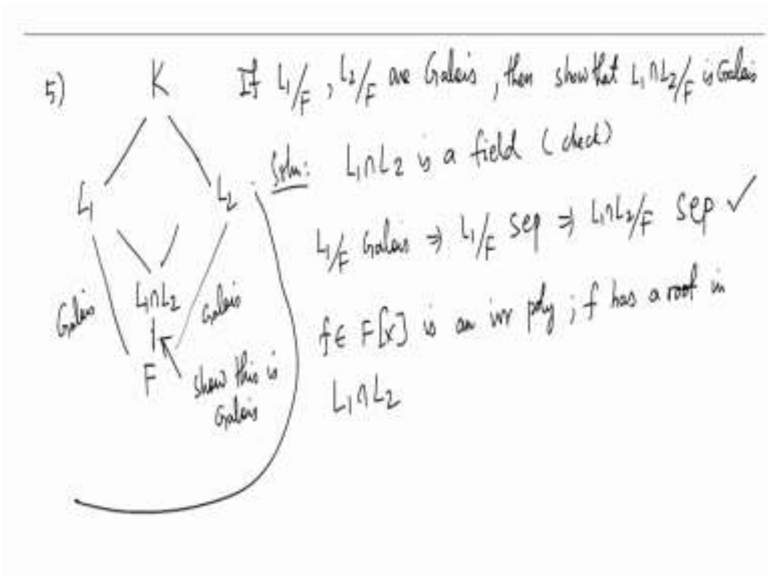
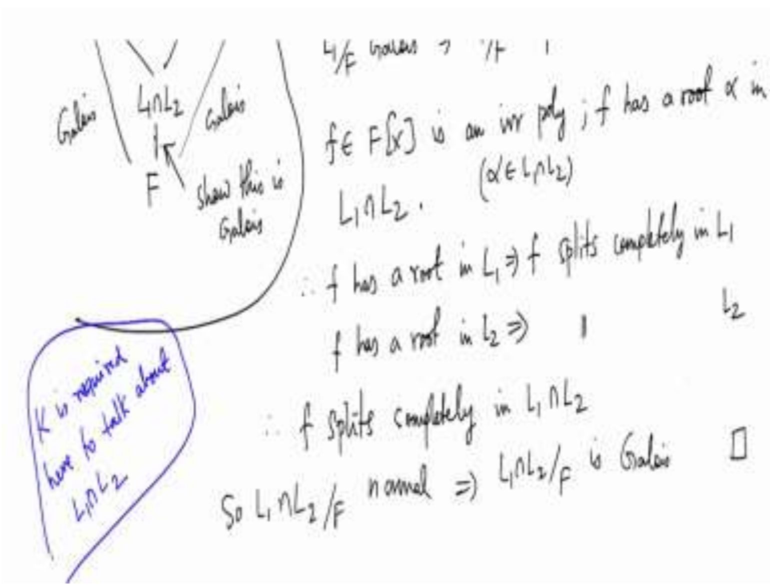
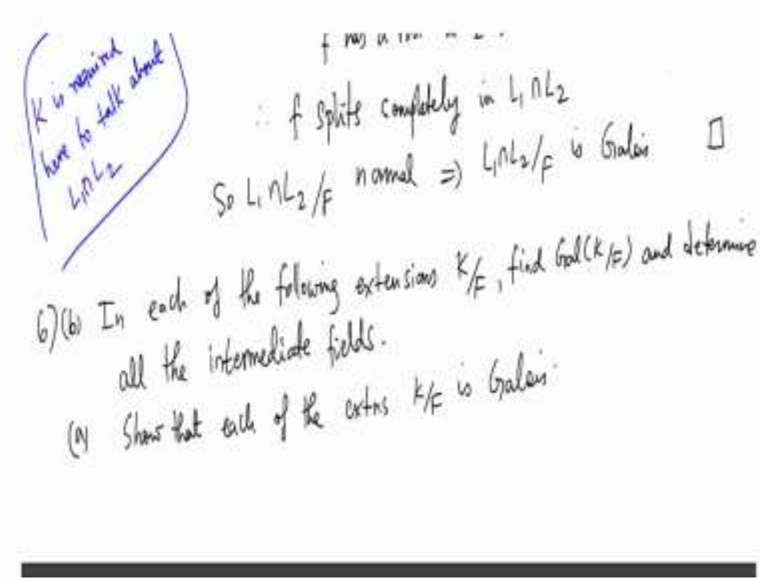
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 28
Problem Session – Part 6

Welcome Back. Let us continue doing problems, so we are in the middle of a problem session. In the last problem, we proved a very nice result about a Galois extension whose Galois group is S3, must be the splitting field of irreducible cubic polynomial. Let me continue now that was the fourth problem.

(Refer Slide Time: 0:33)







So, the fifth problem is a simple statement which sometimes comes in handy, so let us take K, and let us say there are 2 sub fields L1 and L2 and let us say they are both going to contain F, so you have K and F and 2 intermediate fields, that is the point. So, if L1 over F and L2 over F are Galois, then show that L1 intersection L2 over F is Galois. So, let me just draw a bigger picture here.

So, you have L1 and L2, then they both will contain L1 intersection L2, so if this is given to be Galois and this is given to be Galois, then we want to show this is Galois. So, what I will not say anything about is solution, I will assume that L1 intersection L2 is a field. So, check this if you want but it is very trivial because if a and b are both in L1, L2 their product is there, the sum is there and so on.

So, now, we are going to again use the Galois equals normal plus separable, that characterisation of Galoisness. So, clearly L1 over F Galois implies L1 over F is separable, this implies L1 intersection L2 over F is separable because any sub extension or separable extension is separable. So, this is separable, in fact, you do not even need to know that L2 is separable. If L1 is separable over F, L1 intersection L2 is separable.

So, separability is clear to prove normality. So, suppose F is an irreducible polynomial and suppose F has a root in L1 intersection L2. So, this.. I want to show that F splits completely at L1 intersection L2. That is one of the equivalent characterizations of normality. So, F has a root, let us say alpha in L1 intersection L2, so F has a root in… alpha is in L1 intersection L2 so it is in L1 so F splits completely in L1, similarly F has a root in L2 also because the same root alpha is in intersection so it has a root in L2, so it splits completely in L2.

Remember the set of roots of F in some large splitting field is a fixed set, so that means F splits… I mean those roots are same, whatever are the roots in L1 must be same as roots of F in L2 so conclusion is F splits completely, all those roots are in L1 as well as in L2 so there are they are in L1 intersection L2.

So, the point here is, the set of roots of F is some.. is a feature of F itself, it does not depend on extension field because the set of roots in some splitting field is a fixed set so you can always take a large splitting field of F which contains both L1 and L2. In that splitting field the roots are a fixed set so there F splits completely in L1 means that set is in L1, F splits completely in L2 means that set is in L2, that's all.

So, F splits completely in L1 intersection L2 so L1 intersection L2 is over F is normal so this implies L1 intersection L2 over F is Galois because we already argued that, it is separable. So, the only reason that I put a K here is, to consider the intersection, so K is required here otherwise K is not required in the proof. K is required here to talk about L1 intersection L2. So, intersection is a set theoretic operation, so to talk about intersection of 2 sets they must sit inside some ambient set.

So, I need a K containing both L1 and L2. So, that is why I took K, so this is a simple problem. So, let us now look at the next problem which asks the following. In each of the following extensions, find the Galois group and determine all the intermediate fields. I should also show actually, in fact, this is second statement, a is, show each of them, first show that each of this Galois and then find the Galois group and determine the intermediate fields.

(Refer Slide Time: 6:27)

(i) $K = \mathbb{Q}(\zeta_8)$ $\quad \zeta_8$: a primitive 8 th root of unity.

$\quad |$

$F = \mathbb{Q}$ $\quad$ Let's find the irr poly of ζ_8 over $\mathbb{Q}$:

$$X^8 - 1 = (X^4 - 1)\underbrace{(X^4 + 1)}_{f(X)}$$

Claim: f is irr

Pf: By Eisenstein criterion:

$X \to X+1$: $f(X+1) = (X+1)^4 + 1$

$= X^4 + 4X^3 + 6X^2 + 4X + 2$

$f(X)$ $\quad X \to X+1$:

$= X^4 + 4X^3 + 6X^2 + 4X + 2$

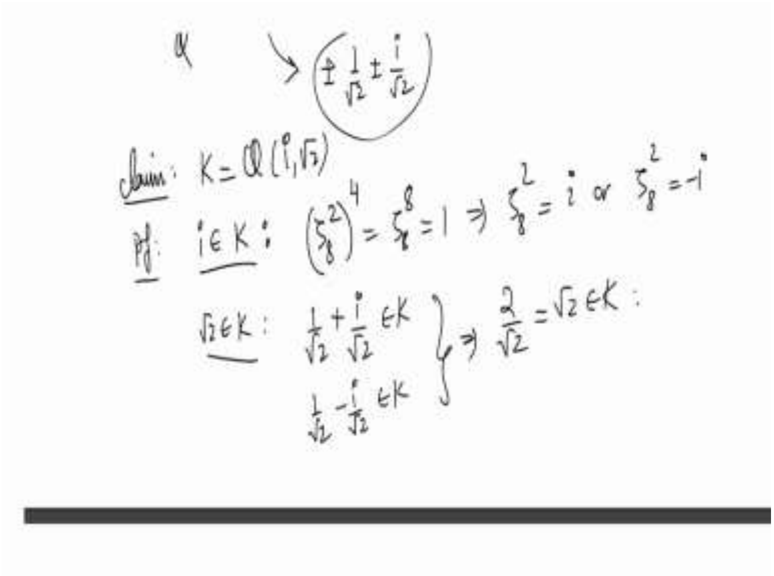
Also: $\zeta_8^4 = -1$ $\quad \therefore f(\zeta_8) = 0$, f is irr

So the irr poly of ζ_8 over $\mathbb{Q}$ is $X^4 + 1$.

$K = \mathbb{Q}(\zeta_8)$ $\quad$ Note that the primitive 8th roots of unity are

$4 \, |$ $\quad \zeta_8 = \cos \frac{2\pi}{8} + i \sin \frac{2\pi}{8}$.

$\mathbb{Q}$



So, the first one, so let us do this, K equals Q zeta 8 over, so zeta 8 is a primitive 8th root of unity. So, now I claim that first, let us find the irreducible polynomial in this. So, in order to find the irreducible polynomial, what we have to do is let us start with some polynomial that it satisfies. So, certainly it satisfies this so this factors like this. I claim that, let us call this FX so claim F is irreducible and this is simply a Eisenstein criterion statement.

Of course a priori does not apply because the leading coefficients are just one but change the variable to X plus 1 then, FX plus 1 will be x plus 1 power 4 plus 1 and then you see that, it is X power 4 plus 4x cube plus 6X square plus 4x plus 2. So, then apply with prime number 2, 2 divides all the coefficients, 2 square does not divide the last coefficient and also not that zeta 8 power 4 is not equal to 1 because it is a primitive 8th root that means, it is not a root unity less than 8.

If zeta 8 power 4 is equal to 1, zeta is also a fourth root of unity but a primitive eight root of unity so F of zeta 8 must be zero because x power 8 minus 1 has zeta, it has a zoot. Zeta 8 is not a root of this so zeta, it must be root of this and F is irreducible so the irreducible polynomial of zeta 8 over Q is x power 4 plus 1.So, now that means K which is Q zeta 8 over Q is a degree 4 extension.

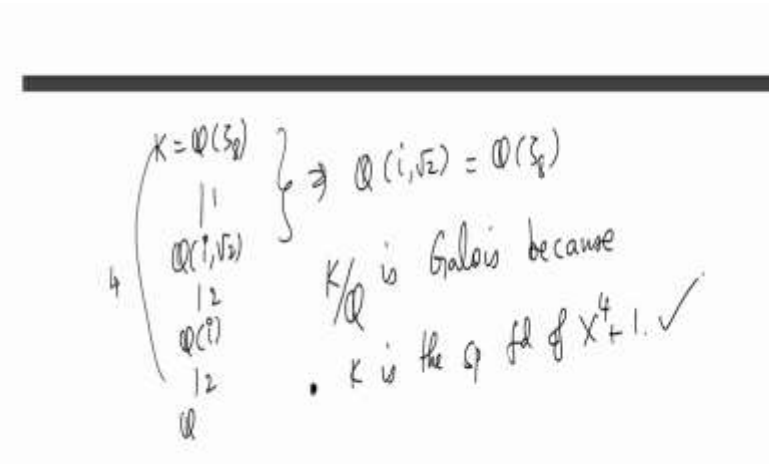
The advantages of finding the irreducible polynomial is that we know the degree of this extension so we conclude this is 4. Now we have to show, that it is Galois, we have to find its Galois group and find the intermediate fields. So, now let us first how that it is Galois, so note that, the primitive 8th roots of unity are… so this is something that I mentioned before when we discussed this particular extension before many a times so the primitive… because zeta 8 can be taken to be cosine 2 pi by 8 plus i sin 2 pi by 8, so this is cosine pi by 4 plus i sin pi by 4.

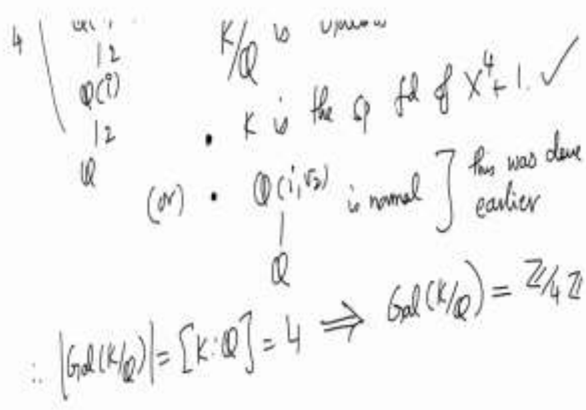
So, in fact, all the primitive 8th roots will be given by plus minus by putting plus minus here plus minus here. So, this is just a parenthetical remark so continuing here are basically plus minus 1 over square root of plus minus i over square root r. So, now I want to claim that, K is actually equal to Q adjoined i root so the proof is, first I claimed that i is in K, why is this?

I is in K because zeta 8 square power 4 is eta power 8 which is 1 that means zeta 8 square is i or minus i, depending on which primitive root we take, it will be either i or minus i, it doesn't matter which one. We conclude that zeta 8 is there so zeta 8 square is there or minus zeta 8 square is there.

So, i is there, once i is there, we can use the fact that 1 over root 2 plus i over root 2 is in K and we just concluded that i is in K, this implies… also we know that 1 minus… actually we do not need i is in K, I guess. So, this is in K because once a primitive 8th root is there, all its powers are there and these are cyclic. So, each of them is the power of the other. So, these are there, that means their sum is there, which is 2 times 2 over root 2.

(Refer Slide Time: 12:04)





So, both i and root 2 are there, this means Q adjoin, i comma root 2 is contained in K, so let me write like this, K which is Q adjoined zeta 8 which is going to contain… so this is already 4 because i and root 2, you can consider so this, I will write down once but… so this is 2 this is 2, but this is 4 so this must be 1 so this implies Q adjoin i root 2 equals 2 equals Q adjoin zeta 8.

Actually we can conclude Galoisness in any number of ways but one way to conclude that is K over Q is Galois because one reason, K is the splitting field of X power 4 minus plus 1. So, that shows that it is normal and we are in characteristic zero so it is separable, so normality is all required. Or we can alternatively argue that, is normal because i minus i are the conjugates that are there and root 2 and minus root 2 are conjugates which are there.

So, this is vague but we did this earlier so I am giving 2 alternate elements so this is Galois so now that means, the cardinality of the Galois group is equal to the degree of the field extension which is 4 so this implies. Now let us determine the either z not 4z , there are only 2 groups up to isomorphism of order 4 or Galois group is not cyclic. So, either it is cyclic then it is z not 4 z or its client for group in which case it is z not 2 z cross z not 2z.

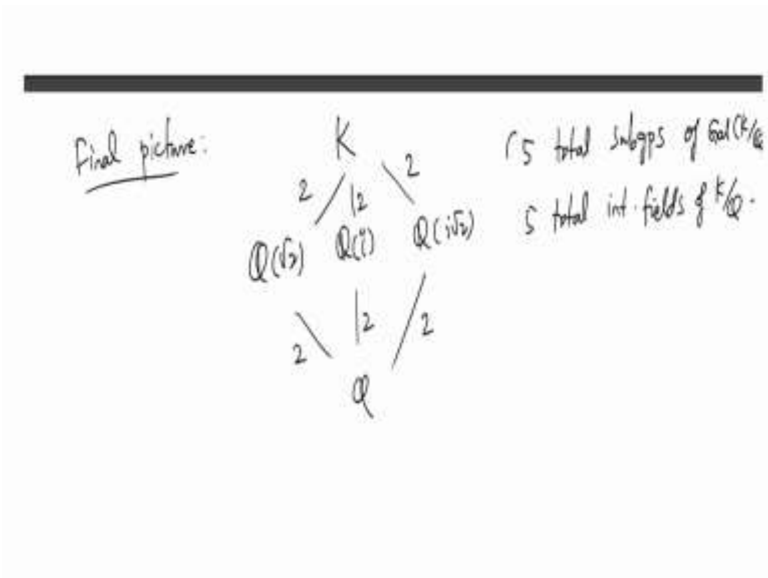
But which one is this? Here is where we are going to use the main theorem, if it is a cyclic group then K or Q has exactly one intermediate field L such that K colon L is 2, of course in that case L colon Q will also be 2. Why is this? This is because zma 2 for z so this is sorry, that is z ma 4z has exactly one sub-group of order 2. So any intermediate field with degree 2 corresponds to a sub group of order 2 of which there is exactly 1.

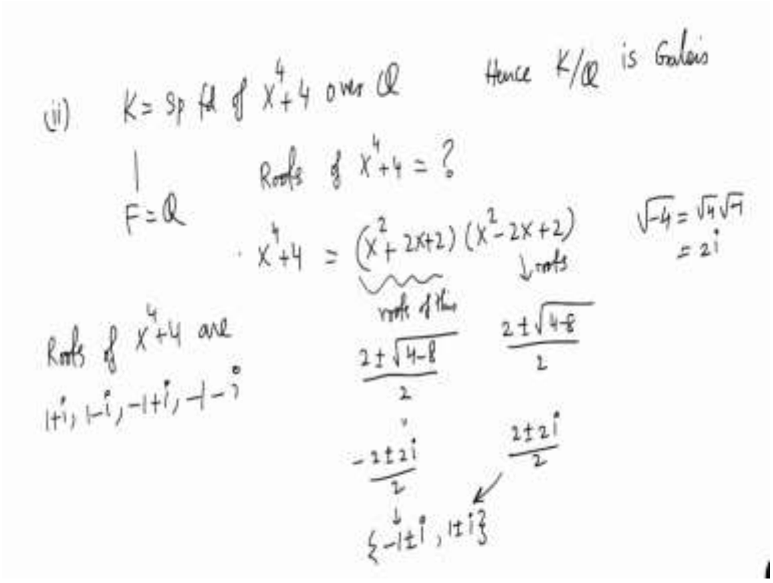
But, this is the point, but K over Q has more than 1 such intermediate field. This is clear to us because it contains Q root 2 and Qi. So, this is something that i should…. At some point say but these are not equal because this is in r, this is not in r. So, these are distinct. Hence, this is the opposite direction, we know something about the field extension, we are concluding about the Galois group hence, Galois group cannot be cyclic.

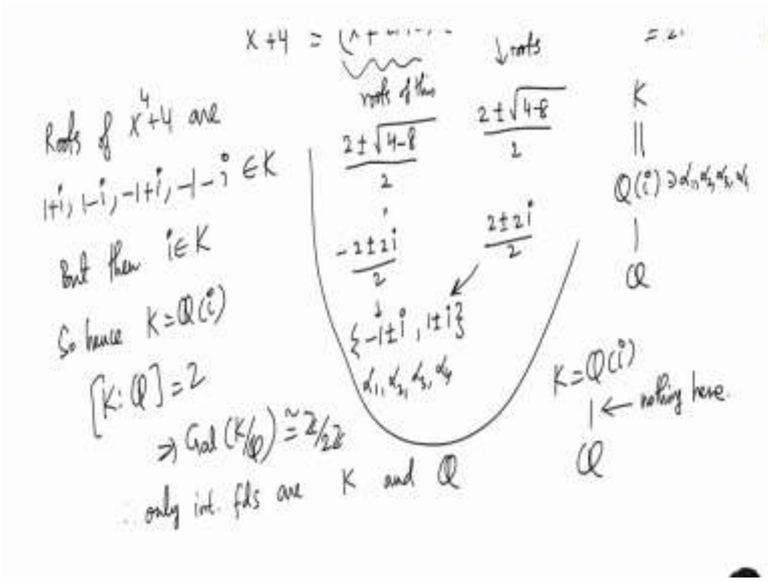
It has to be isomorphic and then that determines the Galois group, so in each of these chases we have to show its Galois which we did, find the Galois group, which we did. Now finally find the intermediate field. Now we will use the opposite direction of the main theorem knowing something about groups to conclude something about intermediate phase.

This group has 3 sub-groups of order 2 which give you this but there is one more which of course is, so the final picture is, it has 3 sub-groups of order 2 and 2 more sub groups, the entire group and the trivial group.

(Refer Slide Time: 17:00)







So, the final picture of intermediate fields is Q root 2, qi, what is the third one? If you think about it that is just Q root Q adjoin i root. We discussed this at length, so there are 5 total sub groups of G and 5 total intermediate fields of K. So, this is the picture so that completely analysis this problem so this one, it is the first part of 6.

So, let us do the second part. So, this is K, is the splitting field of this polynomial, so this is automatically… hence the first part is trivial so what we need to do is, to find the Galois group and the intermediate fields but what are the roots of this? So, in order to find the roots let us find out the factorisation of this, in fact, this is not irreducible.

So, this you can factor as x square plus 2x minus plus 2 times x square minus 2x plus 2, okay? This is the simple calculation. I can check that, you can check this so it is x square plus

2x plus 2 times x square minus 2 x plus 2 is exactly x power 4 plus 2. Now what are the roots of this? Roots of this by quadratic formula, equal to 2 plus or minus, minus b plus or minus, b square minus 4 minus 8.

So, 4 minus 8 by 2 and the roots of this are 2 plus or minus 4 minus 8 by 2 and this gives us 2 plus or minus square root of minus 4 so that is 2i by 2 and this gives 2 plus… so this is minus 2 plus or minus that, this is 2 plus or minus 2i by 2 because square root of 4 times square root minus 1, this is 2i. So, this gives us the set 1 so minus 1 plus minus i and 1 plus minus i. So, the roots of x square plus x power 4 are… there are 4 of them so this 1 plus i 1 minus i minus 1 plus i minus 1 minus i.

So, these are all going to be in K and K will be generated by this. So, they are all in K but then i is in K because 1 plus i minus 1 is in K so i is in K. So, hence, K is Qi, I mean this kind of argument we have done several times so K over Q, Qi, Q. So, now each of these roots, let us call them alpha1, alpha 2, alpha 3, alpha 4. They are all here, so once i is there 1 plus i is there 1 minus i is there and so on, so there are all there.

K is generated by them so K is equal to Qi and hence the degree extent of the extension is 2. This shows that the Galois group is… there is only one group of order 2 up to isomorphism. And the only intermediate fields are… so simple enough, so K is Qi and Q and nothing here. So, there are only 2 intermediate fields, though it is a degree 4 polynomial remember, splitting field can have degree smaller than 4, it can be at most 4 factorial, but it can be smaller than 4, so that is 2.

(Refer Slide Time: 21:57)

(iii) Sp. fd of X^3-2 over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$

- X^3-2 over $\mathbb{F}_2$: $X^3-2 = X^3$ sp. fd $= \mathbb{F}_2$ itself. ✓

  $G=\{1\}$

- X^3-2 over $\mathbb{F}_3=\{0,1,2\}$

  $0^3 = 0 \neq 2 \Rightarrow 0$ is not a root

  $1^3 = 1 \neq 2 \Rightarrow 1$ "

  $2^3 = 2 \Rightarrow 2$ is a root

  $X^3-2 = (X-2)^3$ over $\mathbb{F}_3$

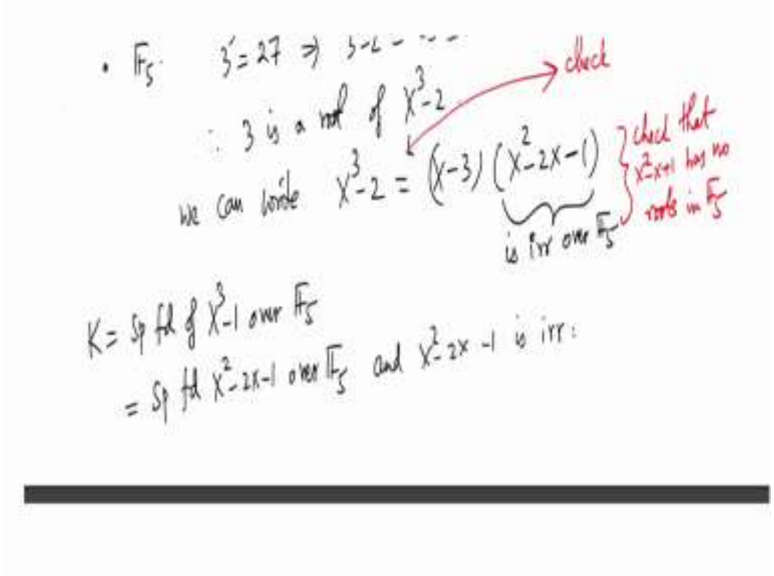
  What is the sp fd of X^3-2 over $\mathbb{F}_3$?

It is $\mathbb{F}_3$ itself. So $K=\mathbb{F}_3$ and $G=\{1\}$.

- $\mathbb{F}_5$: $3^3 = 27 \Rightarrow 3^3-2 = 25 \equiv 0$ in $\mathbb{F}_5$

  $\therefore$ 3 is a root of X^3-2 check

  we can write $X^3-2 = (X-3)\underbrace{(X^2-2X+1)}_{\text{is irr over } \mathbb{F}_5}$



So, let us do one more, let us see x cubed splitting field of x cube minus 2 over… let us do, F2, F3, F4 sorry F5, F7. So, I think I have written these 4 things, so I am going to take 4 fields and loot at all of them So, first x cube minus 2, of course is x cube and splitting field here is F2 itself because the only roots are 0 so this is trivial and the Galois group is identity and there is no intermediate field.

So, x cube minus 2 over F3. What is this? So, this I claim is, what are the roots of this? So, degree 3 polynomial, so I can quickly check the roots. So, F3 has 0, 1, 2, 0 cube is 0. So, zero is not a root. So, 0 is not 2 so any root must have cube is equal to 2. 0 is not a root, 1 cubed is 1 which is not 2 so 1 is not a root, 2 cubed is 2 so this is x minus 2 whole cubed over F3.

So, it is not separable polynomial because the derivative is 0 so not separable. Actually, I cannot say not separable but it has repeated roots because it is not irreducible so I don't want to talk about separability. So, it is x minus 2 whole cube, so what are the splitting field of… there is only 1 root 2 and it is already in F3 so it is F3 itself.

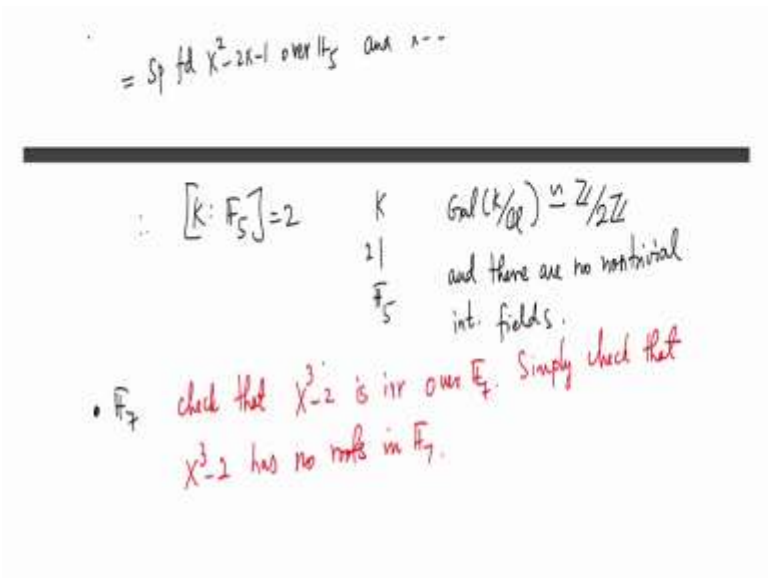
So, just like, in the case F2, K is F3 and G is identity, so Galois group is identity, there is nothing to do here, finally… not finally but F5, so in this case I claim that 2 or rather minus 2 is a root so let us say, what is 0 cubed so let me just check the roots, so 0 cubed… so you can check all of them but 2 cubed is or 3 cubed, let us say 3 cube is 27 so implies 3 cube minus 2 is 25 which is 0 in F5.

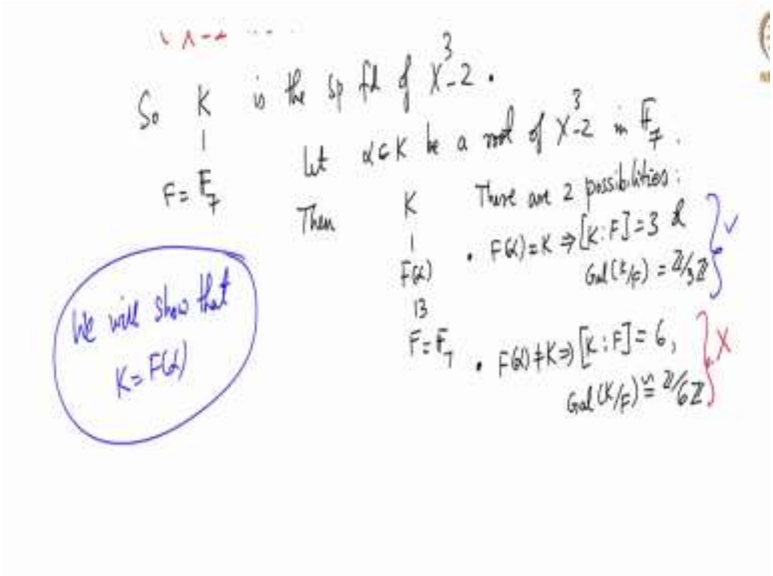
So, 3 is a root of x cubed minus 2 so we can write, so I have already done this calculation so I am going to go over this fast, but it is x minus 3 times x square minus 2x, plus or minus 1.

So, this is something you can check. This is simple calculation so check this. So, it is not irreducible, it has one root but you can also check that, this is irreducible because it is a degree 2 polynomial, all you need to check is that, it has no roots, check that, x square minus x plus 1 has no roots in F5.

For example, if you take 1 square, 1 minus 2 plus 1 is.. sorry… this is minus 1, I should have written. So, what you get is , minus 3 minus 1 so that is plus 3 which is minus 2. So, this is minus 1, if you do 1 minus 2 minus 1 that is 0. That is not 0. So, check that there are no roots. So, the conclusion is K which is the splitting field of x cubed minus 1 over F5 is actually the splitting field of x square minus 2x minus 1 over F5 and X square minus 2x minus 1 is irreducible.

(Refer Slide Time: 27:24)





So hence, K colon F5, is 2. So, K is a degree 2 extension of F5. It is irreducible, it is a splitting field of an irreducible degree to polynomial. So, it must be degree 2 so it just happens that Galois group again, there is not much choice here, is Z not 2 Z and there is no non-trivial intermediate fields. Because it is degree 2 so any intermediate field is either K or F5. So, there are no non-trivial intermediate fields and finally let is do F7.

F7, it is just happens that, is something I will check, I will ask you to check that x cube minus 2 is irreducible over F7. Simply check that x cube minus 7 has no or minus 2 or no roots in F7 because it is a degree to polynomial, if it fails to be irreducible, it must admit a root in that field. But you can check that, there are only 7 elements. 1 cube is not 2, 2 cubed is not 2, 3 cubed is not 2 and so on. So, you can check that, it has no roots.

So, K over F7 is the splitting field of x cube minus 2. So, I need to do some work here, so it is the splitting field of x cube minus 2, so the question is the Galois group… so K colon F7 is either… sorry… K colon F7 is either 3 or 6. So, I have not worked this out in detail but in general if you have a irreducible cubic polynomial, its degree is… its degree of its splitting field is either 3 or 6.

So, either by attaching 1 root, you get all the other roots or you do not get all the other roots. So, basically what I am saying is that, let alpha be a root of x cube minus 2 in F7, so what we have is.. then we have K, F alpha and F which is of course F7. So, there are 2 possibilities, either F alpha equals K in which case K colon F will be 3 and Galois group in this case has to be Z mod 3z. It is a degree 3 extension, in other words, it is a degree 3 order 3 group.

This is one possibility or F alpha is not equal to K, in which case, this will be a degree 2 extension and this will be a degree 3x, this is of course 3 because irreducible polynomial is degree 3. So, in this case, K colon F will be degree 6 and what we know for sure is that, because of the first problem which we did in this problem session in the previous video, the Galois group must be cyclic, so this must be Z mod 6Z.

So, in which case, there will be some intermediate fields, in this case, there are no intermediate fields. So, I am running out of time, so let me stop this video here, in the next video, I will argue that in fact, this occur. So, we will show that K equals F alpha, so it is in fact, this case occurs and this case does not occur. So, we will show that, that is the case and then we will complete this problem and then in the next video, I will start with this and after finishing it, I will do some more problems. Thank you.