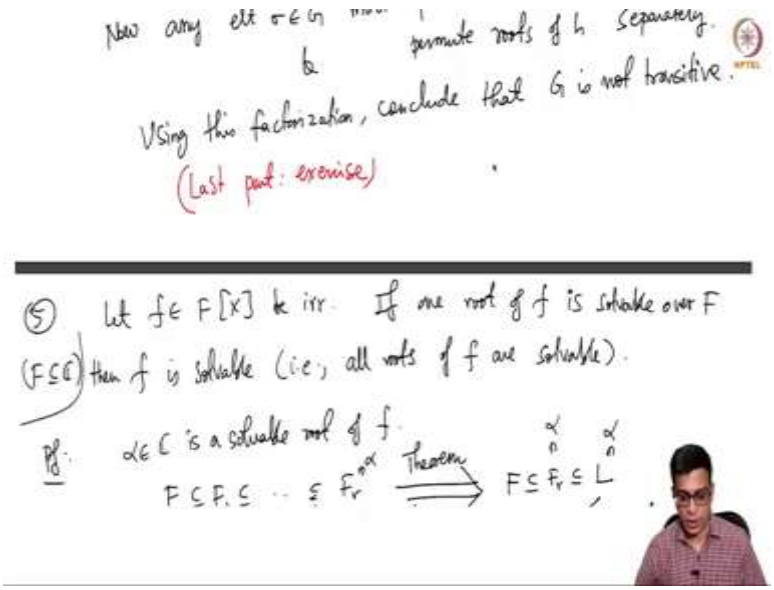
Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Problem Session - Part 12

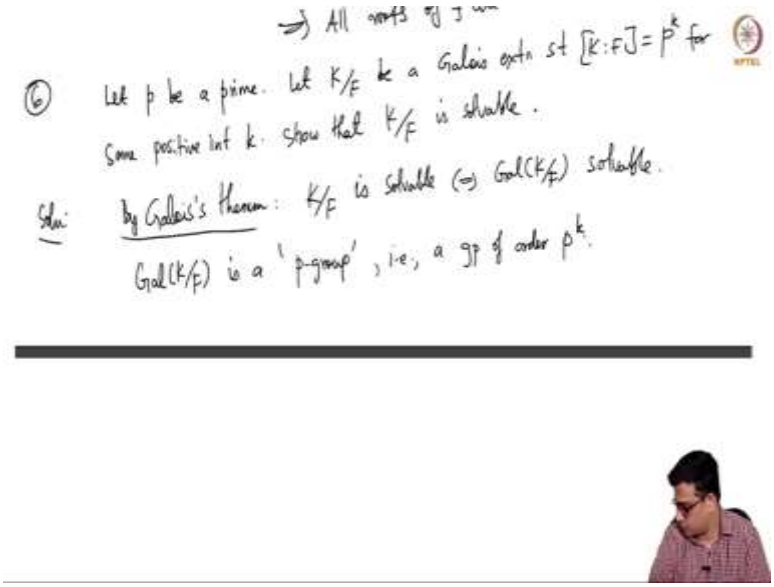
(Refer Slide Time: 0:19)



Welcome back we are in a problem session now. And as I told you, we have completed the content of the course, we have developed Galois theory, defined Galois theory, proved main theorem and talked about Kummer extensions, cyclotomic extensions and so on, and then proved the main result of that Galois theory achieves and which was a long standing problem that is solved, which is that there are quintic polynomials that cannot be solved by radicals.

So, we did all that, we gave examples and now, we are in the middle of doing several exercises to make sure that we understand the concepts better. So, I will do one or two more videos to do more problems.

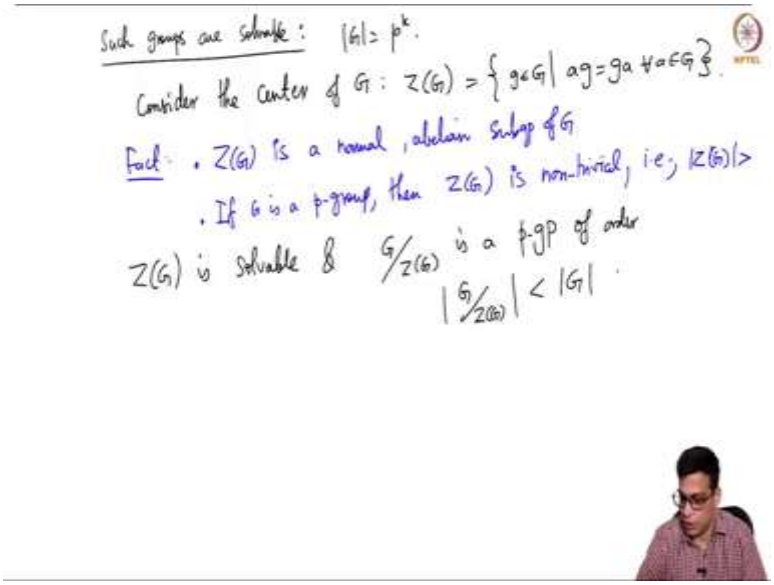
(Refer Slide Time: 0:54)



So, let me just start with this following problem. Let p be a prime and let K over F be a Galois extension such that the degree of the extension is a power of p. So, p power k for some positive integer k. So, the Galois group is in other words a p group in the language of group theory, so show that K over F is solvable. That means, every element of K is soluble over F that is what it means.

So, by our main theorem, our theorem by Galois theorem let me call it, that says that an extension is Galois is solvable if and only if its Galois group is solvable. So, this is a purely group theoretic phenomenon. But Galois K over F is a 'p group' that is a group of order p power k.

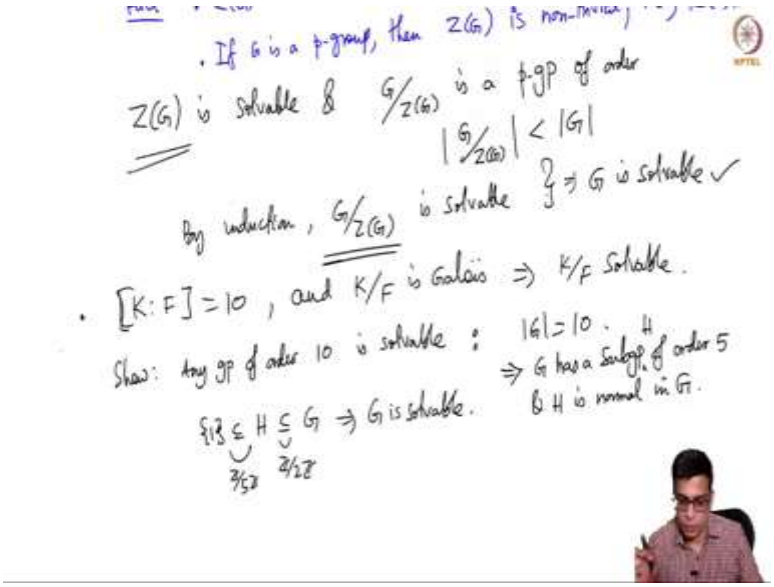
(Refer Slide Time: 2:30)



So, now, this such groups are solvable. So, that I will let you I mean, this is a simple statement, but I will give you a hint on how to proceed with this. So, of course, we know that let us say G is power k by Sylow's theorems for example, or Cauchy's theorem in fact, by Cauchy's theorem G has an element of order p. So, actually, let me be careful here, what I want to do is consider the center of G which is all elements which commutes with everything, so, g and G such that ag equals ga for all a in G.

So, now a group theory fact is a normal subgroup, this is always true and for p-groups then Z G is non-trivial. So, that is, its order is at least 1, at least 2. So, now using these facts, because it is abelian Z G is solvable and G mod Z G is a p-group, because order of Z G will also be a power of p. So, this will be p power k divided by some smaller power of p which is also p power. So, this is a p-group of order strictly less than order of G, because Z G is non-trivial. So, this is a strictly smaller subgroup, a proper subgroup.

(Refer Slide Time: 4:41)

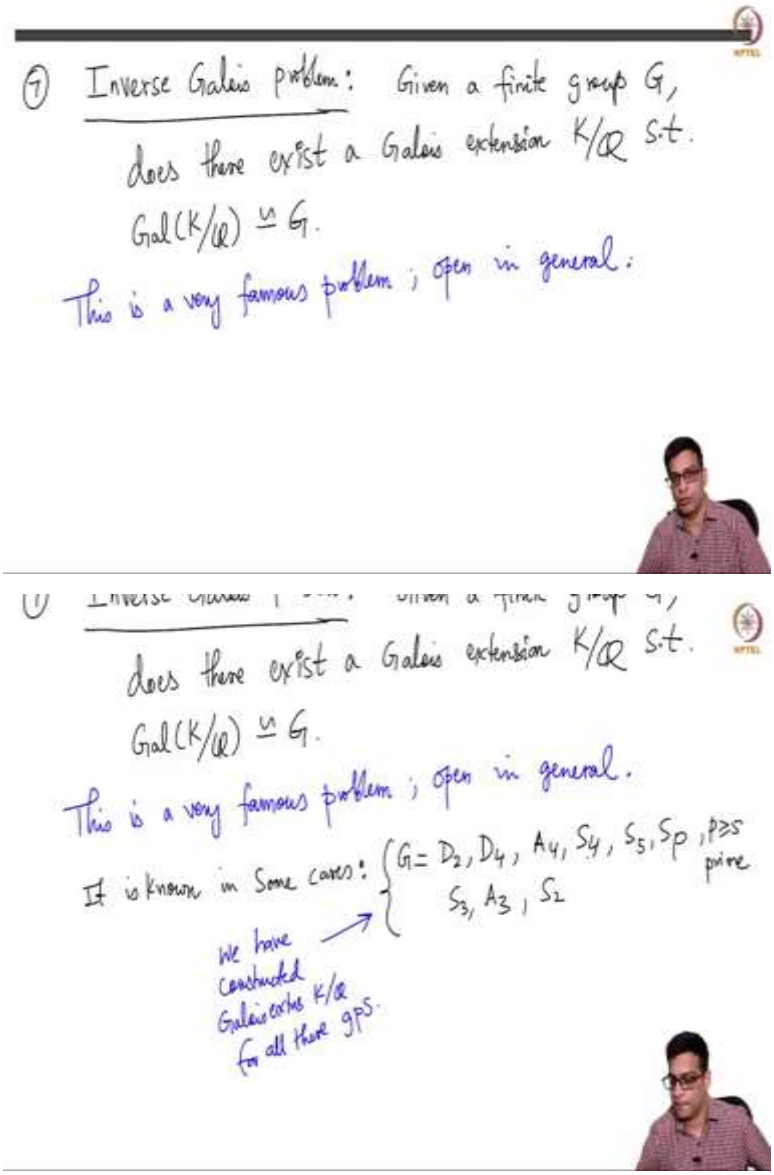


So, by induction hypothesis, I mean I have not set it up properly, but by induction, you first show that for any p group of order p is solvable, that is clear, because it is abelian. So, this will be solvable. So, it is a p group of smaller order, so, Z G is solvable, this is solvable and hence G is solvable, so that solves this.

A similar problem I want to give. I do not want to call it a new thing, new numbering, but let us say K colon Q is 10 and K over Q is Galois. In fact, you can replace Q by F, implies K colon F is solvable. So, all you need to do is that show any group of order 10 is solvable and this is clear because, if G has ordered 10 it could be non abelian, it could be D5.

But, we do know that G has a subgroup of order 5, subgroup H of order 5 and H has to be normal because it is index 2. So, you can consider the series one containing, contained in H contained in G. So, this is quotient Z mod 5 Z, this is normal and quotient is Z mod, and this is Z mod 2 Z. So, this is a series that will give you the solvability of G and hence solvability of the extension K over F. So, the next problem I want to talk about is a famous problem. So, this is not so much as a problem, but in introduction I will cover some exercises as part of this.

(Refer Slide Time: 6:44)

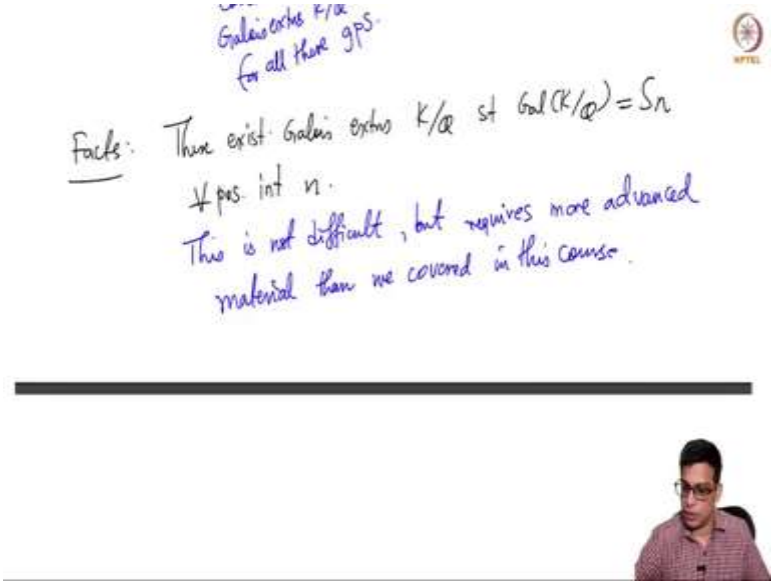


So, there is a famous open problem in Galois theory, it is in fact, a very famous problem. And solving this will make you instantly famous. So, inverse Galois conjecture or problem, it is not a theorem of course. So, given a finite group G does there exist a Galois extension of Q. So, it is important that the bass field is Q, such that its Galois group is G. So, this is a very famous open problem, it is open in general, this is a famous problem, open in general. Meaning there is no general, there is no proof that for every group, there is such a Galois extension of Q, so that is it is open.

And it is a very important problem in mathematics, it led to, working on this led to a lot of deep and beautiful mathematics. However, it is known in some cases, just to give you a flavor of what we can do. For example, if G is D2, D4, A4, S4, S5, S p, p prime. So, we have done all this, S3, A3, we have constructed and S2 Z mod two Z. So, all these cases Galois extensions for all this, for all these groups, we have done good that is not difficult. D2, D4, A4, S4 were covered in the case of quartic irreducible polynomials.

And of course, we also need to put C4 here. That is also in quartic, S5 we have constructed to shows that there are quintics that are not solvable. More generally, we do an Sp for primes and S3, A3 for cubics and S2 for quadratics.

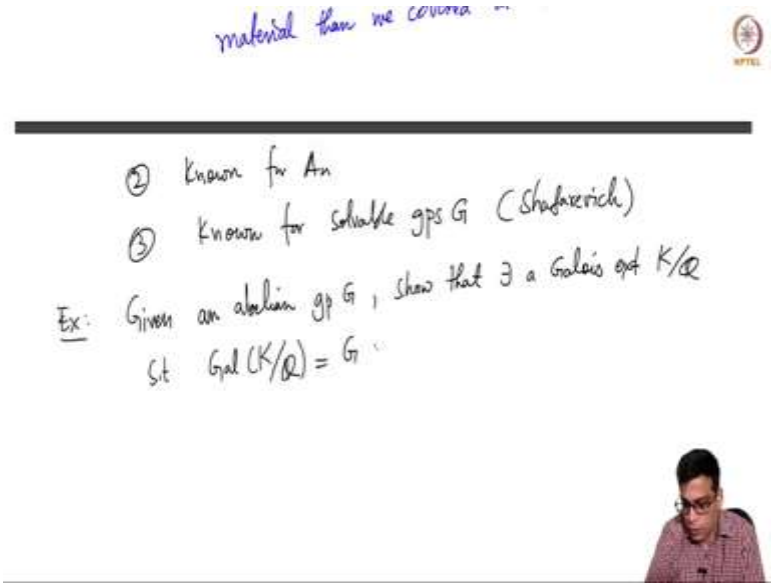
(Refer Slide Time: 9:48)



So, these are some general theorems that are known or facts, let me simply call them as facts, there exist Galois extensions, K over Q such that Galois. So, what we have done for Sp can be done more generally for Sn, for all integers, positive integers n. So, we have done here for 1, 2, 3, 4, 5. And every prime after that 7, 11 and so on. But this is significantly more difficult, so this requires, so this is not difficult, it is not difficult in the sense that it is not a theorem, it is not a research paper, this is not difficult but requires more advanced material.

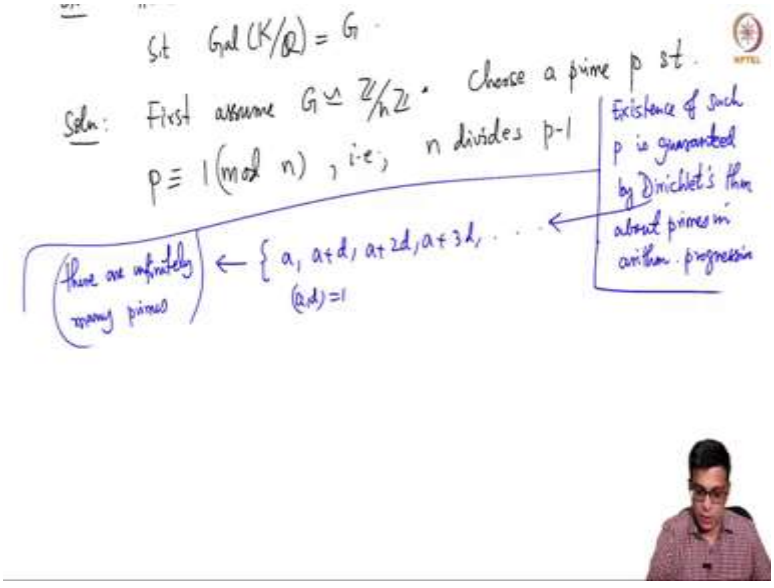
So, it requires either some algebraic number theory or committed to algebra. Then we are, then what we did in this course? But it is good to keep this in mind. So, there is a Galois extension of rational numbers with Galois group Sn and also for San, so that it is also known.

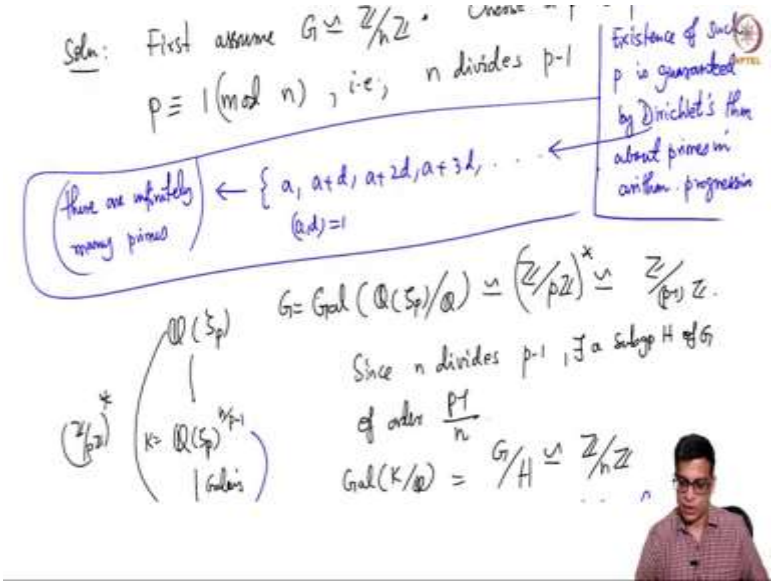
(Refer Slide Time: 11:17)



So, I will simply write like this known for An also. And it is also known for solvable groups. This is a theorem of famous mathematician called Shafarevich. What I want to do now is exercise given an abelian group. This we can do now, modulo some general group theory, show that there exists a Galois extension K over Q such that Galois K over Q. So, after we do this exercise, if you take stock of the inverse Galois problem, you can do for symmetric groups, you can do for alternating groups, you can do for solvable groups, and you can do for abelian groups, the abelian groups is the, is something we can do.

(Refer Slide Time: 12:19)





But in general there is no construction for arbitrary groups. So, this is something that I will do now, which is not, so I will actually do the cyclic case first, because general case is essentially follows from the cyclic case. So, assume that G is a cyclic group, choose a prime p, such that P is 1 modulo n, that is n divides p minus 1. So, n divides p minus 1, so, I want this.

So, now, the existence of such P is a theorem if such P is guaranteed by Dirichlet's theorem about primes in arithmetic progression. Dirichlet proved that if you give, if you start with any arithmetic progression, something like a, a plus d, a plus 2d, a plus 3d and so on, this, there are infinitely many primes in this. So, you have to assume a and d are co prime, there are infinitely many primes. So, you can prove this, this is Dirichlet's theorem, not prove this, but this is a fact and it is a famous theorem. It is not easy to prove this. So, now, let us choose that P, I am not going to discuss this for now.

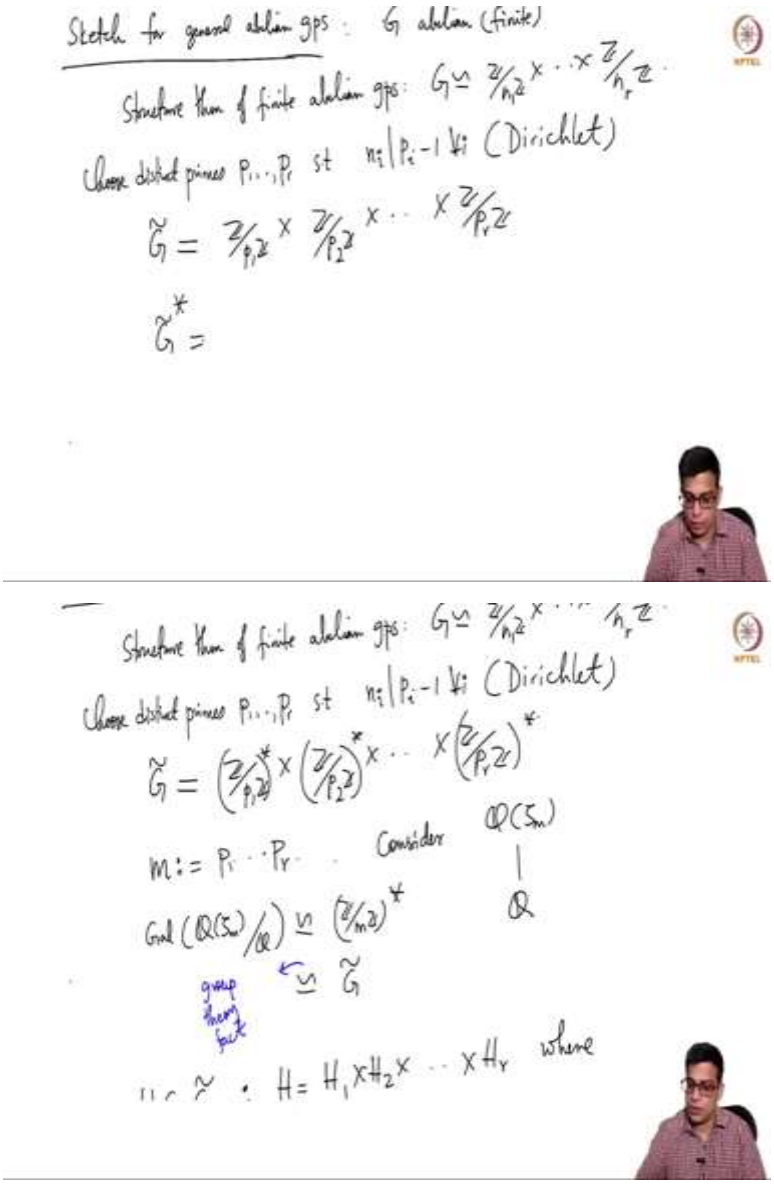
So, choose such P and Q zeta P over Q. So, by what we know already from cyclotomic extensions, Q zeta P over Q is isomorphic to Z mod p Z star, which is of course isomorphic to Z mod p minus 1 Z. So, because P is prime the group of units in Z mod p Z is all nonzero elements so, that is Z mod p Z. So, since n divides p minus 1 there exists a subgroup. So, let us call this G, there exists a subgroup H G of order n by p minus 1.

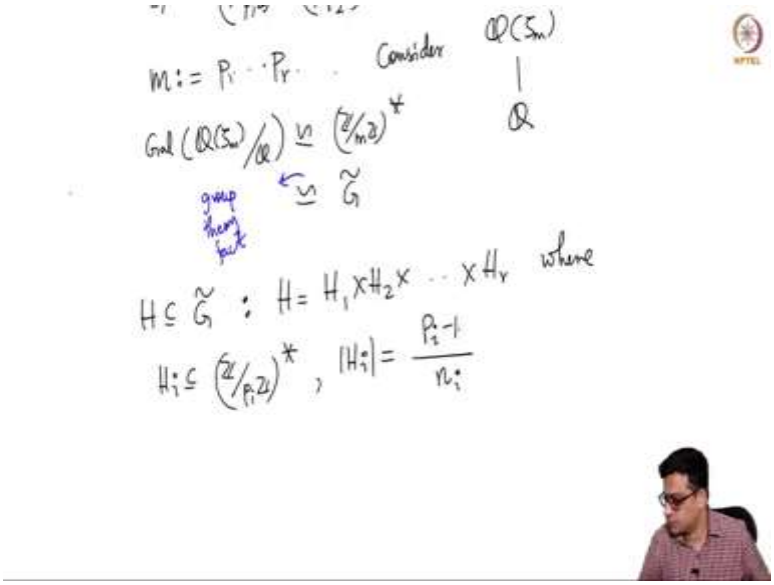
So, now let us take the fixed field of that. So now, this, because this is an abelian extension every subgroup is Galois. So, this is every intermediate field is Galois over Q. This is Galois with what is the Galois group of let us call this K. What is Galois group of K over Q? This is Z mod p

minus 1 Z modulo Z mod. Basically G mod H, which is a cyclic group, because quotient of a cyclic group is cyclic, it is order n rather I should write p minus 1 by n here, it is p minus 1 divided by p minus 1 by n. So, it is Z mod n Z.

So, this is the desired, this is the Galois extension we are looking for. So, this is the Galois extension we are looking for, we are looking for a Galois extension of Q with Galois group being this cyclic group of order n. So, this is done.

(Refer Slide Time: 16:41)





Now, quickly sketch for general abelian groups. I am not giving you the details, but this is more or less self-contained modulo these details. So, structure theorem for abelian groups of course, all our groups are finite here shows that. So, let us say G is abelian and finite always G can be factored as Z mod n 1 Z cross Z mod n RZ, any abelian group is a product of cyclic groups.

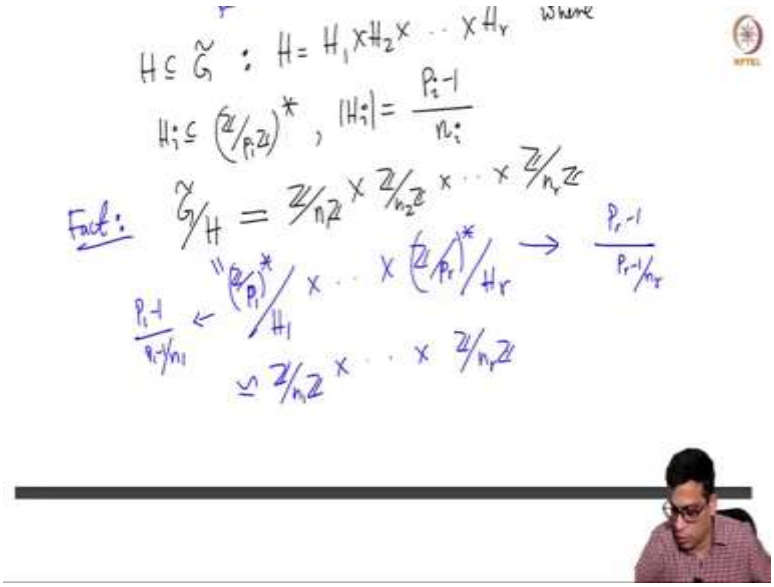
Now, choose primes p1 through pr, such that ni divides pi minus 1. So, again this is possible. So, choose distinct primes. So, pi is not equal to p for i different from j, so we can choose distinct primes like this and this is a consequence of Dirichlet's theorem. Now, consider G tilde to be Z mod p1 Z cross Z mod p2 Z cross Z mod pr Z. Now, G tilde star is, so, let me for now say the following.

So, let us say m is equal to, let us take m to be product of these primes. So, then consider the Galois group, I mean the Galois extension Q Z time over Q, Z time is of course, a primitive nth root of unity. Then, Galois group of this is isomorphic to Z mod m Z star which happens to be G tilde. So, this is a fact because m has this decomposition and this is a group theory fact. So, I will proceed after, without saying anything further about this.

So, now construct H a subgroup of g G are as follows. H is H1 cross H2 cross Hr, where Hi is inside Z mod p1 Z star. So, by the way, I think I made a mistake here. So, what I mean here is star. So, I do not want to take Z mod p1 Z, but Z mod p1 Z star, so I want to take starts here. So, Hi is a subgroup of this. And the cardinality of Hi is pi minus 1, which is the cardinality of this

divided by ni, just like we did in the cyclic case. So, I am sorry, I am going over this fast, I hope you understood the cyclic case, and then this is just putting all of them together.

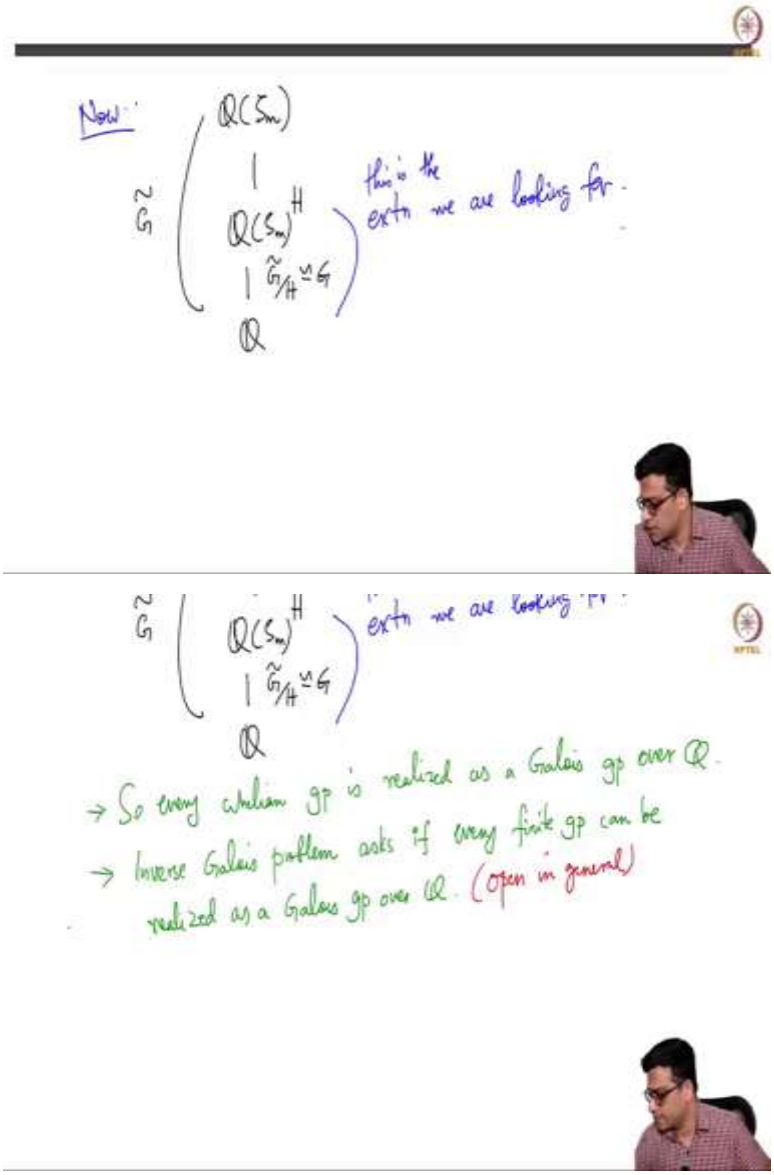
(Refer Slide Time: 20:25)



So, now, H is a subgroup of G tilde of index, index is a cyclic subgroup H is actually what I want to now say is that this I will let you verify is Z mod n1 Z cross Z mod n2 Z, so this is a fact. Again, standard group theory facts. By the way, we constructed this, this is actually nothing but, this is nothing but Z mod p1 star modulo H1 which will have this is Z mod pr star modulo Hr, but because this is order p1 minus 1 divided by p1 minus 1 divided by n1.

So, this will be a cyclic group of order n1. So, and this will be order pr minus 1 divided by pr minus 1 by nr. So, this will be a cyclic group of order Z mod nr. But this of course, is by construction G. So, this is fairly easy. So, now, we are done. So, now, all we need to take, maybe I will write here.

(Refer Slide Time: 22:03)

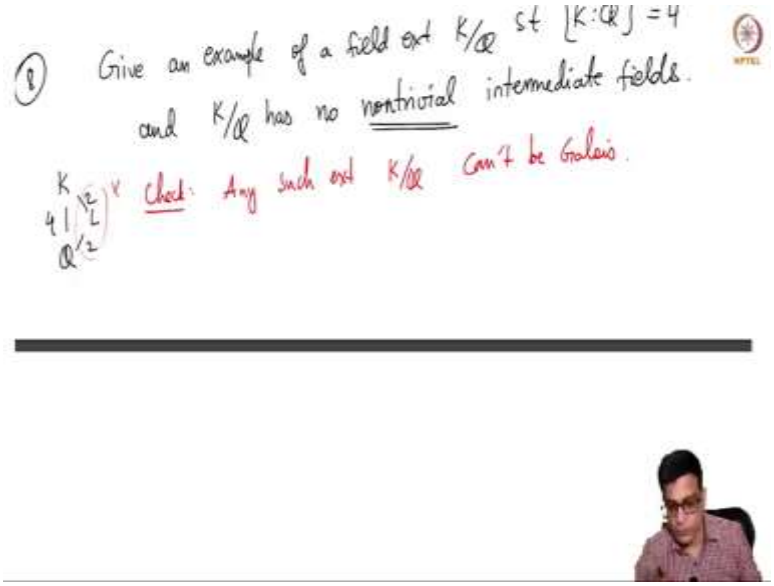


Now, what we do? We have the field Q zeta m and we take the fixed field of H, over, this is G tilde, so, this is G tilde mod H which is G. So, this is the extension we are looking for. So, this completes the statement that every abelian group is realized as a Galois group our Q. So, every abelian group is realized as a Galois group over Q. So, this is a short way of saying that there is a Galois extension of Q whose Galois group is that abelian group.

So, now, inverse Galois problem asks, if every finite group can be realized as a Galois group over Q. So, this is open in general and as I remarked earlier, it is true for abelian groups, it is true for symmetry groups, it is true for solvable groups, it is true for alternating groups and so on. So,

still it remains an open question for other kinds of groups. So, arbitrary non abelian groups. So, now, let us continue. So, let me do 1 or 2 more problems in this class, then I have one more video where I can finally wrap up the course.

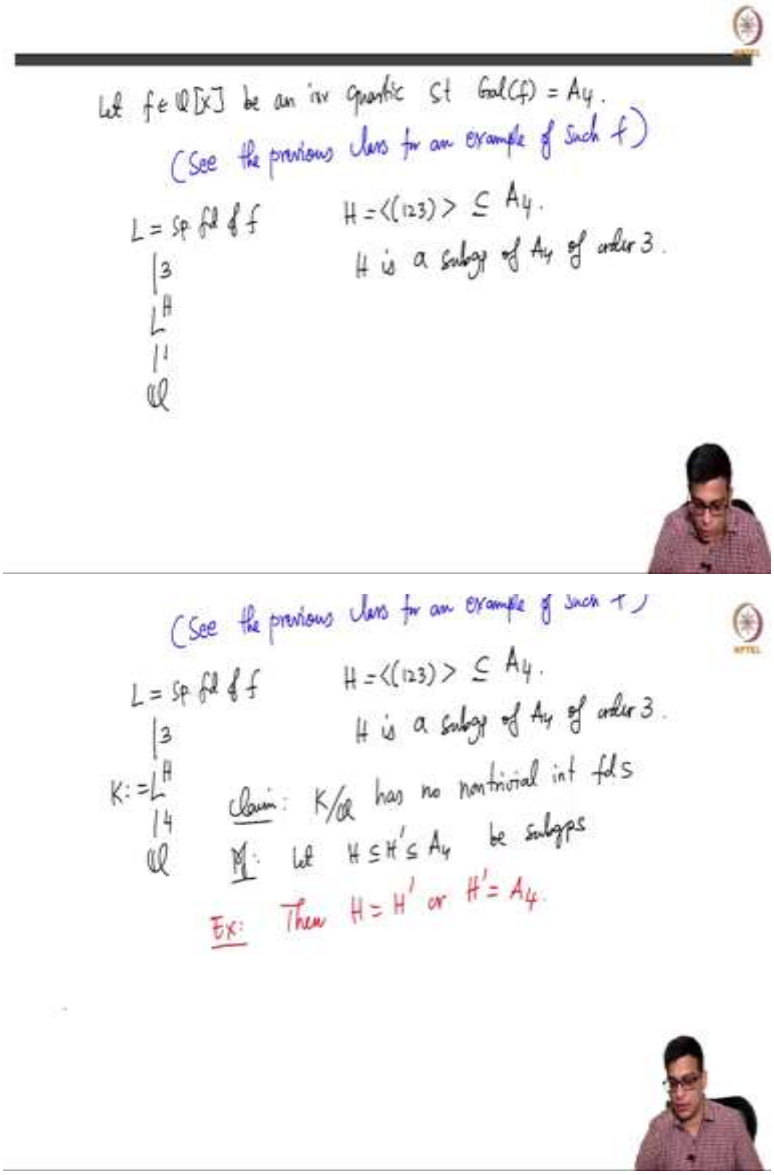
(Refer Slide Time: 24:04)



So, eighth problem, give an example of a field extension of a Galois extension, of a field extension K over Q such that the degree is 4 and K over Q has no non trivial intermediate fields. So, what I want is an extension of degree 4 of Q such that there is nothing in between other than K and Q of course, non trivial means a degree 2 extension here, that cannot happen, so that does not take. So, that is what I want to do.

So, as an simple sanity check, you can check that any such extension has to be, or cannot be Galois let us say, because if it is Galois, the Galois group is either cyclic of order 4 or a client 4 group both of which are a subgroup of order 2, normal subgroup. So, you can take the fixed field and that will give you an intermediate field. So, you cannot take a Galois extension.

(Refer Slide Time: 25:40)

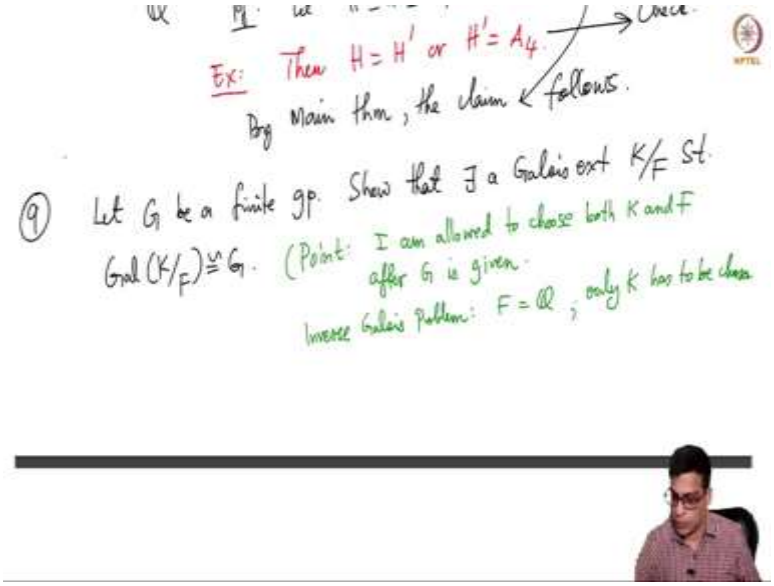


So, the example I will give you now is let f be an irreducible quartic degree 4 irreducible polynomial such that Galois group is a4, we in the previous class, we did see such examples. So, previous class for an example of such f, so, we did construct a quartic irreducible polynomial whose Galois group is A4. So, let us take K, or I just want to call L, the splitting field of l, and we have Q. Now, let us consider H to be the subgroup generated by these three cycles of A4, this is a cyclic subgroup. And H is in fact, a normal sub, H is a subgroup of A4 of order 3 of course. So, I am going to take its fixed field.

Now, I am going to claim that it cannot have any intermediate fields. So, let me just, I want to just take a look because I do not want to mess up anything. So, here what is the degrees here? Because H is order 3, this is order 3, and because H is index 4, this is degree 4. So, this is going to be my claim. So, claim K over Q has no non trivial intermediate fields. Proof is because L over Q is Galois, we can apply main theorem. So, what we will show is let H be a subgroup, I mean H is given, but let H prime be a subgroup of A4 contained in a4 but containing H. So then, this is an exercise, group theory exercise show that H is H prime or H prime is A4.

So, there are no proper subgroups of A4 that properly contain H. So, this is a maximal proper subgroup in some sense. So, by main theorem, the claim follows, this claim follows because if there is any intermediate field that must correspond to a subgroup H prime of A4 which contains H, but such a thing cannot happen. So basically, the whole problem is to check this exercise which I will let you do. So, now, let me give you an idea of how to do this for arbitrary field extensions.

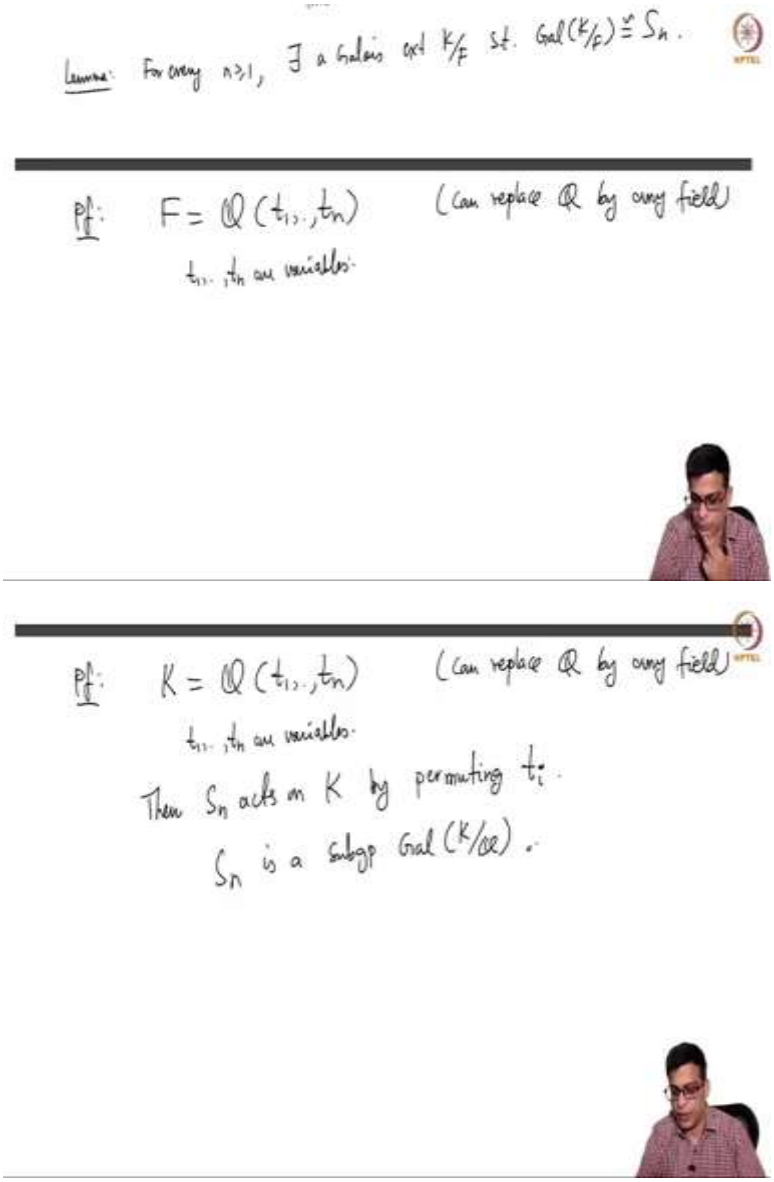
(Refer Slide Time: 28:46)

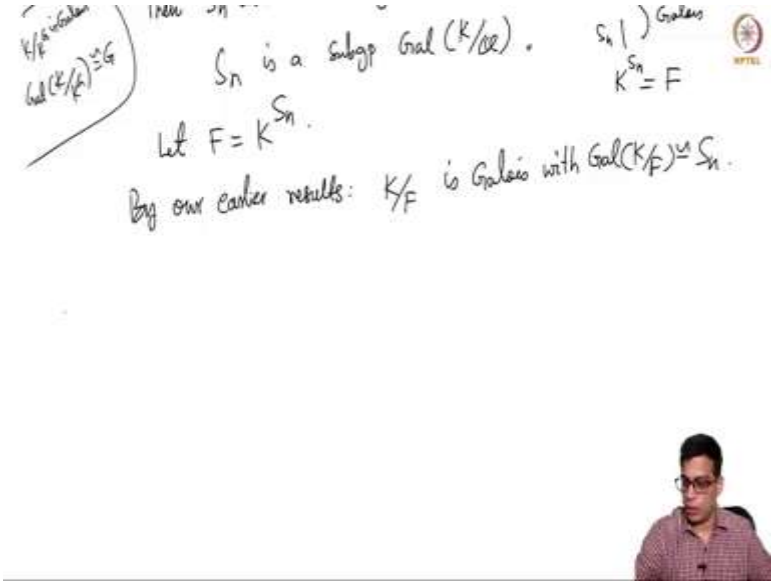


So now, 9 problem. So, this is in context of Galois, inverse Galois problem. Remember inverse gamma problem asks, If any finite group can be realized as a Galois group over Q. If you do not insist on the base field Q, we can always do this. So, let G be a finite group show that they there exists a Galois extension K over Q, K over, of course, if I prove that that will be solving inverse Galois problem.

So, I want to say there is a Galois extension K over F such that. So, here the point is, I am allowed to choose both K and F depending, after you give me G, inverse Galois problem F has to be Q, only K has to be chosen. So, that makes it much more difficult. In fact, this problem is easy exercise. And that problem is an open problem. So, if you insist on F equal to Q, it is an open problem. But if you are allowed to choose any F you want, it is an easy exercise. And how do we do this?

(Refer Slide Time: 30:24)



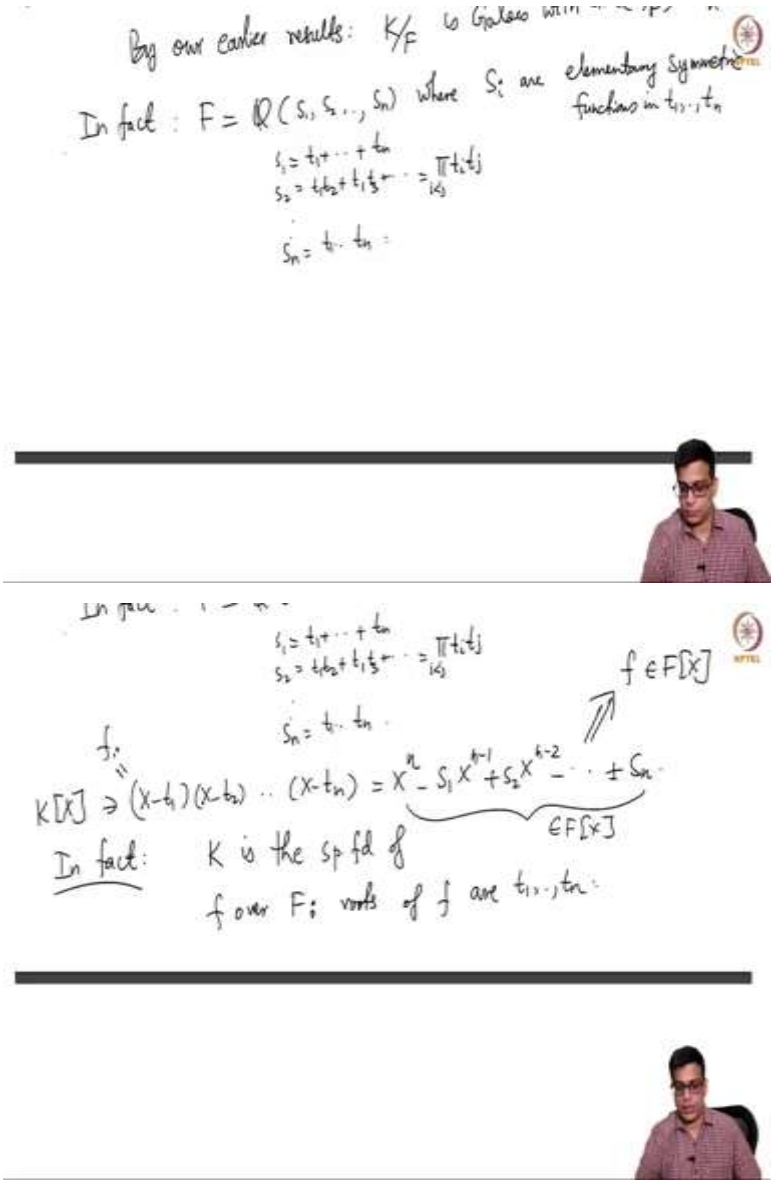


First, we will show that lemma for every n, there exists a Galois extension K over F, such that Galois K over F is isomorphic to Sn. So again, for over Q, you can do this, this is true, but significantly harder than what I am going to do. So, this requires more work. So, what I do is, you take F to be Q adjoined some variables, t1 through tn. So, I can take, can replace Q by any field here, but just for concreteness, I will do this. So, this is ti's are variables. So, what I do is, so this is a rational function field or Q in n variables.

So, then, so I am going to take this to be K actually, then Sn acts on K by permuting ti. So, of course, it fixes Q, but ti goes to ti via the action of Sn. So, take a permutation and just see where 1 goes to, if 1 goes to 3, t1 will go to t3. So, that means, sigma in Sn. So, basically Sn is in a subgroup of Galois K over Q. Of course, Galois K over Q is an infinite group, because K is an infinite extension of Q. So, there will be infinitely many elements here, but Sn is a finite subgroup.

So, let F be K power Sn. So, the fixed field of Sn. So, you have K, K power Sn and it is a triviality by our earlier results K over F is Galois with the Galois group, this is even before we talked about Galois extensions and some of the preliminary results that we did way back in the course. So, this is Galois and Galois group is Sn. In general, if you remember things like this. So, these are from earlier. Now, I want to just give you a brief idea of what F is.

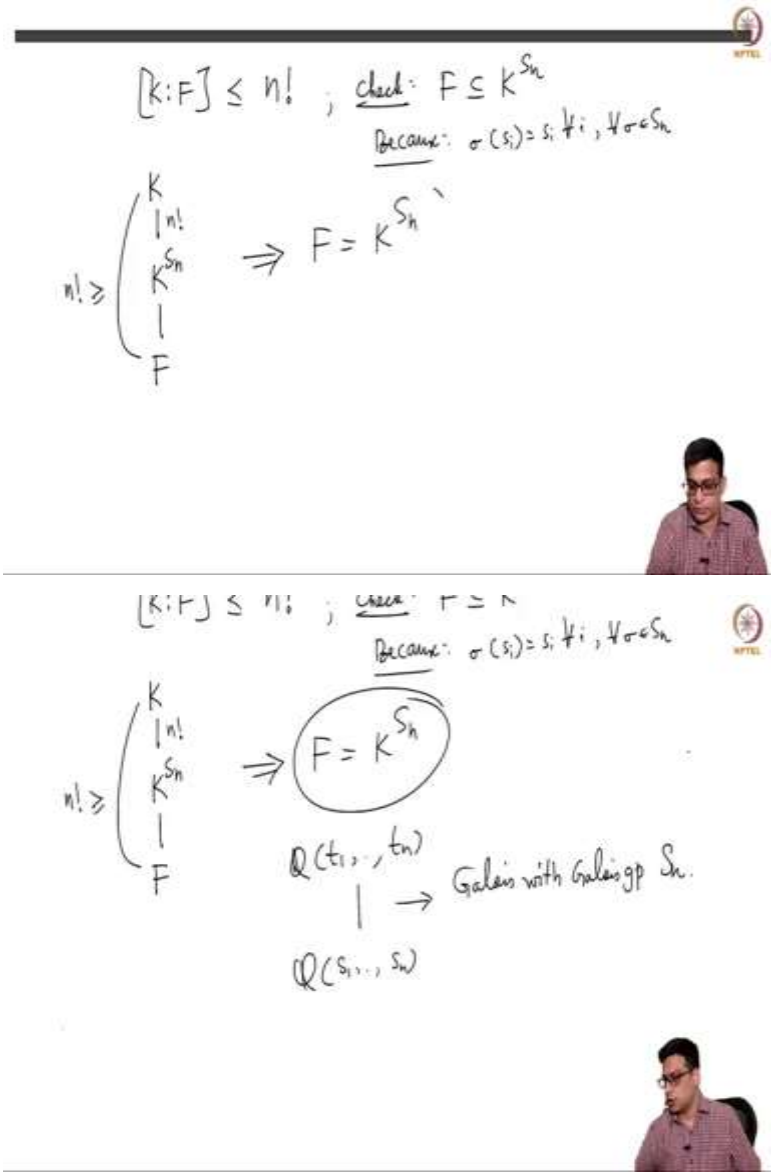
(Refer Slide Time: 33:12)



So, in fact, F is Q adjoined S1, S2, and Sn where Si are elementary symmetric functions. So, that is S1 is in t1 through tn, S1 is actually nothing but small s1 is nothing but t1 plus tn, S2 is t1, t2 plus t1 t3 and so on. So, this is in fact ti tj, i less than j. And finally, Sn is the product of all of them. So, basically what I am saying is that if you take X minus t1, X minus t2, X minus tn, this is a priori in K X is actually in FX. So, elementary symmetric functions are the coefficients of this, because coefficients of x power n minus 1 will be the sum of this and the constant term will be tn, t1 through tn, so Sn.

So, in fact, K is the, so basically this implies that, let us call this f, f is this polynomial, f is in FX, because all the coefficients are in capital F. So, k is the splitting field of f over capital F, because the roots of F are t1 through tn and of course, these are distinct elements.

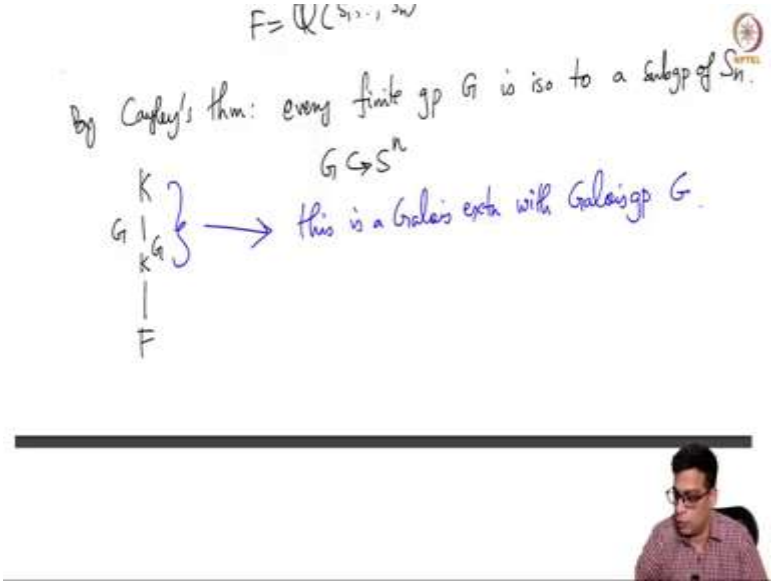
(Refer Slide Time: 35:17)



So, Kw is the splitting field, so the degree of this is at least or at most n factorial, because in general if you have a splitting field of a degree n polynomial the degree is at most n factorial, the factorial of the degree. So, now, what is k power Sn? So, I claim that f is contained in K power Sn because, this is because sigma fixes these are symmetric functions. So, by their very nature, any permutation will fix them because if you permute the sum you are not changing anything.

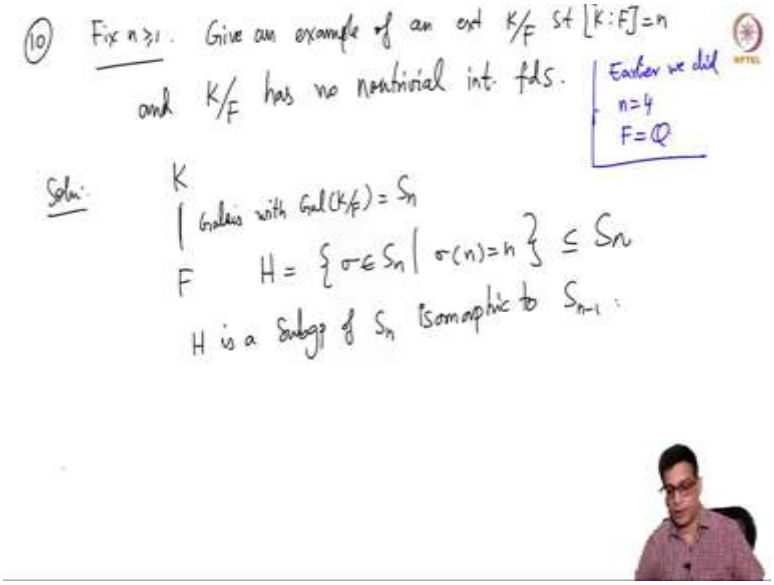
So, f, so, we have K, K power Sn and F here. So, this is less than or equal to n factorial and this is equal to n factorial. This means F equals K power Sn. So, the desired Galois extension of Galois group Sn is Q adjoined t1 through tn over Q adjoined S1 through Sn is Galois with Galois group Sn. So, this can be done for any n. Now, let us prove the solution of the, let us give the solution of the problem.

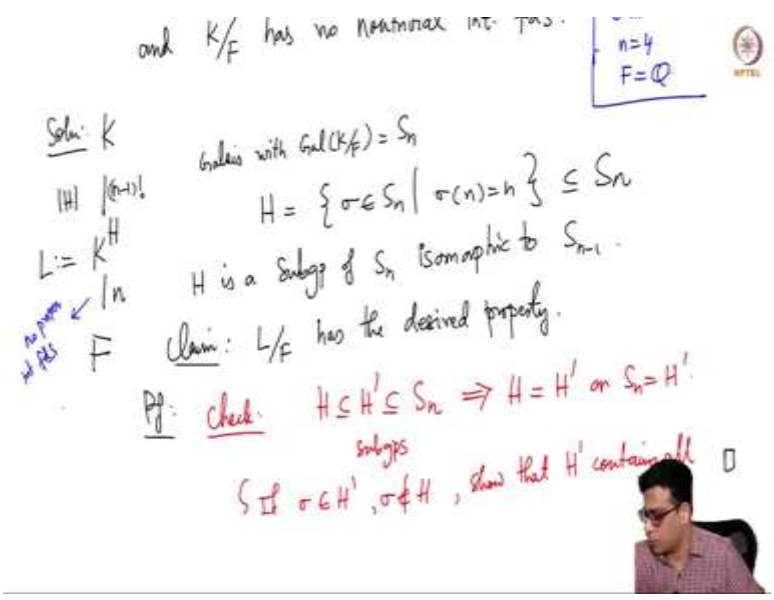
(Refer Slide Time: 36:54)

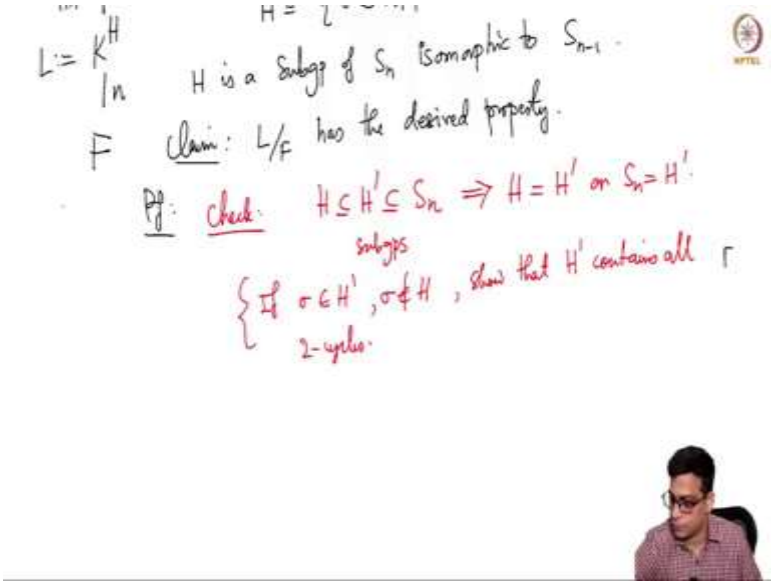


So, by Sylo theorem, by Cayley's theorem, every finite group is isomorphic to a subgroup of Sn. So, now, we are done. So, we first take K and you take F. So, G is isomorphic to so as subgroup of Sn. So, we will simply take K power G. So, this is the Galois extension, this is a Galois extension with Galois group G. So, this solves the problem. So, problem asks you to show that there is a Galois extension with Galois groups to be any given finite group and you are, you have done that, but the important thing is of course, you are allowed to choose both the top and the base feeds, if the base filed is fixed to be Q, there is no solution to this problem, this is a open problem called inverse Galois problem.

(Refer Slide Time: 38:14)







Now, last problem I want to do in this class is for every n, integer n give an example of an extension K over F such that the degree of the extension is n and K over F has no proper or non trivial intermediate fields. So, now, this is just like earlier we did n equal to 4 and F equal to Q in fact, but in general we have to allow F to be arbitrary. So, what do we do?

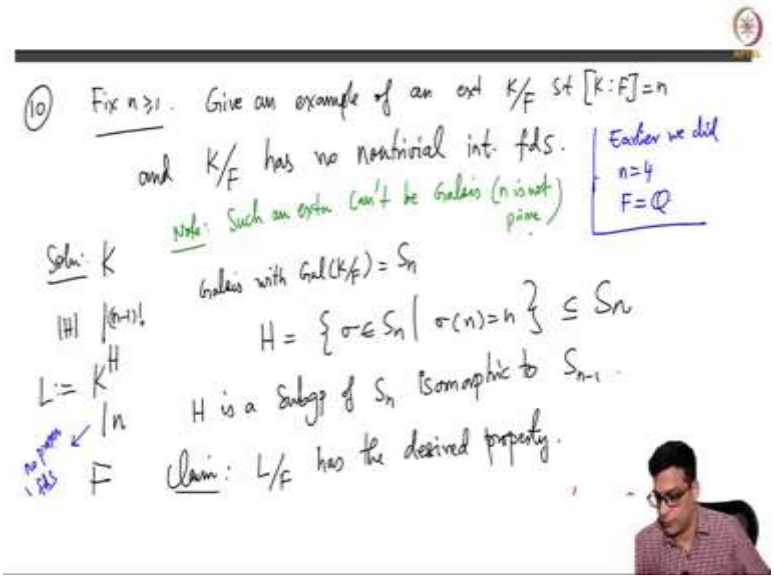
Solution, I want to quickly wrap this up. So, you take K and F Galois with Galois group Sn. Now, what do we do? What we do is the following. Let us take H to be all elements of Sn, which fix let us say n. So, this is a subgroup of Sn. So, H is a subgroup of Sn isomorphic to Sn minus 1 because it interchanges the first n minus 1 indices does nothing to the nth, last index. So, this is what we have. So, now, what we do?

As you can guess, you take K power H. So, K power H, K is a Galois extension of K power H with Galois group H which has n minus 1 factorial, the whole extension is n factorial, so this is n. So, claim is L F has the desired property. The proof is very easy, this is just like in the n equal to 4 case. All you need to do is that Sn minus 1 the way we have defined it here is a maximal proper subgroup.

So, which I will let you do this, this is a simple group theory statement. So, if you have H is contained in H prime is contained in Sn subgroups, then H equals H prime or Sn equals H prime. So, this is a statement one can show basically show that if sigma belongs to H prime and sigma is not in H that means it is not equal to H. Show that H prime contains all two cycles. So, this came up earlier when we showed that Sn is generated by a two cycle and an n cycle.

So, similar to that kind of argument you show this. So, the claim will then follow, so that any proper intermediate field must correspond to a subgroup containing capital H, but any subgroup containing capital H, is either H in which case the intermediate field is this or Sn in which case intermediate field is F. So, there is nothing in between these two, no proper intermediate fields or no nontrivial intermediate fields. So, that settles the problem with constructing degree and extensions with no proper intermediate fields.

(Refer Slide Time: 42:07)



And again, as I noted there note, such an extension cannot be Galois except in some trivial cases like n equal to prime, so, let us assume n is not prime. Otherwise there will be a prime divisor and there will be a proper subgroup, so there will be a proper intermediate field. So, I will write unless n is prime.

Of course in which case the Galois extension will not have a trivial, will not have a proper intermediate fields because a group of order p cannot have proper nontrivial subgroups. So, I think that is, I do have 1 or 2 problems but let me stop here. In the next class we will do a couple of more problems and that will end the course. Thank you.