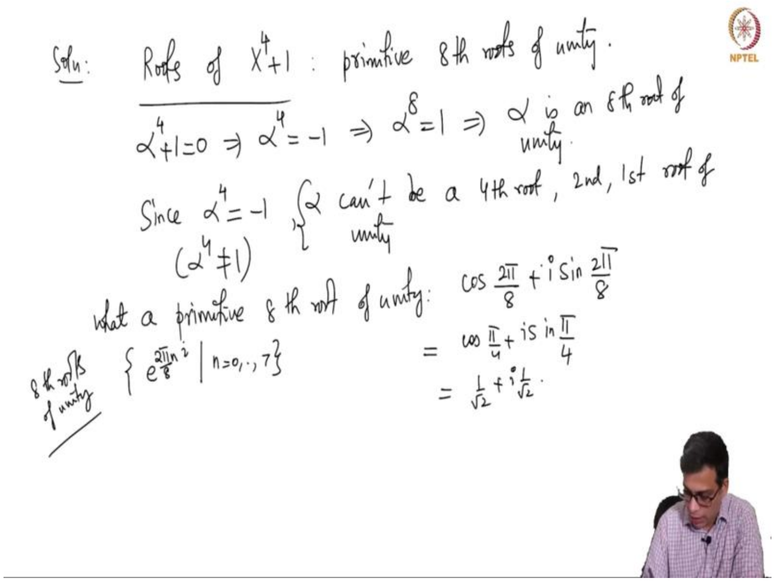
I claim that that is at most p. So, this degree is less than or equal to p. And similarly this degree is less than equal to p minus 1. So, let me show it. I cannot show it here but, so this degree is less than equal to p minus 1, this degree is less than equal to p this is because these are both primitive extensions, the A is the primitive extension of this because it is generated over this field by just zeta p. This is also a primitive extension because this K or Q zeta p is generated by pth root of 2.

The irreducible polynomial let us say of pth root of 2 over Q zeta p has degree less than p. This is because irreducible polynomial of x power p pth root of 2 over Q itself is degree p. So, the irreducible polynomial over a bigger field it can possibly split so it cannot be higher degree. So, it is at most p. So, similarly this is at most p minus 1, this is at most p but now you have a this. So, let us focus on this direction. This number is at most p, the product is divisible by p so that number in both cases, both of these must be equalities because p and p minus 1 are co-prime.

You cannot have a smaller number than p here and still have the product with p minus 1 to be divisible by p. So, they are both co-prime. So, that is not possible. That means, so this solves the problem. So, the splitting field is degree p times p minus 1. So, now let us do why p, I mean the proof does not work with p not prime but in fact the statement is also wrong with p not prime.

(Refer Slide Time: 24:38)





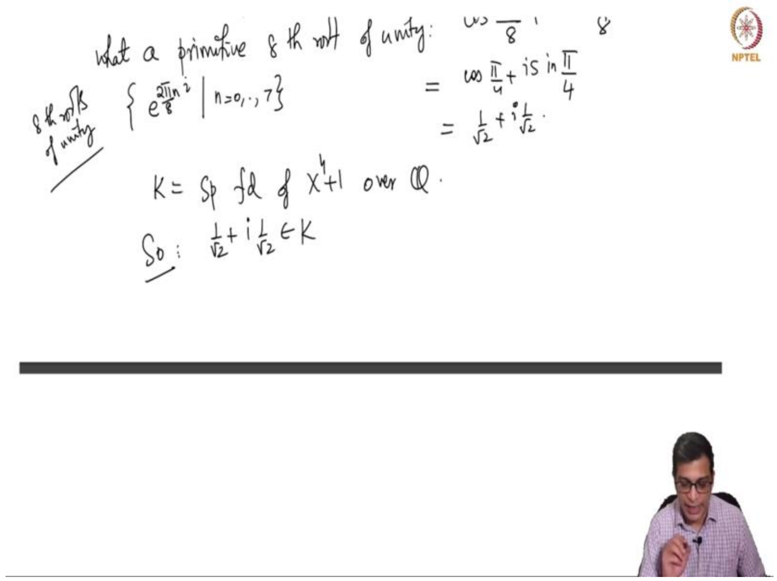
So, the second example is find, so I will come to the second example but maybe first do some other things which come up in 4. So, for example find the splitting field of x power 4 minus 4 minus, so I think this I mentioned in the video where I recalled spitting fields but let me I am going to use this. So, let me just recall the splitting fields. So, x power 4 minus 1, so this actually let me do x power 4 plus 1. So, because that is going to be the polynomial that I will need it for later. So, this if you take what are the roots of.

So, I claim that roots of x power 4 plus 1 are precisely primitive 8th roots of unity. So, these are primitive 8th roots of unity. This is because if alpha power 4 plus 1 equals 0, then alpha power 4 equals minus 1 that means alpha power 8 is 1. So, that means alpha is in eighth root of unity. But if it is not a primitive 8th root of unity, for example i is an ith root of eighth root of unity but i power 4 is 1, so i power 4 plus 1 is not 0. So since, so alpha power 4 is equal to minus 1, alpha 4 is not equal to 1. So, alpha cannot be a root of unity, cannot be a fourth root.

So, any root eighth root of unity is either a fourth root of unity or a second root of unity or first root of unity. It cannot be a fourth root, second root or first root of unity. So, if alpha, alpha power 8 is 1, then either alpha is 1 or alpha square is 1 or alpha 4 is 1 or alpha power 8 is 1. So, it cannot be any of those.

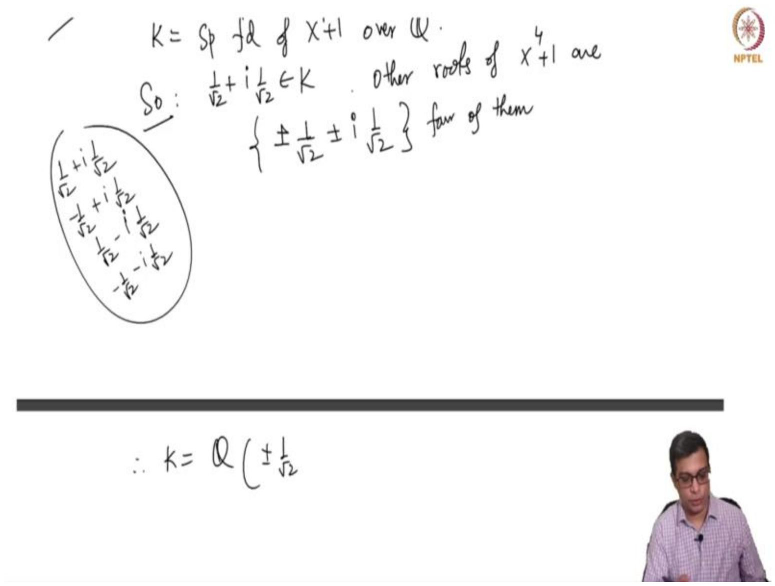
So, alpha is a primitive eighth root of unity. What are primitive eighth roots of unity? What is a eighth primitive root of unity? So, let me write, this is precisely cosine 2 pi by 8, plus i sine 2 pi by 8. So, in general all the root eighth roots of unity are given by, these are the eighth roots of unity. You can take i equal to 1 that will give you a n equal to 1 that will give you a primitive eighth root of unity but this is cosine pi by 4 plus I sine pi by 4. This is 1 by root 2 plus I times 1 by root 2. Now if you think about this. So, this is what I want to say for now. So, the prim x by 4 plus 1 has this.

(Refer Slide Time: 28:45)



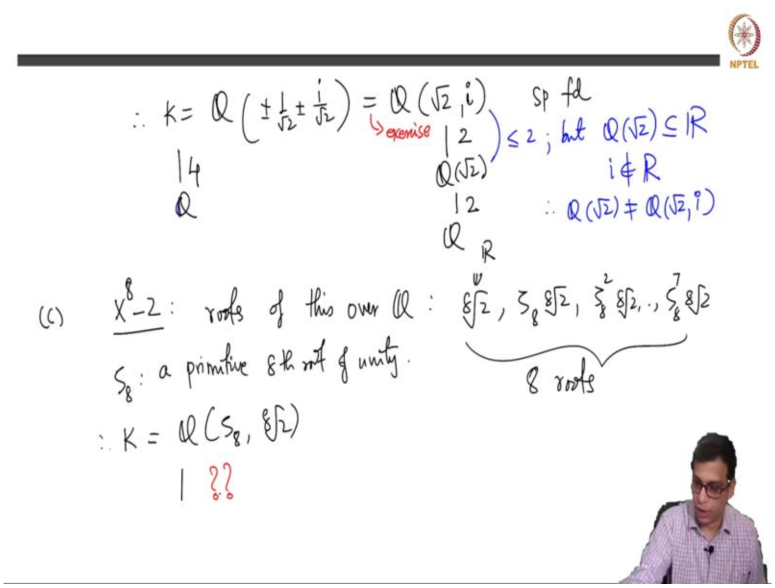
So, I have to add, so if let K be the splitting field of x power 4 plus 1 or 2 over Q. So, what we have now shown is that. It becomes what we have shown is that 1 by root 2 plus i times 1 by root 2 is in K. So, 1 by root 2 plus i sine, 1 by root 2 plus i times 1 by root 2 is in K.

(Refer Slide Time: 29:12)



So, I claim that other roots, other roots of x power 4 plus 1 are. So, one can check easily, these are going to be you can put so I should have really written it like this. So, these are the 4 roots. So, you can take 1 by root 2 with plus sign or minus sign, i times 1 by 2 with plus sign or minus sign. So, there are 4 of them. So, you can immediately conclude that K is equal to Q joined, plus minus 1 by root 2. So, I mean, you understand what I mean here. So, 1 is, the other is this so, these are the roots. If you, clearly you can check that their 4th power will be minus 1.

(Refer Slide Time: 30:18)



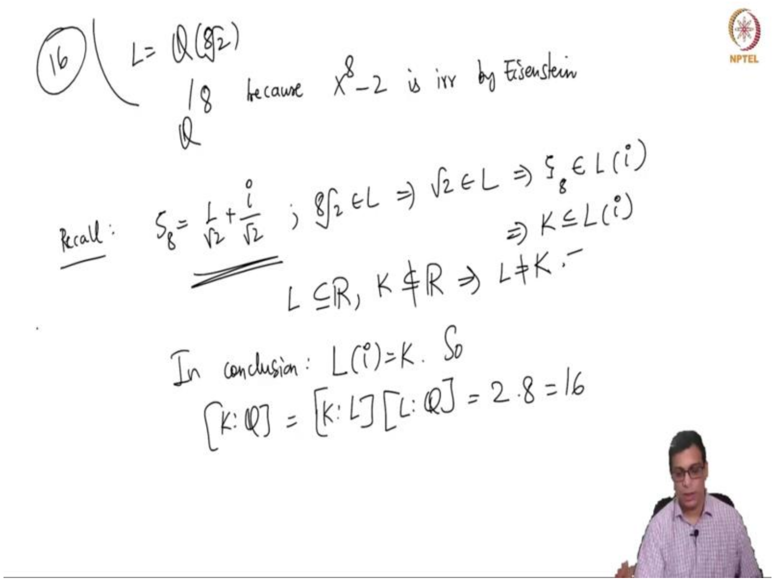
So, these are the roots. But then if you think about this, both root 2 and root i must root 2 and i must be there because you can, for example add the first 2 here that gives you i 2 times i times root 2, so root 2 i. So, you can play with these things and conclude that both root 2 and i are there. Once root 2 and i are there all of them are there. So, this is a little exercise for you which you can easily do by manipulating these elements. So, that means what is the degree now? This is the splitting field and what is the degree of Q?

Of course, this will you can compute this by doing first Q to Q. So, this is 2 because x square minus 2 is the irreducible polynomial. This is also true because i satisfies a degree 2 polynomial of Q. So, it can be at most 2. So, you first note that this is at most 2 but then Q root 2 is in R, i is not in R. So, this cannot be equal. So, Q root 2 cannot be equal to Q root 2 comma i. So, this is at least 2 but at the same time it is at most 2. So, it cannot be, it has to be 2.

So, that means K over Q is 4. So, that is the solution to this and the final thing that I want to do just very quickly C is x power 8 minus 2, just to compare this with x power p minus 2, which we discussed earlier. The degrees is p times p minus 1 so if the same result is true here it will be 8 times 7, 56. But it is not so as we will see. What are the roots of this? Roots of this over Q are just going by the same argument as earlier. So, there are 8 roots. This much is true. I mean, you have eighth root of 2, this is a real number and then you take zeta 8 times eighth root of 2 that square is also that eighth power is also 2. So, this is clear? So, my notation is always this is a primitive eighth root of unity.

So, again as before, K must be equal to Q, zeta 8 eighth root of 2. Now the question is, what is this degree? I claim that this degree is 16. That is because we are going to break this up into a tower like this. This is 2, this is 8 because what is irreducible pol sorry this sign take eighth root of 2. What is irreducible polynomial of eighth root 2 over Q? That is just x power 8 minus 2 and this is irreducible by Eisenstein’s style. So, the question now boils down to what is this? What is this degree? Now zeta 8 over Q has degree 4 as we saw earlier. So, K is of course zeta 8. So, this is at most 4. So, you already see that this cannot be 56. So, this is at least at most 32.

(Refer Slide Time: 34:29)



But in fact I claim that this is 2. Why is that? So, now this is I am going to quickly wrap this up because I have already spent too much time on this video. So, let me wrap this up by saying that Q. So, if you call K, so let us say I call this L. So, I call this L. So, basically, I claim that Li is K, so Li is K. So, what is the proof of this claim here? So, Li is K. Why is that? Zeta 8 as we agreed is 1 by root 2. 1 choice of, 1 choice for primitive eighth root is this. So, zeta 8 is this but so recall this. But we already know that eighth root of 2 is in L that means square root of 2 is in L because eighth root of 2 power 4 is square root of L.

That means zeta 8 is in L adjoined I right because if you adjoin I, root 2 is already in L. So, then zeta 8 can be you can describe zeta 8 as a polynomial in i with coefficients in L, exactly this way. So, zeta 8 is in L that means K is contained in Li but note that as before L is contained in R, K is not contained in R, this means L is not equal to K. So, together this imply that. So, in conclusion Li is K.

So, K colon Q is K colon L times L colon Q. K colon L is 2 because K is Li and L colon Q is 8 so that is 16. So, all I am saying is this is 8, this is 2. So, this is 16. So, I am sorry that I went very fast over the last part of this problem but I hope this gave you an idea of how to use various results that we have recalled and compute the degrees of splitting field extensions. In the theory field in the Galva theory course, we are going to further analyze this splitting fields. We know

now how to compute the degrees but we are going to talk about automorphisms of K which fix Q. So, that is the goal for us in the rest of the course. Thank you.