

Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 46
Problem Session – Part 10

(Refer Slide Time: 0:17)

Theorem: $F \subseteq \mathbb{C}$, $f \in F[X]$ $\deg f = 5$. Suppose the Galois group of f is S_5 or A_5 .
 Then f is not solvable. f must be irreducible

Pf: Let $G = \text{Gal}(f)$. First suppose $G = S_5$.
 $K = \text{Sp. fld of } f \text{ over } F$ Let $D = \text{Disc}(f)$
 $G = \text{Gal}(K/F) = \text{Gal}(f)$ $\delta = \sqrt{D} \in K$.

$K \mid A_5$
 $F(\delta) \mid K$
 $F \mid F(\delta)$

Since $\text{Gal}(K) \not\subseteq A_5$, $\delta \notin F \Rightarrow [F(\delta):F] = 2$.
 $\therefore \text{Gal}(K/F(\delta)) = A_5 \Rightarrow$ Galois group of f over $F(\delta)$ is A_5 .
 $\therefore \text{Gal}(K/F(\delta)) = A_5 \Rightarrow$ Galois group of f over $F(\delta)$ is A_5 .
 P. will follow $\Rightarrow f$ is not solvable over $F(\delta)$.
 $\therefore f$ is not solvable over F .

Welcome back, last time we proved this theorem, which says that if you have a quintic polynomial over a subfield of complex numbers; whose Galois group is either S_5 or A_5 , then it is not solvable. So, it gives us a way to construct a non-solvable quintic polynomial. We need to now go ahead and construct a polynomial whose Galois group is S_5 or A_5 . So, this previous class completed the course really; we have covered everything that we wanted to do. Remember in the beginning I said goal is to prove Galois theorem about solvability of polynomials with rational coefficients. We have done that, so I have some loose ends to take care off and also give some exercises.

(Refer Slide Time: 01:13)

Hence f is NOT solvable over F □


Problem Session

1) Let p be a prime number, $p \geq 5$. Suppose $f \in \mathbb{Q}[x]$ is an irr poly of deg p , s.t. f has exactly 2 non-real roots. Then $\text{Gal}(f) \cong S_p$. p=5 gives us a non-solvable quintic.

Soln: $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_p \in K$ be roots of f in a S_p fld K of \mathbb{Q} .
 Let $\alpha_1, \alpha_2 \notin \mathbb{R}$; $\alpha_3, \dots, \alpha_p \in \mathbb{R}$. Let $G = \text{Gal}(K/\mathbb{Q}) = \text{Gal}(f)$.

First claim: $(12) \in G$: $\sigma: K \rightarrow K$ complex conjugation.
 $\sigma(a+ib) = a-ib$. $\alpha_2 = \overline{\alpha_1}$

2nd claim: σ is in G . σ is an auto of K , so $\sigma \in \text{Gal}(K/\mathbb{Q}) = G$. 2



So, the remaining few videos in the course will be exercises, and in this exercise session we will; we will prove some results that we have used earlier in the course without proof. And I also will give you several examples on how to compute Galois groups, and solve some interesting problems on Galois groups. So, am going to go ahead and start this and one by one will do; and will see how much we can do. In the first problem we will take care of the pending issue, which is construction of a polynomial with rational coefficient, whose Galois group is S_5 . So, we are going to do a slightly more general problem as follows.

So, let P be a prime number, and let us assume P is at least 5. Suppose f is an irreducible polynomial of degree 5, of degree P , such that f has exactly 2 non-real roots. So, it has P roots of course because it is irreducible polynomial of degree P ; it will have distinct roots and complex numbers. I am assuming that it has exactly 2 non-real roots; other P minus 2 are inside \mathbb{R} . Then, Galois group of f is S_p , so Galois group of over \mathbb{Q} of course. Every time you take a polynomial in a particular field, the Galois group when I refer to the Galois group and that polynomial; I mean the Galois group over that field.

So, remember if you take P equal to 5 gives us a non-solvable quintic. So, we have to construct a polynomial, which exactly has 2 real roots will do that; so let us prove this. This proof is quite simple and it is instructive; so let us call the roots $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_P$ be roots of we can take K, f in a splitting field K of f over \mathbb{Q} ; the usual sentence. So, we have this

splitting field of that polynomial; it will have P roots. Take, call then α_1 through α_P , and let say α_1, α_2 are not in \mathbb{C} are not in \mathbb{R} ; so α_3 and up to α_P are all in \mathbb{R} .

We know that exactly 2 are not real numbers; so we have this. First I claim that so let G be the Galois group of the splitting field, which of course what we call the Galois group of the polynomial. First I claim that the permutation 12 the 2-cycle 12 is in G ; why is this? Consider the map from K to K given by complex conjugation. So, here any $a + ib$ will go to a minus ib .

(Refer Slide Time: 05:00)

First claim: $(12) \in G$: $\sigma: a+ib \mapsto a-ib$. $(\alpha_2 = \alpha_1)$

Facts: σ is an auto of K ; so $\sigma \in \text{Gal}(K/\mathbb{Q}) = G$. } easy exercise.
 $\sigma(\alpha_1) = \alpha_2, \sigma(\alpha_2) = \alpha_1$ & $\sigma(\alpha_i) = \alpha_i \forall i=3, \dots, P$.
 So $\sigma = (12) \in G$. $\therefore (12) \in G$ So G contains a 2-cycle.



So, some in general facts which one can show facts σ is an automorphism of K , and which fixes \mathbb{Q} ; any automorphism of an extension of \mathbb{Q} fixes \mathbb{Q} . So, it is an element of the Galois group and also σ of α_1 is α_2 , σ of α_2 is α_1 ; and σ of α_i equals to α_i , for all i from 3 to P . Here, these are some general facts; because we know that roots of a rational polynomial, complex roots of a rational polynomial appearing conjugate pairs, non-real complex roots. So, α_1 and α_2 are basically conjugates of each other. Everything is a conjugate I mean if α_3 is also conjugate of itself.

But, that is because conjugates of α_3 is in α_3 itself, because they are real numbers. But, otherwise the non-real ones are appearing in conjugate pairs; so this is an easy exercise. I am going to in order to do as well any problems as I can; I am going to skip some facts which are either group theoretic; or some general facts that come from earlier parts of algebra. So, that I

can focus on the Galois Theory part; so this is one such. So, we assume we assume these facts; so sigma is in fact.

So, sigma is in fact permutation 12, because it sends 1 to 2, 2 to 1; and it fixes all other, so 1 2 belongs to G. So, sigma is in G, so this is empty. G contains 2-cycles, so G contains 2-cycles transposition of 2-cycle. Now, I am going to argue that it also contains P-cycle; so we have because f is irreducible. The action on the G of the roots is transitive; so there is an order of orbit of order P size P.

(Refer Slide Time: 07:26)

Handwritten notes on a slide:

- Diagram showing field extensions: $K \supset \mathbb{Q}(\alpha_1) \supset \mathbb{Q}$ with f irreducible over \mathbb{Q} .
- Equation: $p \mid [K:\mathbb{Q}] = |G|$.
- Cauchy's theorem: $\Rightarrow G$ contains an elt of order p .
- Group-theoretic fact: $\xrightarrow{p \text{ prime}} G$ contains a p -cycle.
- Order of a product of disjoint cycles $\sigma_1, \dots, \sigma_n$ is $\text{LCM}(\text{ord}(\sigma_1), \text{ord}(\sigma_2), \dots, \text{ord}(\sigma_n))$.
- Example: ex- with a bracket pointing to the LCM formula.

So, P divides it or more directly we have K contained in Q of alpha1 contained in Q; and this is a degree extension because f is irreducible. That is because the irreducible polynomial of alpha1 is f; so this is a degree P extension. Hence, P divides K colon Q, which is of course the order of G. But, by Cauchy's theorem, G contains an element of order P; this so far we have not used the fact that P is prime, but now we are going to use. So, P prime implies G contains a P-cycle. This is only true for prime P; in general if you have an order 4 element; it does not mean it is a 4-cycle. However, for P prime it must mean.

This requires some group theoretic facts. So, I will just, order of a product of disjoint cycles is equal to LCM of order of each of those individual. So, now in order for a element to have a order P; that element can be written as a product of disjoint cycles. And those orders will have LCM P; but they are all because P is prime. This implies this and as I said I am going to leave certain

group-theoretic statements as exercises for you. So, any element of order prime must be a P-cycle; it cannot be written as a product of cycles of different sizes. In general you can do that, but not if P is prime. So, G contains a P-cycle and G contains a 2-cycle.

(Refer Slide Time: 09:42)

General fact: $G \subseteq S_n$ contains a 2-cycle & an n -cycle $\Rightarrow G = S_n$.

Proof: $\sigma = (12) \in G$, $(12 \dots n) = \tau \in G$. Then $\tau \sigma \tau^{-1} = (23) \in G$.
 $\tau (23) \tau^{-1} = (34) \in G$. Similarly, we conclude $(i, i+1) \in G \forall i$.
 $(1, i) = (i, i-1)(i-1, i)(i, i-1) \in G \Rightarrow (1, i) \in G \forall i$.
 $(1, i)(1, j)(1, i) = (i, j) \in G \Rightarrow G$ contains all 2-cycles $\Rightarrow G = S_n$.

So, now again a general fact, which I will in fact prove because this is an important fact. So, if G is in S_n and contains, here n is any number; a 2-cycle and an n-cycle, then G is S_n . So, any subgroup that contains a 2-cycle and an n-cycle is all of S_n . So, the fact is proof of this, we can assume 12 is in G; let us call that sigma. Of course, the way that is just a matter of rearranging the indices; but we can also assume that this is the n-cycle. Because you take n-cycle and you take some sufficiently powers of them one by one; eventually you will get this, because n-cycle is P cycles group and they are all powers of each other.

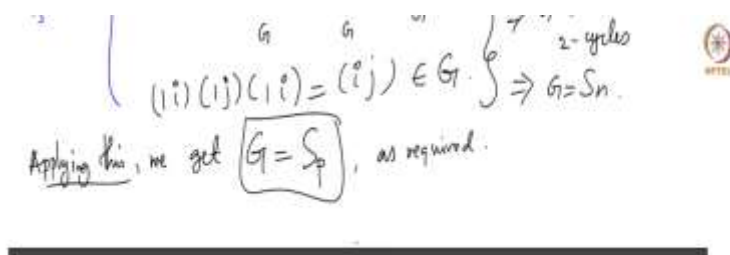
So, any n-cycle you have you can take some power, and you can get this particular n-cycle; let us called this tau. So, then it is an easy computation tau sigma tau inverse is actually 23; this is because you can work this out, I mean this is a trivial exercise. So, write down tau inverse, then apply sigma, then apply tau; you get this. So, now that means this is in G, because tau and sigma are in G. Any product of things in G is in G; so that is in G. But, if you do tau times 23 times tau inverse; that is actually 34 that is in G; so is also an exercise. So, I am not doing the explicit computation here, because that is easy and you can do this.

So, similarly we can conclude that $i, i+1$ is in G for all i ; so we have 12 by hypothesis, 23 I have exhibited 34. And then you do $\tau_{34} \tau_{34}^{-1}$, you get 45 and so on. But, once you have these you can now compute $1, i$ is actually equal to $1, i-1, i-1, i, 1, i-1$. So, this is in G by induction; this is in G by this construction; this is in G by induction, so this whole thing is in G . So, that means, I am going over this very fast, but $1, i$ is in G , for all i .

Now, it is well known that they generate S_n in particular because you know that $1, i$ times $1, j$, times $1, i$ is actually i, j . So, 1 goes to i , i goes to 1 ; so 1 goes to 1 goes to i , i goes to 1 , so 1 is fixed; i goes to j , j goes to 1 , 1 goes to i ; so j goes to i and similarly i goes to j . So, that means all this very quickly what I said is G contains all 2-cycles. But then it is well known that every permutation in S_n is a product of 2-cycles.

So, this is a standard group theory fact, but I sort of try to give you a quick proof of this. So, I hope I did not confused you, you can just note down all the equalities I wrote here; and check them one by one, it is a trivial check. So, a group contains S_n subgroup of S_n contains a 2-cycle and n -cycle; it is S_n . So, now our Galois group here contains 12 and a P -cycle.

(Refer Slide Time: 13:50)



Handwritten mathematical proof showing that a group G containing a 2-cycle and an n -cycle must be the symmetric group S_n . The proof uses the identity $(1 i)(i j)(1 i) = (i j)$ and concludes that $G = S_n$.

$$(1 i)(i j)(1 i) = (i j) \in G \Rightarrow G = S_n$$

Applying this, we get $G = S_n$, as required.



So, applying this to our situation this is as required; so the problem ask you to show that if you an irreducible polynomial of degree P , which has exactly 2 non-real roots; the conceptual part of it is very simple. The complex conjugate permutes the non-real roots fixes all the real roots; so that

is a 2-cycle. And because you have an irreducible polynomial, you have a order P element; because P is prime, it must be a P -cycle. And a general fact about symmetric groups is that any 2-cycle comma any P -cycle together will generate all of S_n , so G is S_P . This now settles the question of polynomials having its Galois group is S_P . Now, we have 2 still construct a polynomial with exactly 2 now real roots.

(Refer Slide Time: 14:51)

Examples of irr poly $\in \mathbb{R}[X]$ with exactly 2 real roots.

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" $f(x) := g(x) + 2$
 $= X^5 - 4X + 2$
 $\text{is irr by Eisenstein}$

We conclude: f has exactly
 $\begin{cases} 3 \text{ real roots} \\ 2 \text{ non-real roots} \end{cases}$

check this carefully

Hence $\text{Gal}(f) = S_5$ & f is not solvable ✓

This is the main result of Galois theory

2) $f = X^5 - 16X + 2 = X(X^4 - 16) + 2 = X(X^2 - 4)(X^2 + 4) + 2$

is irr by Eisenstein $\text{Gal}(f) = S_5$ ✓

has exactly 3 real roots & 2 non-real roots
 \Rightarrow So does f .

Examples of polynomials of irreducible polynomials with exactly 2 real roots. So, I am want to give you a couple of them to completely settle the issue. So, what we do here is, so this is let me just go and quickly tell you this. So, the point is we need for degree 5 first; because the

ultimately the whole point of the course is produce a quintic which is not solvable. So, what I wanted is exactly 3 real roots; so let us take the polynomial $X^5 - 4X$, let us take this polynomial. This is not reducible, but what kind of polynomial is this we have X times $X^4 - 4$.

So, this is actually let me take here, so this is X times $X^4 - 4$, $X^4 - 4$. So, this degree 5 polynomial has exactly 3 real roots. So, then g has exactly 3 real roots, exactly 3 real roots, and 2 non-real roots. So, the 3 real roots are 0 square root of 2, minus square root of 2 and. So, the non-real roots are $\sqrt{2}i$ minus $\sqrt{2}i$; so these are not in \mathbb{R} , these are in \mathbb{C} . Now, this is a good polynomial for us, except that it is not irreducible. So, if you look at its graph, it looks something like this. So, the it goes through 0, so this is 0, this is square root 2, this is minus square root 2, this is the graph of G_g .


But now what I do is shift this up by let say 2. So, let us $f(x)$ equals $g(x) + 2$; so this is $x^5 - 4x + 2$, and this is irreducible by Eisenstein style. So, I have chosen 2 so that you get an irreducible polynomial. What is the graph of this? I claimed that its graph is shifting this up by 2. So, graph of, so this is the graph of; so you can also use some calculus to intermediate value theorem and mean value theorem, to give a concrete proof, but it does not matter. So, it is clear that when you shift this; it will continue to have 2 real roots 3 real roots.

So, we conclude f has exactly 3 real, 2 non-real roots. So, this is a function polynomial irreducible; it has 3 real roots and 2 non-real roots. So, one has to do a little bit more work, check this carefully; so I will leave that part to you. Because that is just you compute; for example that it it will be negative here, positive here. So, it will at least cross x axis 3 times; it cannot cross more than 3 times, because g does not. So, hence Galois group of f is S_5 and f is not solvable; so this is good. So this means that you have a polynomial of degree 5 which cannot be solve by radicals; so this is the main result of Galois theory in some sense.

So, Galois gave an explicit construction of polynomials, which cannot be solved by radicals. So, I will give you one more example which is along the same lines; but I thought it would be good to have 1 more example. So, this is irreducible by Eisenstein and this can be written as x times $X^4 - 4x + 2$. So, this is X times $X^4 - 4$, $X^4 - 4$ plus 2. So, this is X times $X^4 - 4$, $X^4 - 4$ plus 2;

so, this has exactly 3 real 0 to minus 2 non-real roots and hence so does f . So, again it is irreducible it has 3 exactly 3 real roots Galois f is S_5 ; so this proves that this is also not solvable.

(Refer Slide Time: 21:06)

3) For any $n \geq 5$, let $f(x) = X^{n-5}(X^5 - 16x + 2)$. \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 $f = (x^2 + 4)(x-2)(x-4) \cdots (x-2(p-2)) + 2$


$\in \mathbb{Q}[X]$

$\deg f = p$

claim: f is irr $\checkmark \rightarrow$ Pf uses Eisenstein criterion.

$f = X^p + 2(a_1 X^{p-1} + \cdots + a_{p-1} X)$

$= (4(2)(4) \cdots (2(p-2))) + 2$



claim: f has exactly $p-2$ real roots.

Reasoning is same as above:

$f = g + 2$; g has roots $\pm \sqrt{-4}, 2, 4, \dots, 2(p-2)$

$\pm \sqrt{-4}$ not real, $2, 4, \dots, 2(p-2)$ real


is even, but not divisible by 4

$-4(2)(4) \cdots (2(p-2)) + 2$

divisible by 4

Hence $\text{Gal}(f) = S_p$.

In particular, we constructed a Galois ext K/\mathbb{Q} s.t. $\text{Gal}(K/\mathbb{Q}) \cong S_p$ for any prime $p \geq 5$.



You can construct now any for any n ; let f be X power n minus 5, times X power 5 minus 16x plus 2. So, then Galois group of f , of course f is not irreducible; but however we know that Galois group of f is S_5 . Because this already has roots, so splitting field of f is the splitting field of this, which is S_5 ; so, this implies f is not solvable. Every time you have the Galois group S_5 or A_5 , it is not solvable. So, hence for every n we have a polynomial of degree n which is not

solvable. We do not have irreducible polynomial that requires a significantly more work. But, for prime numbers we can construct that.

So, let P greater than equal to 5 be a prime number. Let f be X power let say X square plus 4 times X minus 2, X minus 4, x minus 2 times P minus 2 plus 2; so this is in $\mathbb{Q}[X]$. Degree of f is P because this these are P minus 2 terms here, there is a square term here; so degree is P . So, I claim that f is irreducible, so the proof simply uses Eisenstein criteria. Because if you now expand out f can be written as X power P plus these; these are all even numbers 4, 2, 4 2 times P minus 2. So, every term that you have in the middle of this polynomial, all intermediate terms like this or even.

So, you can factor out it too, because for example what is X power P minus 1 term? So you have to take degree 2 and all but one of these. So, you have to take P of P minus 3 of this; so and the last one you have to take the coefficient. So, that is even so that will be even times X power P minus 1. So, and then what is the constant term? Constant term is 4 times; so you will have actually here. So, 1 2 up to P minus 2 terms; so you have to take these minus 2 minus 4, minus 2 times P minus 2. P is odd, so P minus 2 is odd. So, there will be a minus sign here; and then you will have. So, I will write the constant term minus 4 times 2 times 4 times 2 times P minus 2 plus 2.

But, this is divisible by 4 obviously; so the constant term is even but not divisible by 2, by 4. Because 4 divides this term and 4 does not divide this. So, constant term is even but not divisible by 2; so you can apply Eisenstein time to conclude that f is irreducible, so far so good. And now I claim that f has exactly P minus 2 real roots; and this is the reasoning is same as above. What is the reasoning? Reasoning is you look at g which is X power P ; so f is g plus 2. So, I am taking this to be g ; so I am taking this to be g , then g has roots plus or minus square roots of minus 4, and 2, 4 up to 2 times P minus 2. So, this is not real, these are real.

So, and then you shift up by 2; so that means f will also have exactly 2 non-real roots, and P minus 2 real roots. So, f has exactly f is irreducible has exactly P minus 2 real roots and hence. So, in particular so I want to highlight this because we will get back to this later. In particular, we construct a Galois extension K over \mathbb{Q} , such that Galois K over \mathbb{Q} is isomorphic to S_p , for any prime; for any prime P at least 5. So, I want to comeback to this statement later, because the

question is given any group can you construct such a Galois extension. That is an open problem, very famous open problem.

But, so what we have really done here is that we can do S_5 . This example will not give you S_n , because this is not irreducible polynomial; it will only gives us S_5 . So, this settles the question of exhibiting polynomials, which are now solvable by radicals. Now, what I want to do is do some examples of computing Galois groups. So, this might be a good time to stop; so let me stop this class here. In next class we will continue with the more exercises. Thank you.