

Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Problem Session – Part 11

(Refer Slide Time: 0:19)

3) For any $n \geq 5$, let $f(x) = X^{n-3}(X^5 - 16X + 2)$. \rightarrow not irreducible.
 Then $\text{Gal}(f) = S_5 \Rightarrow f$ is not solvable.
 Hence for every n , we have a poly of deg n which is not solvable.

4) Let $p \geq 5$ be a prime number. $p-2$ terms
 Let $f = (X^2 + 4)(X-2)(X-4) \dots (X-2(p-2)) + 2$
 $\in \mathbb{Q}[X]$.

deg $f = p$ claim: f is irr $\checkmark \rightarrow$ Pf uses Eisenstein criterion.
 $f = X^p + 2(a_{p-1}X^{p-1} + \dots + a_1X)$
 $= X^p + 2(4(2)(4) \dots (2(p-2)) + 2)$

claim: f has exactly $p-2$



1) deg $f = 5$ $g = X^5 - 4X = X(X^4 - 4) = X(X^2 - 2)(X^2 + 2)$
 Then g has exactly 3 real roots & 2 non real roots.
 $0, \sqrt{2}, -\sqrt{2} \in \mathbb{R}$ $\sqrt{-2}, -\sqrt{-2} \notin \mathbb{R}$

graph of f

graph of g

 "Shift up by 2" $f(x) := g(x) + 2$
 $= X^5 - 4X + 2$
 is irr by Eisenstein

We conclude: f has exactly
 { 3 real roots
 { 2 non-real roots

check this carefully

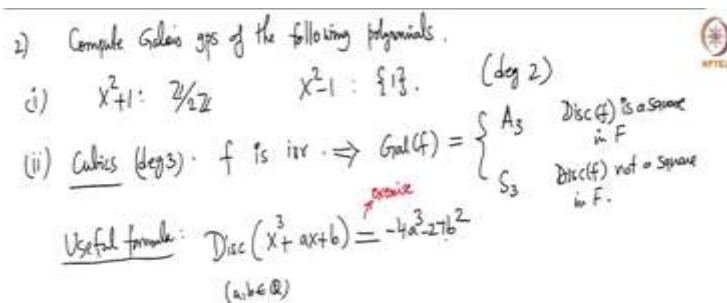
Hence $\text{Gal}(f) = S_5$ & f is not solvable \checkmark
 Pf. \therefore main result of Galois theory



Welcome back we are doing some problems. In the previous session we exhibited polynomials whose Galois group is S_5 or more generally S_p , where p is a prime number. And thereby we showed that these polynomials cannot be solved by radicals and these solutions require a little bit of work, which I did not conclusively prove, but these are left to you to explicitly construct,

show that the polynomials we constructed will have only 3 real roots and 2 non real roots. So, that is an easy exercise that you can do.

(Refer Slide Time: 0:55)



2) Compute Galois groups of the following polynomials.

(i) $X^2 + 1: \mathbb{Z}/2\mathbb{Z}$ $X^2 - 1: \{1\}$. (deg 2)

(ii) Cubics (deg 3): f is irr $\Rightarrow \text{Gal}(f) = \begin{cases} A_3 & \text{Disc}(f) \text{ is a square in } F \\ S_3 & \text{Disc}(f) \text{ not a square in } F \end{cases}$

Useful formula: $\text{Disc}(X^3 + aX + b) = -4a^3 - 27b^2$
($a, b \in \mathbb{Q}$)



So, now let us continue with the second problem. So, the first problem was to do SP, and we looked at some interesting examples of that, but let us now do compute Galois groups of some polynomials. So, I am going to go a little fast with these examples, I will indicate what needs to be done and maybe leave some exercises for you to do along the way. So, let us do some simple things first, I am in for example, X square plus 1. So, I will simply write the Galois group is here $\mathbb{Z} \bmod 2\mathbb{Z}$ and if you take X square minus 1, the Galois group is trivial.

So, if you take a degree 2 polynomial its splitting field will have Galois group, a subgroup of S_2 . So, if the polynomial is irreducible, it will be all of us to which is $\mathbb{Z} \bmod 2\mathbb{Z}$ if it is not irreducible, then it will be trivial. So, I just want to set that simple case first. Now, let us look at cubics so that has degree 3. So, we know that and we assume that f is irreducible. Otherwise, it will be a product of linear and degree 2 which we have already considered so there is no reason to look at it again.

So, we assume f is irreducible, then Galois group of f is either A_3 , if discriminant of f is a square in f , wherever you are, f is defined, so the base field is F , then if it is a square it is and if the discriminant is not a square. So, this is just to recall what we have done. It is not a square that

means it is S_3 all of S_3 . So, a useful formula that can be proved using some tedious computation is the following.

If you take a polynomial, irreducible polynomial of sorry, if you take a degree 3 polynomial without any degree 2 term something like this, for a and b are rational numbers let us say, the discriminant is actually minus $4a$ cube minus $27b$ square, this is an exercise I have written down the discriminant for an arbitrary degree 3 polynomial earlier in the course, but if you apply that with the quadratic term being 0 you get this. So, just using this, let me just give you 2 examples.

(Refer Slide Time: 3:33)

Useful formula: $\text{Disc}(X^3 + ax + b) = -4a^3 - 27b^2$
 $(a, b \in \mathbb{Q})$

any root $\frac{r}{s}$ must have $r \equiv \pm 1 \pmod{3}$ and $s \equiv \pm 1 \pmod{3}$ but r, s are not units.

- $X^3 - X - 1 \in \mathbb{Q}[X]$ (check irreducible)
 $\text{Disc} = 4 - 27 = -23 \Rightarrow \boxed{\text{Gal}(f) = S_3}$
- $X^3 - 3X + 1 \in \mathbb{Q}[X]$ (check irreducible)
 $\text{Disc} = -4(-27) - 27 = 4 \cdot 27 - 27 = 3 \cdot 27 = 9^2$
 $\Rightarrow \boxed{\text{Gal}(f) = A_3}$

Rational root test: $f = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X], a_n a_0 \neq 0$.
 Let $r, s \in \mathbb{N}$. Then $\frac{r}{s}$ is a root of $f \Rightarrow r | a_0$ and $s | a_n$.
 $(r, s) = 1$ Form: $a_n \frac{r^n}{s^n} + \dots + a_1 \frac{r}{s} + a_0 = 0 \Rightarrow a_n r^n + a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} + a_0 s^n = 0$

So, if you take $X^3 - X - 1$ in $\mathbb{Q}[X]$, so check that it is irreducible. I am going to give you a quick reason why in a minute, but it is irreducible. I can check then what is the discriminant? This is equal to, this is a polynomial of this form, it is called a depressed cubic meaning the x^2 term is not there. So, a is minus 1. So, minus 1 cube is minus 1. So, that is 4, b is minus 1, b square is 1. So, this is minus 23, not a square. So, the Galois group is S_3 .

On the other hand, if you take $X^3 - 3X + 1$ again check that it is irreducible. Then discriminant is minus 4 times minus 3 whole cube that is minus 27. It will be plus 27. Because minus 27 minus 4 times 27 b square so that is, this is minus but then it will be 4 times 27 minus 27, b is 1 so that is minus 27. So, this is 3 times 27 which is of course 9 square. So, this implies Galois group is A_3 , it is a cyclic group of order 3, in this case it is S_3 . So, I wanted to do these 2

examples, because I wanted to indicate that both cases occur. So, this is not particularly surprising to you, we have discussed these such things in the past.

(Refer Slide Time: 5:35)

Rational root test : $f = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X], a_n a_0 \neq 0$.

Let $r, s \in \mathbb{N}$. Then $\frac{r}{s}$ is a root of $f \Rightarrow r | a_0$ and $s | a_n$.

(r, s) = 1
coprime

Easy: $a_n \frac{r^n}{s^n} + \dots + a_1 \frac{r}{s} + a_0 = 0 \Rightarrow a_n r^n + a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} + a_0 s^n = 0$

$\Rightarrow r(a_n r^{n-1} + \dots + a_1 s^{n-1}) = -a_0 s^n$

$\Rightarrow r | a_0 s^n \Rightarrow r | a_0$



So, just to give you one test for irreducibility which maybe I have not discussed earlier in the course, in the beginning when I gave you some irreducibility tests, I do not recall if I did this, so usual things Eisenstein reduction modulo p , but this is also very useful. So, this is if f is any arbitrary polynomial like this with integer coefficients and of course, we assume a_n is nonzero, but we will also assume that a_n times a_0 is nonzero. So, both the leading term and the constant term are nonzero, leading coefficient and constant coefficient are nonzero.

So, then let us take two integers r and s which are co prime. So, co prime, then r by s is a root of f . So, rational root tells whether r by s a given rational number is a root or not, it at least says when it cannot be root then our divides is a_0 and s divides a_n . So, this is easy proof. So, a general version of this is from Eisenstein criterion, but you can or Gauss lemma but you can directly do this because, if you do this is standard, so if r by s is a root, you have a_n times $a_1 r$ by s plus a_0 is 0.

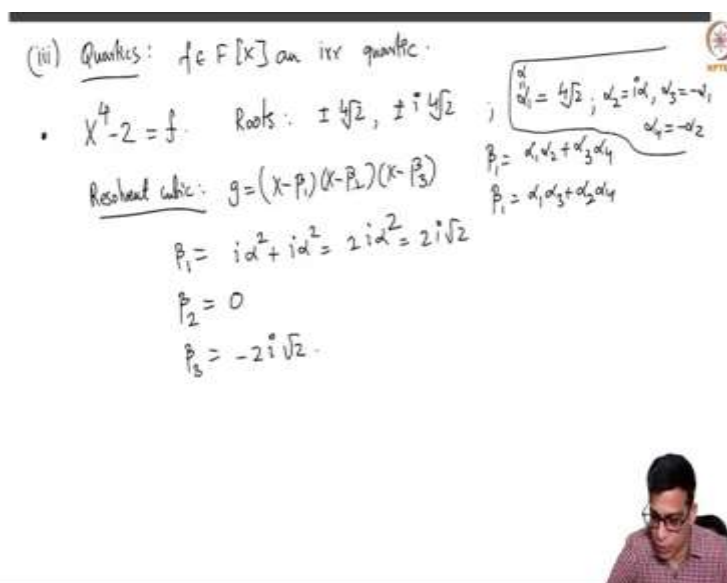
So, this implies $a_n r^n$ plus $a_{n-1} r^{n-1} s$ plus $a_{n-2} r^{n-2} s^2$ plus $a_{n-1} r^{n-1} s$ plus $a_0 s^n$ equal to 0. So, multiply by clear denominator I mean so you get this, but this implies. So, I am just quickly giving you a reason for this. So, by taking the last term on the other side, you get r times $a_n r^{n-1}$ plus $a_1 s^{n-1}$ equals minus a_0

sn. So, all the terms except the last one are divisible by r. So, this implies r divides a_0 sn but r and s are co prime So, r divides a_0 . So, that is the first part.

Similarly, you can get s divides a_n . So, this is very useful especially when you have leading term 1 or constant term 1 like in these examples, so all you need to check is that here these are degree 3. So, they are irreducible if they have no roots. So, any root must have, because constant is 1, leading term, leading coefficient is 1. So, only possible rational roots are 1 and minus 1 which you can quickly check are not roots, 1 and minus 1 are not roots for this.

So, these 3, these 2 cubic polynomials do not have roots. So, they must be irreducible. So, this rational root test is a very nice convenient way of checking the irreducibility of degree 2 or degree 3 polynomials.

(Refer Slide Time: 9:19)



(iii) Quartics: $f \in F[X]$ an irr quartic.

• $X^4 - 2 = f$. Roots: $\pm \sqrt[4]{2}, \pm i \sqrt[4]{2}$

Resolvent cubic: $g = (X - \beta_1)(X - \beta_2)(X - \beta_3)$

$\alpha_1 = \sqrt[4]{2}, \alpha_2 = i\sqrt[4]{2}, \alpha_3 = -\sqrt[4]{2}, \alpha_4 = -i\sqrt[4]{2}$

$\beta_1 = \alpha_1 \alpha_2 + \alpha_3 \alpha_4$
 $\beta_2 = \alpha_1 \alpha_3 + \alpha_2 \alpha_4$
 $\beta_3 = \alpha_1 \alpha_4 + \alpha_2 \alpha_3$

$\beta_1 = i\alpha^2 + i\alpha^2 = 2i\alpha^2 = 2i\sqrt{2}$
 $\beta_2 = 0$
 $\beta_3 = -2i\sqrt{2}$

Now, let us go to the quartic case. And again, I am going to take an irreducible quartic because if it is reducible, its roots are already in, it is already a product of smaller degree polynomials whose Galois groups we have discussed. So, there is no new phenomenon, all you need to do is consider irreducible quartics. So, I have to, I want to introduce certain.

So, then first I want to do some simple ones before I give you some general formulas which help us. If you take X power 4 minus 2 as your f its roots are as we know very well, the roots are plus minus fourth root of 2 and plus minus i times fourth root of 2. So, fourth root of 2 is a real fourth root of 2. So, you take plus minus fourth root of 2 and plus minus i times fourth root of 2 because

I use a primitive fourth root of unity, every time you have a real fourth root of 2 you can multiply by i to get other roots.

So, let us say α_1 is fourth root of 2. So, I want to just explore what happens here. Recall the analysis that we have done for quartics, there we had to first consider resolvent cubic, resolvent cubic was X minus β_1 , X minus β_2 , X minus β_3 , where β_1 is $\alpha_1 \alpha_2 + \alpha_3 \alpha_4$ and so on. So, in this case, β_1 will happen to be. So, if you call them α_1 , α_2 , actually, so α_1 is this, α_2 is $i \alpha_1$, α_3 is $-\alpha_1$, α_4 is $-\alpha_2$.

So, this is how I define the label the indices, so there are 4 roots like this. So, then β_1 will be actually $\alpha_1 \alpha_2 + \alpha_3 \alpha_4$, which will be $i \alpha_1^2 + \alpha_1^2$, so α_1^2 is equal to α_2^2 plus $\alpha_3^2 + \alpha_4^2$, so, that is also $\alpha_1 \alpha_2$, which is also $\alpha_1 i \alpha_1$ so $2i \alpha_1^2$, which is of course, $2i \sqrt{2}$. If you took β_2 , which is $\alpha_1 \alpha_3 + \alpha_2 \alpha_4$, you see that it is 0. So, that is a simple calculation, and β_3 is $-\alpha_1 \alpha_2 + \alpha_3 \alpha_4$, which is of course, $-2i \sqrt{2}$. So, I do not want to spend too much time on this, this is just a computation which is not that interesting. So, I will breeze pass this.

(Refer Slide Time: 12:20)

Resolvent cubic: $g = (X - \beta_1)(X - \beta_2)(X - \beta_3)$

$\beta_1 = i\alpha^2 + i\alpha^2 = 2i\alpha^2 = 2i\sqrt{2}$

$\beta_2 = 0$

$\beta_3 = -2i\sqrt{2}$

$\therefore g = (X - 2i\sqrt{2})(X + 2i\sqrt{2})X = X(X^2 + 8) = X^3 + 8X$

reducible

Know: $\text{Gal}(f) = D_2$ or D_4 or A_4 . has exactly one root in \mathbb{Q} .

$K = \mathbb{Q}(i, \sqrt{2})$

$12 = 2^2 \cdot 3$

What is $[K:\mathbb{Q}]$? (8)

$\therefore \text{Gal}(f) = D_4$


But then we can now compute g that will be X minus $2i \sqrt{2}$ times X plus $2i \sqrt{2}$ times X , X minus β_2 is 0 X . So, this actually will give you X times X^2 plus 8 because $2i \sqrt{2}$ whole square is 4 times minus 1 times 2. So, this is X^3 plus $8x$ and this is reducible, in fact

has exactly 1 root in \mathbb{Q} . So, if you Now recall the table for quad discrim. So, g reducible, g irreducible, d square, d not a square, these are the 4 possibilities, I think this was A4, this was S4, this is D2, this is D4 or C4.

So, g is reducible here and even without looking at the discriminant we know that the Galois group of f must be D2 or D4 or C4, because this case cannot occur, because G is reducible. And I think we in fact, analyzed it further. If it is completely reducible, then it is D2, if it has exactly 1 root it is D4 or C4. So, we can rule this out, because g is not completely reducible in \mathbb{Q} , but which 1 will occur here? So, now, here is where we look at the degree.

What is the degree of K colon \mathbb{Q} ? K is of course, a splitting field. So, K is nothing but i and fourth root of 2. So, this will have degree 8, it is 8. Now, only D4 has order 8, C4 has order 4, so this cannot happen. So, looking at the specific polynomial we will conclude that it is D4. So, let me just give you some more simple. So, I hope this is clear. So, here it is D4 and this is in fact something that is not new for us we have considered this.

(Refer Slide Time: 14:45)




$\mathbb{Q} \xrightarrow{14}$

$\bullet X^4 + 1$

$K = \mathbb{Q}(\sqrt[4]{2})$
 $\mathbb{Q} \xrightarrow{14}$

$\therefore \text{Gal}(K) = D_2$

$\text{roots: } \pm 1, \pm i$
 $g = X^3 - 4X \rightarrow \text{completely reducible in } \mathbb{Q}$
(no cubic)



$K = \mathbb{Q}(\sqrt{2})$
 $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$
 \mathbb{Q}
 $f = X^4 - 4X^2 + 2$
 irr by Eisenstein
 $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$
 Ex: $\sqrt{2+\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in K$
 $\sqrt{2+\sqrt{2}} \in K \Rightarrow 2+\sqrt{2} \in K \Rightarrow \sqrt{2} \in K$
 $\Rightarrow \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in K$
 Claim:
 check that roots are: $\pm \sqrt{2 \pm \sqrt{2}}$ ✓
 $x = \sqrt{2+\sqrt{2}} \Rightarrow x^2 = 2+\sqrt{2}$
 $\Rightarrow (x^2-2) = \sqrt{2}$
 $\Rightarrow (x^2-2)^2 = 2$
 $\Rightarrow x^4 - 4x^2 + 2 = 0$
 $[K:\mathbb{Q}] = 4$
 $G = D_2 \cong C_4$
 K
 \mathbb{Q}



So, if you do $X^4 + 1$ here the roots are plus minus 1 plus minus i . So, you can actually by hand compute the resolvent cubic, G will always denote resolvent cubic for me in this case situation, resolvent cubic is actually nothing but $X^3 - 4X$, so this is an exercise. So, you take all of the beta i and we compute this. So, this completely reduces, completely splits in \mathbb{Q} , because its roots are 0 and 2 and minus 2. So, it will, it has 3 roots there. So, the Galois group is D_2 here, but of course, we know that already, because the splitting field is \mathbb{K}_i , so this is just revisiting a well known example with something that we already know.

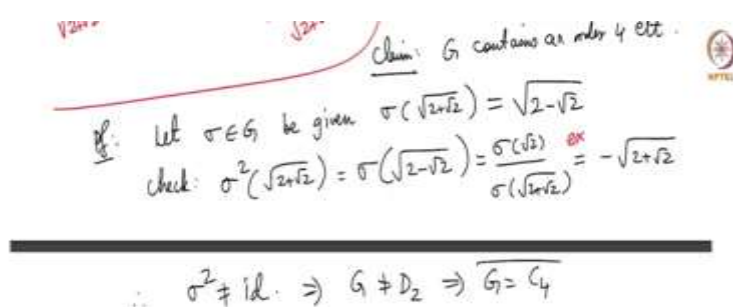
So, now the third example I want to do, so maybe I will just, I do not want to use A, B, C because I will use them later. So, this one is $X^4 - 4X^2 + 2$. So, I want to do this also explicitly without using any formulas for resolvent cubic. So here, you check that roots are plus minus $2 \pm \sqrt{2}$. So, here, in fact, what you can do is if you take X equal to $2 \pm \sqrt{2}$ square root and you compute the irreducible polynomial, you get X^2 equals $2 \pm \sqrt{2}$, and then do $X^2 - 2$ equals $\pm \sqrt{2}$, so that means square again.

So that will be $(X^2 - 2)^2 = 2$. So, this is $X^4 - 4X^2 + 2$, so that is plus 2 equal to 0. So, the irreducible polynomial of this is this and this is of course, irreducible by Eisenstein. And we know that earlier two polynomials are also irreducible, one can check that time in I will leave that for you and this is irreducible and the other roots are given by this.

Of course, you can take minus of this it will give, it will have the same irreducible polynomial, but you can put minus here also. So, the splitting field is actually. So, this is an exercise again. So, the 4 roots are, negative of this is already there, but all you need to do is to show that square root 2 minus root 2 can be expressed as a polynomial of this, so and that I can, I will tell you what it is and you can check this.

So, this is again in K because 1 square root 2 plus root 2 is there. So, square root 2 plus root 2 is in K. It means 2 plus root 2 is in K, because you can square this, but 2 is of course in K. So, root 2 is in K that means root 2 divided by and then you simply check that these are equal this ratio is this, this is a triviality. So, here Galois group has order 4, Galois group has order 4 because K over Q is degree for you, attach one of the roots, other roots are already there. And that root has degree 4. So, and in our list, what are the degree 4 things, it is either D2, which has degree 4, D4, D4 has degree 8, A4 has degree twelve, S4 has order 24. So, it is either D2 or C4, but which is it.

(Refer Slide Time: 19:04)



$\sqrt{2+\sqrt{2}}$ $\sqrt{2-\sqrt{2}}$ Claim: G contains an order 4 elt. NPTEL

$\sigma \in G$ be given $\sigma(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}}$

check: $\sigma^2(\sqrt{2+\sqrt{2}}) = \sigma(\sqrt{2-\sqrt{2}}) = \frac{\sigma(\sqrt{2})}{\sigma(\sqrt{2+\sqrt{2}})} = -\sqrt{2+\sqrt{2}}$

$\sigma^2 \neq \text{id} \Rightarrow G \neq D_2 \Rightarrow G = C_4$



So, I claim that you can check this by computing the resolvent cubic and showing that it will have exactly 1 root and not all 3 roots in Q, but more directly, one can check that G contains an order 4 elements. What separates the client 4 group and the cyclic group of order 4? Client 4 group has all elements of order two other than the identity, C4 has an element of order 4, so if G contains an element of order 4, one can show that, then it will follow that it is C4.

So, let us consider this particular sigma of square root. So, to determine automorphism of K , all you need to say is what is the image of the generator which is square root of 2 plus root 2, I will define this to be it can be any of the 4 other, 3 other conjugates, any of the 4 conjugates. So, I will take 2 minus root 2 square root. So, then check that sigma square of this is actually sigma of this which is square root 2 minus root 2.

So again, I am going fast about this, and using the fact that square root 2 minus root 2 is root 2 divided by sigma of square root 2 plus root 2. And then you do a little bit of analysis and show that, so this is an exercise. So, as I said, I want to do more as many problems as possible. So, I do not want to do every detail, so I want to isolate where I leave the exercise for you. So, this equality is an exercise, it is a trivial exercise, same computational exercise.

So, that means sigma square is not identity. So, this is not square root 2 plus root 2. So, this means g cannot be D_2 , because in D_2 , every element has square equal to identity, so G is C_4 . So, you have an example with C_4 , you an example with D_2 . And you have an example with D_4 .

(Refer Slide Time: 21:27)

Resolvent cubic of $x^4+cx+d = x^3-4dx-c^2$ - pages in literature

- $f = x^4 - x - 1 \in \mathbb{Q}[x]$. [check: f is irr: check by going modulo 2]
- $\text{Disc}(f) = -283$ not a square
- $g = x^3 + 4x - 1 \in \mathbb{Q}[x]$ is irr (by rational root test)



And for other things, I want to introduce now some more theory, and some general useful facts about discriminants and resolvent cubics. And this is the following. So, if you have a quartic polynomial of the form $X^4 + CX + D$, so it has no cubic or quadratic term, then it just happens to be $256 D^3 - 27 C^4$. And the resolvent cubic of the same polynomial. So, these are some computational things, which one can find in literature, you can take help from some notes, online notes that you will find and compute this.

And so I do not want to get into that computation. I would rather use just these formulas to give you some interesting examples. So, these are facts. So, you can find them in literature, just search for this. If you have any questions about where to find them, please feel free to contact me or ask in discussion forums. So, now using this, I want to consider this polynomial as a rational polynomial. And again, I want to quickly move on to the next problem. So, I will let you check this f is irreducible. Check by going modulo 2, so go modulo 2 and show that that column is reducible, it is not enough to show that it has no roots. Because it is degree 4.

First you have to show it has no roots, then it can split potentially as a degree 2 times degree 2, you show that that is not the case modulo 2. So, this is an exercise for you. So, this is an irreducible polynomial of this form. So, the discriminant, you can compute using this formula here happens to be minus 283. So, this is not a square, because it is a negative number. So, it is not a square and g happens to be $X^3 + 4X - 1$.

So, this also you can check is irreducible. I will let you check this by, for example, rational root test, here any root must be 1 or minus 1, but neither of those is a root so there are no roots, it is a cubic polynomial. So, it is irreducible. So, we have g reducible and D not a square, so it must be S_4 . So, Galois group of f is S_4 . So this, I have, I am trying to give you examples of every group here, D_2 is covered, D_4 , C_4 are covered, S_4 is covered. Now, let us look at an example with A_4 .

(Refer Slide Time: 24:34)

$\therefore \text{Gal}(f) = S_4$
 $f = x^4 + 8x + 12 \in \mathbb{Q}[x]$
 is irr
 $D = (3^2 - 2^6)^2$: a Square in \mathbb{Q}
 $g = x^3 - 48x - 64$
 is irr (check modulo 5)
 Exercises:
 check: ① f has a root using rational root test.
 ② Show that $f \pmod{5} = (\text{linear}) (\text{cubic irr})$
 ③ $f = gh \Rightarrow f$ has 2 roots modulo 5.
 $\uparrow \uparrow$
 deg 2 deg 2



And this also, I will sort of not explain in detail. You take this. I claim, I mean you cannot apply Eisenstein and it is not clear. I mean, it is not immediate, it requires some work to do this, first show that F has no roots. Using rational root test, show that it has no roots that one can check because any root must be an integer that divides 12 and you check for all of those divisors of 12, none of them is a root. So, it has no rational roots, but that does not immediately imply unlike in the degree 2 or 3 case that is irreducible, because there is a chance that it can split as an irreducible quadratic times another irreducible quadratic.

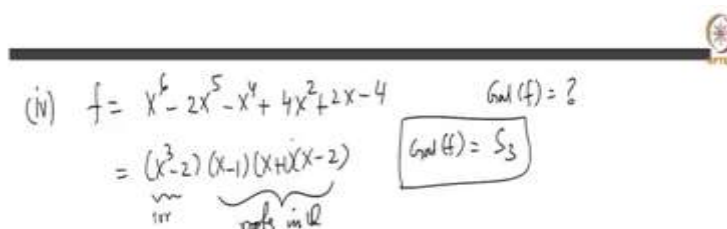
Now, show that $f \pmod{5}$ is a linear polynomial times a cubic irreducible polynomial. So, a linear polynomial times a cubic irreducible polynomial and you show that if f has, if f has gh , g and h are degree 2 irreducible, then if you have, this implies that f has 2 roots modulo 5, but this violates this. So, f has exactly 1 root modulo 5. So, you can show this, all this using these exercises. So, this is not easy.

So, this is an exercise, but one can do this, this is a good exercise to get experience with computing irreducible, verifying irreducibility of polynomials but I do not want to get into that. So, this is irreducible and just applying blindly this formula, you conclude that discriminant is actually $3^2 \cdot 2^6$. So, D is a square. So, just blindly apply this and you get the formula is here, you apply the formula for discriminant, you get this.

And g happens to be $X^3 - 48X - 64$. And you can check that this is irreducible by going modulo for example 5. So, you can either do rational root test or directly check modulo 5 and you look at it and you show that it has no roots, so it is irreducible modulo 5. So, this is mod irreducible in \mathbb{Q} itself. So, we are in this situation where discriminant is a square but g irreducible and hence, Galois group of f is A_4 . So, you have all possibilities now, that we have covered. So, you have A_4 , S_4 , D_2 , D_4 , C_4 , so, all the 5 examples are covered now.

So now, let me just do one more simple thing to just illustrate what happens if you have a higher degree. So, let us see, so I want to find where I wrote this. So, degree 5 we have considered earlier. And so last thing I will do 5 4, quartics is 3, so 4.

(Refer Slide Time: 28:47)



$$\begin{aligned}
 \text{(iv)} \quad f &= X^6 - 2X^5 - X^4 + 4X^2 + 2X - 4 & \text{Gal}(f) &= ? \\
 &= \underbrace{(X^3 - 2)}_{\text{irr}} \underbrace{(X-1)(X+1)(X-2)}_{\text{roots in } \mathbb{R}} & \text{Gal}(f) &= S_3
 \end{aligned}$$

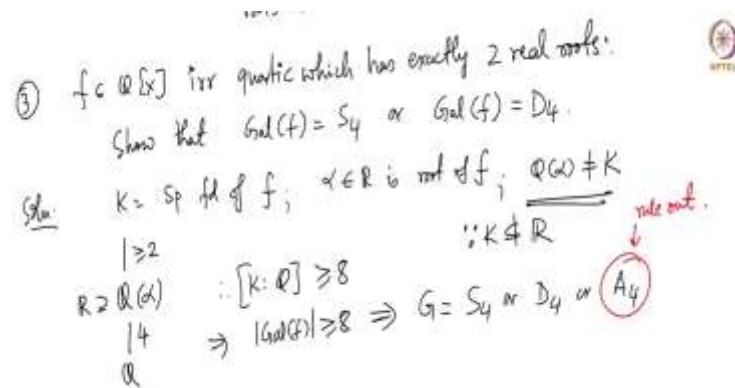


So, I give you a column of degree 6 like this. So, $X^6 - 2X^5 - X^4 + 4X^2 + 2X - 4$, I hope I have done this calculation correctly. So, what you will see this is a trick question. So, what is the Galois group of this? Of course, it looks very strange and you have no way of doing this for degree 6. But it I cooked it up exactly so that you have $X^3 - 2$ times $(X-1)$ times $(X+1)$ times $(X-2)$.

plus 1 times X minus 2. So, 1, minus 1, 2 are all roots of this. So, now these are all going to be linear in \mathbb{Q} and this is irreducible.

So, Galois group of f is actually nothing but S_3 because $X^3 - 2$ has S_3 as the Galois group. I just wanted to do this to illustrate that just because you have large degree does not mean that Galois group will be I mean, it is also a big group, it could, depending on the factorization of the polynomial, you can fall back into smaller essence. So, now let me do one more problem. So, before I stop this video, so I lost track. So, the second problem was computing Galois groups.

(Refer Slide Time: 30:04)



③ $f \in \mathbb{Q}[X]$ irr quartic which has exactly 2 real roots.
 Show that $\text{Gal}(f) = S_4$ or $\text{Gal}(f) = D_4$.
 Sol: $K = \text{sp fld of } f$; $\alpha \in \mathbb{R}$ is root of f ; $\mathbb{Q}(\alpha) \neq K$
 $\therefore K \not\subset \mathbb{R}$ (rule out)
 $[K:\mathbb{Q}] \geq 2$
 $\mathbb{R} \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$
 $\therefore [K:\mathbb{Q}] \geq 8$
 $\Rightarrow |\text{Gal}(f)| \geq 8 \Rightarrow G = S_4 \text{ or } D_4 \text{ or } A_4$
 A_4 is circled and labeled "rule out".

So, third problem still with quartics. So, let us say f is an irreducible quartic degree 4 in other words, which has exactly 2 roots, real roots. So, then I claim that, show that the Galois group of f is either S_4 or D_4 , it cannot be others in the list that we have. So, why is this? So, let us prove this.

So, the, let us say K is a splitting field of f , then what we have is and so let us say α is real root of f . So, then we have $\mathbb{Q}(\alpha)$ and \mathbb{Q} . So, this is of course, 4 because f is irreducible. So, this is 4 and $\mathbb{Q}(\alpha)$ is not equal to K , because K is not contained in \mathbb{R} , because it has exactly 2 real roots means the other 2 roots are complex and not real. So, K must not be contained in \mathbb{R} , but $\mathbb{Q}(\alpha)$ is contained in \mathbb{R} . So this cannot be 1, so it is at least 2.

That means $K:\mathbb{Q}$ is at least 8. That means the Galois group order is at least 8. So, now, in our list there are not too many, with order, at least 8 because other things are D_2 and C_4 , they are

order 2 and order 4. So, these are the only possibilities. Now, which of them, can it happen? So, the question is asking, it is either S_4 or D_4 , so we have to rule out A_4 ? How do we rule out A_4 ? We rule out A_4 by, remember A_4 happens when discriminant is a square. This happens when discriminant is not a square.

(Refer Slide Time: 32:20)

$R \supset \mathbb{Q}(\alpha_i)$
 $|4$
 \mathbb{Q}

$\therefore [K:\mathbb{Q}] \geq 8$
 $\Rightarrow |\text{Gal}(f)| \geq 8 \Rightarrow G = S_4 \text{ or } D_4 \text{ or } A_4$

claim: $\text{Disc}(f) < 0$.
pf: $\alpha_1, \alpha_2, Z, \bar{Z}$ are roots of f ; $\alpha_1, \alpha_2 \in \mathbb{R}, Z \notin \mathbb{R}$.
 $Z = a + ib, b \neq 0$
 $\bar{Z} = a - ib$
 $Z - \bar{Z} = 2ib$

$\text{Disc}(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2 = \underbrace{(\alpha_1 - \alpha_2)^2}_{>0} \underbrace{(\alpha_1 - a - ib)(\alpha_1 - a + ib)}_{>0} \underbrace{(\alpha_2 - a - ib)(\alpha_2 - a + ib)}_{>0} \underbrace{(2ib)^2}_{<0}$

$\text{Disc}(f) < 0$
 $\Rightarrow \text{Disc}(f)$ is not a square.
 $\Rightarrow \text{Gal}(f) \neq A_4$.
 $\Rightarrow \text{Gal}(f) = S_4 \text{ or } D_4$

So, now I claim that discriminant of f is negative, then it cannot be square. And this is an easy statement. So, let us say the roots are α_1 , α_2 , Z and \bar{Z} are roots of f with α_1 , α_2 in \mathbb{R} , and Z not in \mathbb{R} . So, then what is the discriminant, I will just go and directly compute the discriminant. I have an arbitrary quartic. So, I cannot use the formula that I wrote earlier. So, this is simply remember, discriminant is $\alpha_i - \alpha_j$ whole square for all i less than j . So, this is $\alpha_1 - \alpha_2$ square. So, I am just going to write all of them.

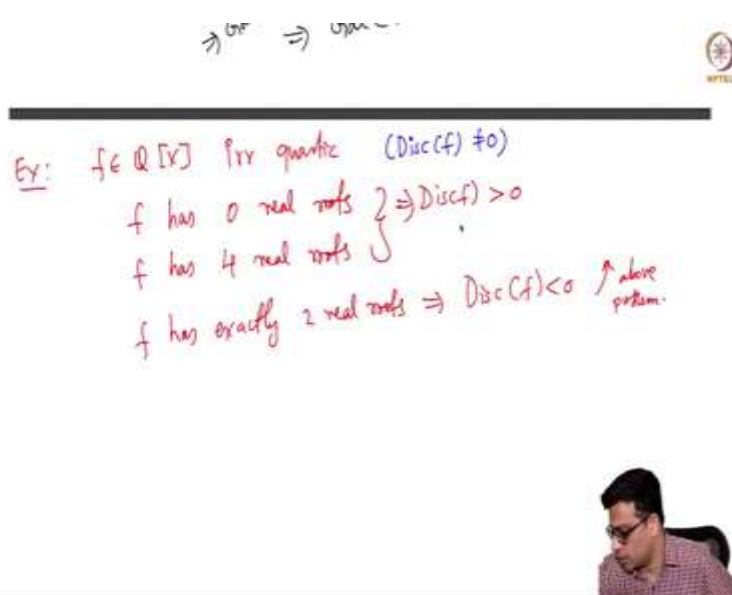
$\alpha_1 - a$ is i . So, Z is $a + ib$ let us say. So \bar{Z} is $a - ib$. So, of course b is nonzero. Because that is not in \mathbb{R} , so $Z - a - ib$ $\alpha_1 - a - ib$ will be $-ib$. And then I will write $Z - a - ib$, $\alpha_2 - a - ib$, $\alpha_2 - a + ib$. You see where this is going? And finally, is $Z - \bar{Z}$. What is that minus that bar? $a + ib - a + ib$. So, this is $2ib$, so $2ib$ whole square.

So, now let us look at individually what the sign of these things are. So, this is of course positive, they are all distinct roots. So, this is positive, and this is negative. That is because that is b , is positive b is nonzero. So, this is $-4b^2$ square. So, that is negative and together, this is α_1

minus a whole square plus b square. So, this is positive, this is positive. So, the discriminant is negative.

And hence the Galois group cannot be, so that means discriminant is not a square. So, this implies Galois group cannot be contained in the alternating group. So, this is ruled out. So, this implies and for order reasons, D_2 and D_2 of course is ruled out because discriminant is not a square but C_4 is ruled out for order reasons and as required it S_4 or D_4 . In fact, both of these occur.

(Refer Slide Time: 35:08)



Ex: $f \in \mathbb{Q}[X]$ irr quartic ($\text{Disc}(f) \neq 0$)

f has 0 real roots $\Rightarrow \text{Disc}(f) > 0$

f has 4 real roots

f has exactly 2 real roots $\Rightarrow \text{Disc}(f) < 0$ ↑ above problem.

And I will leave this as an exercise for you, I do not intend to do this, but a similar calculation will tell you that if f is a irreducible quartic, so exactly as before, so, I do not want to call it a new name. So, irreducible quartic, so this is exercise, f has 0 real roots. So, of course, it has 4 roots, if all of them are non real, then discriminant of f is positive, if f has 4 real roots also the discriminant is positive, and if f has exactly 2 real roots, exactly of course everywhere, then discriminant this we have done. So, this is the above problem.

So, in general, the discriminant will tell you what happens with respect to the discriminant of it, sorry, the number of non, number of non complex, non real roots will tell you the sign of the discriminant. Discriminate is of course are rational number. So, whether it is positive or not, and it is a nonzero number, because you are irreducible polynomials so distinct roots, so discriminant

is certainly nonzero. So, let me do 1 or 2 more problems before I end this class. So, just to settle these are problems that I touched upon in the videos, the earlier parts of the class.

(Refer Slide Time: 36:47)

④ Let $F \subseteq \mathbb{C}$, let $f \in F[x]$ be a poly of degree n . Then f is irr $\Leftrightarrow \text{Gal}(f)$ is a transitive subgrp of S_n .

Soln: \Rightarrow : $\alpha, \beta \in K$ roots of f ; f irr $\Rightarrow F(\alpha) \rightarrow F(\beta)$ F-iso $\alpha \mapsto \beta$ $\text{Gal}(f)$

Extend this to get $\sigma: K \rightarrow K$, $\sigma \in \text{Gal}(K/F)$ $\alpha \mapsto \beta$.

$\text{Gal}(f)$ is transitive



So, let f be as always I will stick to the complex subfields of complex numbers, let f be a polynomial of degree n . Then the problem is asking you to show f is irreducible, if and only if Galois group of f is a transitive subgroup of S_n . We certainly know that Galois group is a subgroup of S_n , but it is a transitive subgroup if and only if f is irreducible.

So, this I needed this statement in the proofs of solvability of radical polynomials, but I wanted to record this explicitly, so that you have this in your notes. So, I do not want to spend too much time proving this because we have essentially proved this. If f , if α and β are two roots of f , K of course is a splitting field, then f irreducible implies there is a function from $F(\alpha)$ to $F(\beta)$, f automorphism, f isomorphism sending α to β .

Extend this to get σ from K to K , σ in Galois group of K/F , which is of course, the Galois group of f sending α to β . So, G is transitive. So, for any two roots, there is a Galois group element which sends one to the other, so it is transitive.

(Refer Slide Time: 38:41)

$G \text{ act}(f)$ is transitive
 \Leftarrow : f is reducible $\Rightarrow f = gh$, $\deg g > 0$, $\deg h > 0$.
Now any elt $\sigma \in G$ must permute roots of g
b permute roots of h separately.
Using this factorization, conclude that G is not transitive.
Last part: exercise)



Suppose, f is not irreducible or in other words f is reducible, then f can be written as g times h where degree g is positive and degree h is positive. But now, any element σ of G must permute roots of g and permute roots of h separately. What I mean is any root of g has irreducible polynomial which is a divisor of g . So, and that cannot be a root of h , we can assume that g and h are co prime. So, what I want to say is that there must be a root of g that is not a root of h , there must be a root of h that is not a root of g . So, no element of, no element σ of G can map a root of g to a root of h .

So, there is a little bit more work involved here, so I will simply say that, so using this decomposition, this is a true statement, using this factorization, conclude that G is not transitive. So, there is a root that you cannot permute. So, the point is it must be a transitive subgroup of S_n , n is important, where n is the degree, it cannot be transitive, it can be a subgroup of, transitive subgroup of smaller symmetric group S_{n-1} and f can fail to be irreducible. But if it is a transitive subgroup of S_n , there must be a root of h that cannot be mapped to a root of g . So, this last part is the exercise. Again, I am not doing everything possible, so that I am covering as many exercise as possible. So, let us do just one more problem before we end this class.

(Refer Slide Time: 41:12)

⑤ Let $f \in F[X]$ be irr. If one root of f is solvable over F (FSC) then f is solvable (i.e., all roots of f are solvable).

pf: $\alpha \in C$ is a solvable root of f .

$F \subseteq F_1 \subseteq \dots \subseteq F_r \xrightarrow[\text{done earlier}]{\text{Theorem}} F \subseteq F_r \subseteq L$

$\underbrace{F \subseteq F_1 \subseteq \dots \subseteq F_r}_{\text{radical}} \xrightarrow{\text{Theorem}} \underbrace{F \subseteq F_r \subseteq L}_{\text{radical + Galois}}$

L/F Galois $\Rightarrow L/F$ is normal

f is irr & has a root α in $L \Rightarrow f$ splits completely in L .

\Rightarrow All roots of f are solvable.



This is also we have done before. Now, let us take f to be an irreducible polynomial, as always capital F is a subfield of C . Then, if a root of, if one root of f is solvable, then all roots of f is solvable, then f itself is solvable, solvable over f of course, then f is solvable that means all roots of f are solvable. And the proof is fairly clear.

So, suppose α in C is a solvable root of f . So, you have a tower starting with F and ending with a field, this is simply radical, simply radical, simply radical and α is here. But now using a theorem that we proved about extending the radical extension to a Galois extension, given a radical extension you can enlarge the field to get a Galois extension which is radical. So, you can extend to some K or L , such that this is radical plus Galois.

But now, L over F is Galois implies L over F is normal and f is irreducible and has a root, so α is of course in F_r , so α is in L , has a root α in L , so f splits in, splits completely in L . So, that means all roots of f are solvable. Because all roots of L is in a radical extension. So, every root is solvable, hence f itself is solvable.

So, let me end this class now, we have done several problems on computing Galois groups and some observations that we have made during lectures I wanted to formally record them here. So, let me stop now, I will continue with more problems in the next class. Thank you.