


**Introduction to Galois Theory**  
**Professor. Krishna Hanumanthu**  
**Department of Mathematics**  
**Chennai Mathematical Institute**  
**Lecture No. 40**

**Discriminants, Galois groups of polynomials**


(Refer Slide Time: 0:16)

54



Theorem: Let  $F \subseteq \mathbb{C}$ ; let  $\alpha \in \mathbb{C}$  be algebraic over  $F$ . TFAE.

- (1)  $\alpha$  is Solvable over  $F$ , i.e.,  $\exists$  a tower  $F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_r$  st  $F_i/F_{i-1}$  is simple radical  $\forall i$  and  $\alpha \in F_r$ .
- (2) There exists a tower of fields:  $F = L_0 \subseteq L_1 \subseteq \dots \subseteq L_n$  st  $\alpha \in L_n$  and each  $L_i/L_{i-1}$  is abelian (i.e., Galois + Galois gp is abelian).
- (3) There exists a tower of fields:  $F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$  st  $\alpha \in K_m$  and each  $K_i/K_{i-1}$  is cyclic (i.e., Galois + Galois gp is cyclic).



Welcome back. In the last class, we proved this theorem, in the last couple of classes, which your characterises when a given complex number is solvable over a given field. So, there are 3 equivalent conditions that I wrote and in fact, I forgot the fourth one, which I am write now.

(Refer Slide Time: 00:48)


each  $K_i/K_{i-1}$  is cyclic

(3) There exists a tower of fields:  $F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$  st  $\alpha \in K_m$  and each  $K_i/K_{i-1}$  is cyclic (i.e., Galois + Galois gp is cyclic).

(4) There exists a tower of fields:  $F = M_0 \subseteq M_1 \subseteq \dots \subseteq M_s$  st  $\alpha \in M_s$  and each  $M_i/M_{i-1}$  is cyclic of prime order (i.e., Galois + Galois gp is cyclic +  $[M_i, M_{i-1}]$  is prime).

Ex: (3)  $\Rightarrow$  (4):  $F \subseteq K$  extn  $\Rightarrow F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = K$   
 $\begin{matrix} \text{cyclic} & \text{prime} & \text{prime} & \text{prime} \\ \text{order} & \text{order} & \text{order} & \text{order} \end{matrix}$

Pf: (1)  $\Rightarrow$  (2): Let  $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_r$ ,  $\alpha \in F_r$ .  
 $\dots F_i = F_{i-1}(\alpha_i)$  with  $\alpha_i \in F_{i-1}$  (meaning of  $F_i/F_{i-1}$  being simple radical)



Because this will also be useful for us as we go forward and this is a very trivial modification from the third one. So, there exist a tower of fields, just like in the previous 3, previous 3 cases. So, let me call this  $M_0, M_1, \dots, M_s$  such that  $\alpha$  is in  $M_s$  of course and  $\alpha$  is in the last one. Each  $M_i$ ,  $M_i$  mod  $M_{i-1}$  is not only cyclic but it is cyclic of prime order, is a cyclic meaning it is Galois. So, Galois plus Galois group is cyclic and moreover plus the index is a prime number. Of course, it is cyclic is now irrelevant here because if it is a prime model it is obviously going to be cyclic but and the prove actually it only proves 1, 2, 3 are equivalent. So, I leave this as an exercise for you for now to show for example that 3 implies 4. There is an easy exercise.

So, basically all you need to do is if  $F$  this is a cyclic extension implies there is a tower, each is cyclic where each is prime order. This is easy but I wanted to record it in the theorem itself so that we can just appeal to this theorem later. So obviously 4 implies 3 is trivial because if there is a tower where each extension is cyclic or prime order, it is of course cyclic but 3 implies 4 you can do by first taking a cyclic extension. Take any, take a subgroup of prime index, you know that such a thing exists because if  $P$  divides the order of the group there exists a subgroup of index  $P$ . That means order of  $H$  is order of  $G$  divided by  $P$ . Then you take the fixed field of that. That would be here.

This is order  $P$  because that is the index and then this index is less than  $K$  colon  $F$  and you proceed by induction. So, this is just a hint. So, any cyclic extension can be expanded by putting more fields in the middle and ensure that each extensions of prime order. So, I just do not want to say anything more but the conclusion of the theorem is that it is enough to consider tower of cyclic extensions of prime model and 2, 3, 4 are all Galois theoretical statement. So, first one is solubility of a radical statement. Now, let us proceed our goal in the rest of the course is to prove.

(Refer Slide Time: 04:08)

$\therefore \alpha$  is Solvable over  $K_0 = F$


---

Goal for the rest of the course:  $F \subseteq \mathbb{C}$  a field;  $f \in F[X]$   
 $n = \deg f$

I  $n \leq 4$ :  $f$  is solvable over  $F$  (i.e., all roots of  $f$  are Solvable over  $F$ )

II  $n \geq 5$ : in general,  $f$  is Not Solvable.  
There do exist polynomials of any degree that are Solvable.  
(eg:  $X^n - 1$  is solvable  $\forall n$ )

---




I  $n \leq 4$ :  $f$  is solvable over  $F$  (i.e., all roots of  $f$  are Solvable over  $F$ )

II  $n \geq 5$ : in general,  $f$  is Not Solvable over  $F$ .  
There do exist polynomials of any degree that are Solvable.  
(eg:  $X^n - 1$  is solvable  $\forall n$ )

We give two different proofs of I and II:

---



So, what is our goal? So, our goal now for the rest of the course is as follows. So, I am going to fix this notation once and for all. So,  $F$  is a subfield of  $\mathbb{C}$ . So, I am going to stick to characteristic 0 and in fact, I am going to stick to subfields of  $\mathbb{C}$  and we take polynomials in 1 variable over this field  $F$ . So, we will first show that  $n$  equal to 4, then  $f$  is solvable. So, let me write that here. So,  $f$  is a polynomial and  $n$  is the degree of  $f$ . So what is the meaning of solvability? It means all roots of  $f$  so solvable maybe I should write capital  $f$ . So, this means all roots of capital  $f$  are solvable, all routes of small  $f$  are solvable over capital  $F$ .

So, if the degree of the polynomial is less than equal to 4, all roots are solvable and if  $n$  is greater than equal to 4 in general,  $f$  is not solvable. So, these are the 2 theorems that we wanted to after the world in general is important here. So, let me remark here that there do exist polynomials of any degree that are solvable. I am not saying that every polynomial of degree 5 is not solvable. I am only saying that there do exist.

So, for example, if you take the polynomial  $X^n - 1$  by the very nature of the roots, these are all  $n$ th roots of unity. This is solvable for all  $n$ , so you can always construct polynomials which are solvable but for  $n$  at least 5, there do exist polynomials which are not solvable and however for  $n$  equal to 1, 2, 3, 4 all polynomials are solvable. So, we are going to give essentially 2 different proofs of this of both of these statements. So, one theorem is, one way is to sort of explicitly understand this polynomials. The second way is to understand it in terms of solvable groups and state the theorem that Galois in fact proved which is a beautiful theorem, which says that a polynomial is solvable if and only if its Galois group is solvable. So, that I will do separately.

(Refer Slide Time: 7:13)

Theorem: Let  $F \subseteq \mathbb{C}$  and let  $f \in F[x]$  be a polynomial of degree  $\leq 4$ .  
 Then  $f$  is solvable over  $F$ .  
Pf: deg  $f=1$ :  $f = X - a$ ,  $a \in F$ . So  $f$  is solvable over  $F$ .  
deg  $f=2$ :  $f = X^2 + bX + c$  quadratic formula does the job.  
 $F(\sqrt{b^2 - 4c}) \ni \frac{-b \pm \sqrt{b^2 - 4c}}{2}$  roots.



$$\begin{aligned}
 \deg f = 2: & \quad K := F(\sqrt{b^2 - 4c}) \ni \frac{-b \pm \sqrt{b^2 - 4c}}{2} \text{ roots} \\
 \left\{ \begin{array}{l} K = F \quad \text{if } \sqrt{b^2 - 4c} \in F \\ [K:F] = 2 \quad \text{if } \sqrt{b^2 - 4c} \notin F \end{array} \right. & \quad \text{Any deg 2 extn is radical. (or } K/F \text{ is cyclic)}
 \end{aligned}$$

deg f = 3:



So, let me first, today our goal is to do the following theorem. If I do not finish it today, I will finish it next class. So, the next 2 classes, the goal is to prove the following theorem. So, let  $F$  be a subfield of  $\mathbb{C}$  and let  $f$  be a polynomial of degree less than or equal to 4. So, then I want to show then  $f$  is solvable. So, let me just do some easy cases first before I develop some theory that will be useful for us later.

So, first degree  $f$  equal to 1, then  $f$  is of the form, some  $x$  minus  $a$ , we can always multiply by a scalar with of course  $a$  in  $F$ . So,  $f$  is obviously solvable. So, I keep forgetting this, solvable over  $F$ . The triviality. Degree  $f$  is 2, then  $f$  is some  $x$  square plus  $bx$  plus  $c$  and this of course, if  $f$  is irreducible, you have to construct a bigger field which where it splits, but otherwise the roots are in  $F$  itself, but either case, quadratic formula I will simply write it like this, quadratic formula does the job because the roots are of course, they are contained in a field like this.

So, this is a degree 2 extension, at most would degree 2 extension. It could be degree one extension if the discriminant is already a square. So, I want to highlight that here. This is  $F$  if is in  $F$  or so let us say  $K$  is this which is a splitting field so  $K$  equal to  $F$  if this, otherwise it is a degree 2 extension and in either case, the roots live in a radical extension because any degree 2 extension is, any degree 2 extension is radical. We do not even need to do that. We can also use the theorem that we proved in the last class, which I recalled at the beginning of today's class; we do have a cyclic extension which contains the fields, which contains the root.

So, either way it is, another way of arguing this is this is cyclic. That means roots are solvable and hence  $F$  is. Degree  $F$  equal to 3, I want to spend some time, but I first want to claim that I have already done this. We already showed so let me set it up properly.

(Refer Slide Time: 10:36)

$K = F(\sqrt[3]{a}) \cong \frac{-b \pm \sqrt{b^2 - 4ac}}{2}$

$\begin{cases} K = F & \text{if } \sqrt[3]{a} \in F \\ [K:F] = 2 & \text{if } \sqrt[3]{a} \notin F \end{cases}$

Any deg 2 extn is radical. (or  $K/F$  is cyclic)

$\deg f = 3$ :  $K = \text{sp. fld. of } f \text{ over } F$ .  $[K:F]$  divides  $6 = 3!$

$K = F$ : Solvable ✓ $[K:F] = 2$ : Solvable ✓	$[K:F] = 3$ : $K/F$ is cyclic and hence $K/F$ is solvable. $\Rightarrow f$ is solvable ✓ $F \subseteq K$ cyclic
--	---

$[K:F] = 6$ : we already showed that  $K/F$  is solvable.

So, let us say  $K$  is a splitting field of  $f$  over  $F$ . So, now we have a bunch of possibilities. So, in this case solvable. This is solvable because this can happen, for example, if your cubic polynomial is reducible and it acts as a reducible quadratic and a linear polynomial. This can very well happen. So, in that case it is solvable. Remember that the splitting field degree divides 6, which is 3 factorial. So it is 1, 2, 3 or 6. So, in this case  $K$  over  $F$  is cyclic. I mean in fact in both cases 2 and 3 it is cyclic and hence  $K$  over  $F$  is solvable because every alpha in  $K$  is in a cyclic extension.

So, if you go back to the theorem that I recall at the beginning of today, then apply the third or second or fourth, all of these will work. So, there is a tower where each extension is abelian or cyclic or cyclical or primordial. All these 3 conditions are satisfied. So, everything in the end of field is solvable. Here, there is only one single extension. The tower consists of a single extension and this is abelian or cyclic or cyclical or in fact primordial. This is solvable. So, every root is solvable and finally the last option is in this case, we already showed as part of an exercise.

(Refer Slide Time: 12:52)



So, I this is degree 2 and this is degree 3. So I if you remember we proved this exercise. Any Galois extension of degree 6 is solvable because you can take a subgroup of order 3 look at its fixed field because that's a group has index 2 it is normal. So, this extension is Galois. So, degree 2 Galois means it is cyclic and this is degree 3, of course, so it is also Galois. So, there is also fine. However, I want to do a little more analysis of degree 3. So, now I will pause the proof and do some generalities. Pause the proof here for some general statements. I will come back to the proof in a few minutes but let me make some general remarks.

(Refer Slide Time: 13:43)

General remarks:  $F \subseteq \mathbb{C}$ ,  $f \in F[x]$ ,  $\deg f = n \geq 1$ .  
 The "Galois gp of  $f$  over  $F$ " is  $\text{Gal}(K/F)$  where  $K = \text{sp. fld. of } f \text{ over } F$ .  
 Prop 1: Galois gp of  $f$  is a subgp of  $S_n$ .  $G_f = \text{Galois gp of } f$   
 Easy:  $f$  has roots  $\alpha_1, \dots, \alpha_n$  and if  $\sigma \in G_f$ ,  $\sigma$  permutes  $\alpha_1, \dots, \alpha_n$ . So  $G_f \rightarrow S_n$   
 $\sigma \mapsto \sigma$   
 If  $\sigma(\alpha_i) = \alpha_i \forall i \Rightarrow \sigma$  is identity



The Galois gp of  $f$  over  $F$  is  $\text{Gal}(K/F)$

Prp 1: Galois gp of  $f$  is a subgroup of  $S_n$ .  $G_f = \text{Galois gp of } f$

Easy:  $f$  has roots  $\alpha_1, \dots, \alpha_n$  and if  $\sigma \in G_f$ ,  $\sigma$  permutes  $\alpha_1, \dots, \alpha_n$ . So  $G_f \rightarrow S_n$  is an injective gp homomorphism.

$\sigma \mapsto \sigma$

If  $\sigma(\alpha_i) = \alpha_i \forall i \Rightarrow \sigma$  is identity on  $K = F(\alpha_1, \dots, \alpha_n)$



So, as always  $F$  is a subfield of  $\mathbb{C}$ , small  $f$  is a polynomial of capital  $f$  and degree  $f$  is at least  $n$  which is a positive integer. So, some positive integer. So, I want to first define for simplicity the Galois group, the terminologies that the Galois group of  $f$  is the Galois group of the splitting field. So, again, I should write here Galois group of capital, small  $f$  over capital  $F$  is Galois group of  $K$  over  $F$ , where  $K$  is a splitting field of small  $f$  over capital  $F$ . So, first, I claim that so I make some remarks here. So, let say proposition.

So, the Galois group of  $f$  is certainly is a subgroup of  $S_n$ . This is clear. This is easy because  $f$  is degree  $n$ ,  $f$  has  $n$  roots. Maybe they are repeating because  $F$  could be reducible nevertheless if it has its roots  $\alpha_1$  through  $\alpha_n$  and so let us say  $G$  is the Galois group of  $f$  and if  $\sigma$  belongs to  $G$ ,  $\sigma$  permutes  $\alpha_1$  through  $\alpha_n$ . So, there is a map from  $G$  to  $S_n$ . Take  $\sigma$  and look at it as a permutation of  $\alpha_1$  through  $\alpha_n$  and  $\sigma$  fixes every  $\alpha_i$  then  $\sigma$  is identity on  $K$  because remember  $K$  is  $F(\alpha_1, \dots, \alpha_n)$ .

By definition  $K$  is a splitting field of capital of small  $f$  of capital  $F$ , so it is generated by them. So, that means this is an injective map. Injective group homomorphism. So, that means  $G$  is isomorphic to a subgroup of  $S_n$ . It could be any subgroup a priori.



(Refer Slide Time: 16:27)

★ Ppt 2:  $f$  is irreducible  $\Rightarrow G$  is iso to a transitive subgrp of  $S_n$ .

"Transitive": given any  $i, j \in \{1, \dots, n\}$ ,  $\exists \sigma \in G$  st  $\sigma(i) = j$ .

Reason: let  $\alpha_1, \alpha_n$  be roots of  $f$  in  $K = F(\alpha_1, \dots, \alpha_n)$ .

$F(\alpha_1) \subseteq \frac{F[X]}{(f(X))} \subseteq F(\alpha_2)$       identity on  $F$  and sends  $\alpha_1$  to  $\alpha_2$

---

Reason: let  $\alpha_1, \alpha_n$  be roots of  $f$ .

$F(\alpha_1) \subseteq \frac{F[X]}{(f(X))} \subseteq F(\alpha_2)$       identity on  $F$  and sends  $\alpha_1$  to  $\alpha_2$

$\sigma \in G = \text{Gal}(K/F)$  and  $\sigma(\alpha_1) = \alpha_2$

Upshot: Given any 2 roots of  $f$ ,  $\alpha_i, \alpha_j$ ,  $\exists \sigma \in G$  st.  $\sigma(\alpha_i) = \alpha_j$ .

---

Now let us say  $f$  is irreducible implies, this is important for us. So, this is sort of an important proposition. So,  $f$  is irreducible implies  $G$  is isomorphic to a transitive subgroup of  $S_n$ . Why is this? First of all, what does transitive mean? Transitive means given any 2 indices,  $i, j$  in the set 1 through  $n$ , there exists  $\sigma$  in  $G$  such that  $\sigma(i) = j$ . So, it means the orbit of any root is the entire set of roots. So, if you forget to the roots and you just think of  $G$  as permuting indices 1 through  $n$ , given any 2 indices, there is a group element which sends one to the other because that means sigma there is a sigma which sends 2 to 3. There is a sigma which sends 2 to 4 and so on and why is this true?

So, let  $\alpha_1$  through  $\alpha_n$  be roots of  $f$  in  $K$  which of course is  $f(\alpha_1)$  through  $\alpha_n$ . Then what is  $f(\alpha_1)$ ? This goes back to some of the earliest thing we did in the course because  $f$  is irreducible, we have this but this is also same as  $F(\alpha_2)$ . So, there is a map like this which sends which is identity on  $F$  and sends  $\alpha_1$  to  $\alpha_2$ . So, basically here  $\alpha_1$  goes to  $\bar{x}$ ,  $\alpha_2$  goes  $x$  bar. So, we compose these 2 to get this map and then you can always extend this using our standard extension theorems.

Extend this maps so  $\sigma$  sends  $\alpha_1$  to  $\alpha_2$  and fixes  $F$ . That means  $\sigma$  is in  $G$  which is Galois group of  $K$  over  $F$  and  $\sigma(\alpha_1) = \alpha_2$ . So, the upshot is, basically the upshot is given any 2 roots of  $\alpha_1, \alpha_2$ , there exists  $\sigma$  in  $G$  such that  $\sigma(\alpha_1) = \alpha_2$  or let me just say  $\alpha_i, \alpha_j$ , this is a property of group, the field homomorphisms. You can interchange any 2 roots.

(Refer Slide Time: 19:22)

This is not true if  $f$  is not irr :  $f = (x-3)(x^2+1) \in \mathbb{Q}[x]$   
 roots:  $3, i, -i = \alpha_1, \alpha_2, \alpha_3$   
 $\text{Gal}(f) \hookrightarrow S_3$ , but  $\text{Gal}(f) = S_2$   
 $G$  only contains  $e, (23)$  : in fact  $G = \{e, (23)\}$ ;  
 So  $G$  is not transitive.



$\text{Gal}(f) \hookrightarrow S_3$ , but  $\text{Gal}(f) = S_2$   
 $G$  only contains  $e, (23)$  : in fact  $G = \{e, (23)\}$ ;  
 So  $G$  is not transitive.  
 If  $f = X^3 - 2$ , then  $G$  is a transitive subgroup of  $S_3$ .  
 In fact  $G = S_3$   
 $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$



And let me warn you that this is not true if  $f$  is not irreducible. For example, if you take  $X$  to be  $x$  minus 3,  $x$  square plus 1 in  $\mathbb{Q}[X]$ . So, the roots are 3,  $i$ , minus  $i$ . So, the Galois group of  $f$  if I use this notation is a subgroup of  $S_3$ , but in fact it is  $S_2$ . So, if you call the roots these roots alpha 1, alpha 2, alpha 3, the only things here are those so  $G$  only contains the trivial identity homomorphism and the automorphism which sends 2 to 3 and 3 to 2. In fact,  $G$  is equal to that so  $G$  is not transitive. Talking about roots,  $G$  has no permutation which sends 3 to  $i$  for example, because 3 and  $i$  have different irreducible polynomials. So, it is not transitive.

However, if  $f$  is let us say,  $X$  cube minus 2, then  $G$  is a transitive sub group of, here roots are cube root of 2, cube root of 2 omega, cube root of 2 omega square. So, in fact  $G$  is equal to  $S_3$  in this case. So, irreducibility is important. So, the proposition 2 says, if  $f$  is irreducible  $G$  is isomorphic to transcripts subgroup of  $S_n$  and this sort of puts conditions on what possible Galois groups can occur. So, this is important for us to keep in mind. I will use this later on.

(Refer Slide Time: 21:36)

折, 折 w, 折 w

Def.  $f(x) \in F[x]$ ,  $\deg f = n$ ,  $\alpha_1, \dots, \alpha_n \in K$  are roots of  $f$ .


The "discriminant" of  $f$  is defined to be:

$$D = \text{Disc}(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2 \in K$$

claim:  $D \in F$ .

pf:

---



claim:  $D \in F$ .

pf: let  $\sigma \in G = \text{Gal}(K/F)$ . Then what is  $\sigma(D)$ ?

Since  $\sigma$  permutes  $\{\alpha_1, \dots, \alpha_n\}$ ,  $\sigma(D) = D$  (Exercise)

---


$n=3$ :  $D = (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2$

$\sigma \in G$ :  $\alpha_1 \mapsto \alpha_1$   
 $\alpha_2 \mapsto \alpha_3$   
 $\alpha_3 \mapsto \alpha_2$

$\sigma(D) = (\alpha_1 - \alpha_3)^2 (\alpha_1 - \alpha_2)^2 (\alpha_3 - \alpha_2)^2$

$= D$

$\sigma(\alpha_2 - \alpha_3)$   
 $= \alpha_3 - \alpha_2$   
 $= -(\alpha_2 - \alpha_3)$



So, now let me continue with general remarks. I will go back to the general situations,  $f$  is an arbitrary polynomial. Of degree  $n$  and let us say  $\alpha_1$  through  $\alpha_n$  are roots of  $f$ . So, capital  $K$  is always fixed to be the fixed field of  $f$  and the roots are  $\alpha_1$  through  $\alpha_n$ . So, the discriminant of  $f$  is defined to be, so discriminant of  $f$  or  $d$  usually will denote this is simply the product of  $\alpha_i$  minus  $\alpha_j$  whole square and we do this for every  $i$  less than  $j$ . For every pair of indices,  $i$  less than  $j$ , we take  $\alpha_i$  minus  $\alpha_j$ . So, the claim now is  $D$  is  $F$ .

So, a priori it is in  $K$ , of course because  $\alpha_i$  and  $\alpha_j$  are in  $K$ .  $\alpha_i$  are all in  $K$ . So, this is in  $K$  but in fact, it is in the base field. This is because let  $\sigma$  be in the Galois group of  $K$

over  $F$ . Let us call that  $g$ . So then, what is  $\sigma$  of  $D$ ? What is  $\sigma$  of  $D$ ? So, I claim that  $\sigma$  of  $D$  since  $\sigma$  permutes  $\alpha_i$ , so this is an easy exercise for you. This set, I claim that  $\sigma$ , so basically I want claim this, so let me explain this.

So, here, for example if  $n$  equal to 3, just as a simple example. So, here, we have  $\alpha_1$  minus  $\alpha_3$  or let us say  $\alpha_2$  first,  $\alpha_1$  minus  $\alpha_3$  square square and  $\alpha_2$  minus  $\alpha_3$  square and now you take any  $\sigma$  in  $G$ . It simply permutes the 3 roots. As an example, let us say  $\alpha_1$  goes to  $\alpha_1$ ,  $\alpha_2$  goes to  $\alpha_3$ ,  $\alpha_3$  goes to  $\alpha_2$ . So, here we have  $\alpha_1$  minus  $\alpha_3$  whole square.  $\sigma$  is an automorphism. So, you can just apply inside the bracket.  $\alpha_1$  goes to  $\alpha_1$ ,  $\alpha_3$  goes to  $\alpha_2$ ,  $\alpha_2$  goes to  $\alpha_3$  and  $\alpha_3$  goes to  $\alpha_2$ .

So, remember  $\sigma$  of  $\alpha_2$  minus  $\alpha_3$  is  $\alpha_3$  minus  $\alpha_2$ . However, once you square, so this is minus of  $\alpha_2$  minus  $\alpha_3$ . So, this is sort of a crucial observation. So,  $\alpha_2$  minus  $\alpha_3$  goes to minus of  $\alpha_2$  minus  $\alpha_3$  but because  $D$  is squaring all these terms, you get no new element. So, this I will leave as an exercise for you to, the general proof. Essentially the same idea.

(Refer Slide Time: 25:02)

$\sigma(\alpha_i - \alpha_j)^2 = (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})^2 \Rightarrow \sigma(D) = D \checkmark$   
 Hence  $\sigma(D) = D \forall \sigma \in G \Rightarrow D \in K^G = F$  ( $\because K/F$  is Galois)  
Facts:  $n=2$ :  $D = (\alpha_1 - \alpha_2)^2 = b^2 - 4c$  where  $f = x^2 + bx + c$   
 $\begin{cases} \alpha_1 + \alpha_2 = -b \\ \alpha_1 \alpha_2 = c \end{cases}$   
 $(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1 \alpha_2 = b^2 - 4c$   
 $n=3$ :  $f = x^3 + a_2 x^2 + a_1 x + a_0$   
 $\text{Disc}(f) = (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2$   
 $\text{fact} = -4a_2^3 a_0 + a_2^2 a_1^2 + 18a_2 a_1 a_0 - 4a_1^3 - 27a_0^2$

So,  $\sigma$  of  $\alpha_i$  minus  $\alpha_j$  is an  $\alpha$  of  $\sigma i$ , thinking of  $\sigma$  as a permutation. So, you take the product, apply  $\sigma$  inside the product. Everything appears somewhere else and because  $\sigma$  is an automorphism of  $\alpha_i$  equal to  $\alpha_j$ , we are able to say that  $\sigma$  of  $D$

is equal to  $D$  but that means so that part is an exercise. So, this implies  $\sum D$  is equal to  $D$ . So, this I will let you to do that. So, hence  $\sum D$  equals  $D$  for all  $\sigma$  in  $G$ . So, this implies  $D$  is inside  $K^G$  which is  $F$  because  $K$  over  $F$  is Galois, because it is a splitting field of a polynomial and we are in characteristic 0. So,  $D$  is in  $F$ .

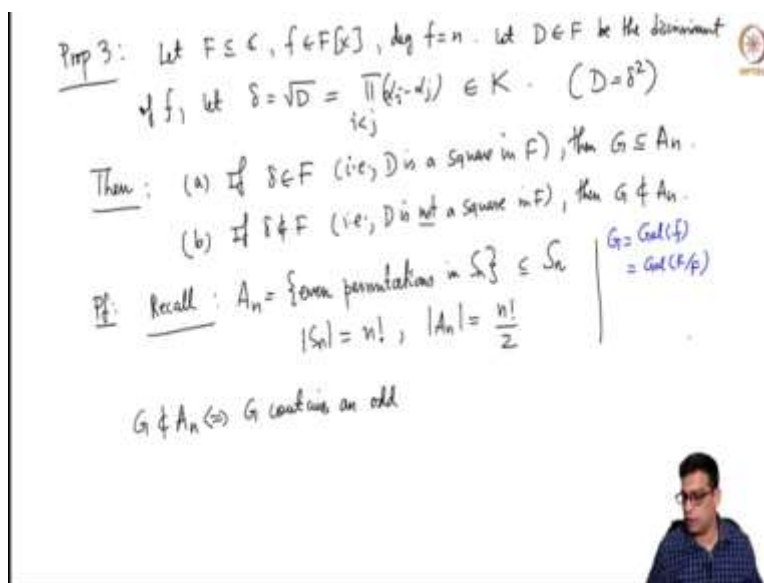
So, that is a statement and some facts that I will write here for degree 2, you take  $F$  to be a degree 2 polynomial. What is the discriminant? You simply have  $(\alpha_1 - \alpha_2)^2$ . There is only one pair  $i, j$  and if you think about this, this is exactly the, if you think about this, this is if  $f$  is  $x^2 + a_1x + a_2$ , then you get this, so this or rather maybe I will just write it. The  $x^2 + bx + c$ , then you get the usual discriminant that you are familiar with because  $\alpha_1 + \alpha_2$  remember is  $-B$ ,  $\alpha_1 \alpha_2$  is  $C$ .

So, use this to conclude this because if you take  $(\alpha_1 - \alpha_2)^2$  or  $\alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2$  that will be  $(\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2$  because this is  $\alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2$ . Here you get  $b^2 - 4C$ . That is all. So, I have done the exercise for you.

So, this of usual discriminant but if  $n$  equal to 3 in which case  $f$  equal to so I am going to write it like this,  $f$  is  $x^3 + a_2x^2 + a_1x + a_0$ . Then discriminant of  $f$  has a formula which is significantly more computation to do than the degree 2 case. However, you can do this. It is not completely impossible, but you can do this. So, this is a fact that I will write which in the examples I am going to use this occasionally. So, this will happen to be  $-4a_2^3 - 27a_0^2 + 18a_2a_1a_0 - 4a_1^3$ .

So, this is just a significantly messier formula but it is irrelevant for the theory that we want to develop. So, I just want to record it because in some examples I might want to mention this. In general, of course in higher degrees the discriminant becomes significantly more complicated to write.

(Refer Slide Time: 28:50)



Prop 3: Let  $F \subseteq \mathbb{C}$ ,  $f \in F[x]$ ,  $\deg f = n$ . Let  $D \in F$  be the discriminant.  
 $\sqrt{f}$ , let  $\delta = \sqrt{D} = \prod_{i < j} (\alpha_i - \alpha_j) \in K$ . ( $D = \delta^2$ )  
Then: (a) If  $\delta \in F$  (i.e.,  $D$  is a square in  $F$ ), then  $G \subseteq A_n$ .  
 (b) If  $\delta \notin F$  (i.e.,  $D$  is not a square in  $F$ ), then  $G \not\subseteq A_n$ .  
Pf: Recall:  $A_n = \{\text{even permutations in } S_n\} \leq S_n$   $G = \text{Gal}(F/\mathbb{Q})$   
 $= \text{Gal}(K/F)$   
 $|S_n| = n!$ ,  $|A_n| = \frac{n!}{2}$   
 $G \not\subseteq A_n \Leftrightarrow G$  contains an odd

And we do not care for a closed formula for it but now let me make this third proposition which I want to do. So, let  $F$  be a subfield of  $\mathbb{C}$  as always.  $f$  is a polynomial in the base field and degree  $f$  is  $n$ . Let  $D$  be the discriminant of  $f$  and let  $\delta$  be square root of  $D$ . Remember square root of  $D$  is actually  $\alpha_i \alpha_j$ ,  $\alpha_i - \alpha_j$ ,  $i < j$ . Discriminant is the product of the squares of the differences. Square root of the discriminant is just product of the differences. This is of course in  $K$ .

Now I claim that whether it is so  $D$  is  $\delta^2$ , whether  $\delta$  is in  $F$  or not determines something about the Galois group. So, then the first statement is if  $\delta$  is in  $K$  or rather  $\delta$  is in  $F$  that is  $D$  is a square in  $F$ . That means  $D$  has a square root of  $F$ . Then  $G$  is contained in  $A_n$ ,  $A_n$  is the alternating group. That means it is a subgroup of  $S_n$  consisting of even permutations. If  $\delta$  is not in  $F$  that is  $D$  is not a square, then of course  $G$  is not contained in here. So, the proof is so recall  $A_n$  equals even permutations in  $S_n$ . So, this is a normal subgroup of index 2. So, the order of  $S_n$  is  $n$  factorial and there are exactly half of them which are even. So, this is just to recall for you.

So, now note the following.  $G$  is not in  $A_n$ . This is only if  $G$  contains an odd permutation. So, of course, remember,  $G$  which is the Galois group I should have mentioned that  $G$  is the Galois group of  $F$  which is the Galois group of the splitting field of  $K$  of  $F$  over  $F$ . That  $G$  contains an odd permutation. It is the statement that  $G$  is not in  $A_n$  but if it is in  $A_n$ , it cannot contain an odd

permutation and if it contains in an odd permutation, if it is not contained in  $A_n$ , it means it contains an odd permutation. This is just a definition of not being  $A_n$ .

(Refer Slide Time: 32:04)

Handwritten notes on a whiteboard:

- $|S_n| = n!$
- $G \not\subset A_n \Leftrightarrow G$  contains an odd perm  $\sigma$
- $\Leftrightarrow \sigma(\delta) = -\delta + \delta$  for some  $\delta \in G$
- $\Leftrightarrow \sigma \notin K^G = F$
- Ex: Given  $\sigma \in G$ , either  $\sigma(\delta) = \delta$  or  $\sigma(\delta) = -\delta$
- $\delta$  is even  $\delta$  is odd
- $\sigma \in S_n$  is odd  $\Rightarrow \sigma$  can be written as a product of an odd no of 2-cycles.
- $\sigma(\delta) = -\delta$

Now that means I claim now  $\sigma(\delta)$  is equal to  $-\delta$ . So, this point is related to this. This proof that I asked you to do because if  $\sigma$  is an odd permutation so let us say  $\sigma$  is odd, then that means it interchanges, you can argue like this. I mean so it, so it can be written as a product of, so maybe  $\sigma$  can be written as a product of an odd number of 2 cycles or transpositions. Now let us say 5 transpositions. Now, let us go back to  $\delta$ .  $\delta$  is right here.

So, if  $\sigma$  can be written as a product of 5 transpositions, all 5 of those will interchange  $\alpha_i$  and  $\alpha_j$ . So, the sign of  $\alpha_i - \alpha_j$  changes. So, there will be 5 sign changes. All together, they will give a minus sign so that means  $\sigma(\delta)$  is  $-\delta$ . So,  $\sigma$  is odd, this happens. This basically if and only if because if  $\sigma$  is even that means it can be written as end product of an even number of transpositions or 2 cycles, then there will be an even number of sign changes and they cancel each other and  $\delta$  is fixed by  $\sigma$ .

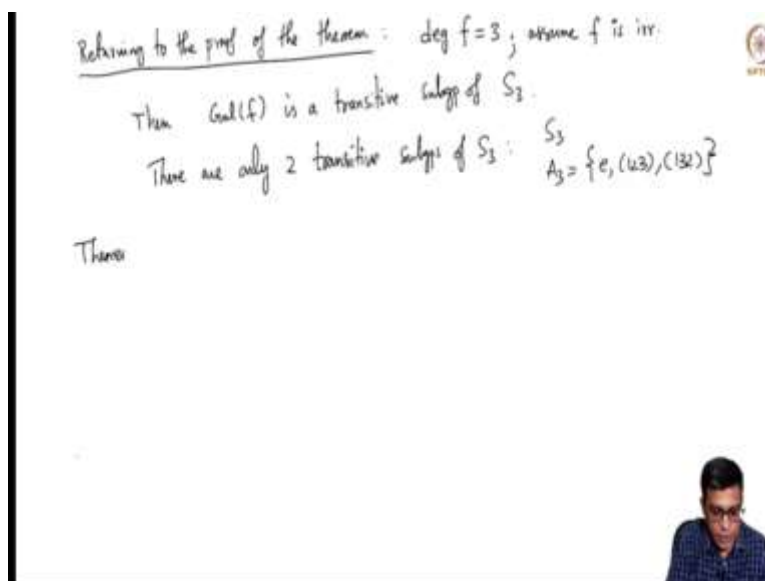
So,  $\sigma(\delta)$  is  $-\delta$  if and only if it is odd. That means  $\delta$  is not in, of course because we are in characteristic 0  $-\delta$  is not  $\delta$ . So,  $\sigma$  is not in  $K^G$  that means it is not in  $F$ . So, this is a bit confusing but what I am saying, is that for a fixed  $\delta$  in  $S_n$ , if it is not enough that means  $\sigma$ , that means some  $\sigma$  does not fix  $\delta$  but whatever that does not fix  $\delta$  must be odd.



So, basically the exercise that I want to do is given  $\sigma$  in  $G$  either  $\sigma(\delta) = \delta$  or  $\sigma(\delta) = -\delta$  and this happens only if and only if  $\delta$  is even. This happens only if, if and only if this is odd. So, this is the exercise which essentially sort of is proved here but I want you to spend some time to think about this and make sure that you understand. This is a crucial observation about Galois groups of polynomials. The image of the square root of the discriminant under a Galois group element is either always that itself or it is minus.

So if it is not, if it is in the fixed field, that means it everything in  $G$  fixes it. That means only things in  $G$  are even permutations. That means  $G$  is an  $A_n$ . If it is not in  $F$  that means something in the group element, something in the group does not fix it but that means something in the group is not odd, not even. That means something in the group is even. That means  $G$  is not contained in  $A_n$ . So, this I went over this somewhat fast, but hopefully this makes sense to you. So, please make sure that you sort of understand what I have done here, whether the Galois group is in alternating group or not is deducible from the square root of the discriminant.

(Refer Slide Time: 36:33)



Referring to the proof of the theorem:  $\deg f = 3$ ; assume  $f$  is irr.

Then  $\text{Gal}(f)$  is a transitive subgroup of  $S_3$ .

There are only 2 transitive subgroups of  $S_3$ :  $S_3$   
 $A_3 = \{e, (123), (132)\}$

Then:

Theorem:  $f$  as above,  $\delta = \sqrt{d}$ .  
 (i)  $\delta \in F \iff G = A_3$  and  $[K:G] = 3$ .  
 (ii)  $\delta \notin F \iff G = S_3$  and  $[K:G] = 6$ .  
 Examples: (i)  $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$  Ex: Use Eisenstein (after  $X \rightarrow X-1$ ) to conclude  $f$  is irr  $\mathbb{Q}[X]$ .



Now returning to the proof of the theorem. So, the pause that I said earlier now we are going to return to the proof of the theorem, which is that any degree 4, 3, 2, 1 polynomials are solvable and let us first look at degree  $f$  equal to 3. So, assume that 1 and 2 I have done. So, I am going to safely assume that  $f$  is irreducible because if it is not irreducible it is a product of a linear polynomial and a quadratic polynomial and each of them individually are solvable so  $f$  is. So, I might as well consider irreducible degree 3 polynomial. Then, the Galois group of  $f$  is a transitive subgroup of  $S_3$  because  $f$  is irreducible by the proposition 2, its Galois group is a transitive subgroup of  $S_3$ .

There are only 2 such things namely  $S_3$  which consists of all of them or  $A_3$  which consists of the 3 cycles because other subgroups of  $S_3$  are the order 2 subgroups and none of them is transitive because for example, if you take this this does not send 1, 2, 3. So, this cannot be transitive. So, there are only 2 possibilities for the Galois group of an irreducible cubic. It is either  $S_3$  or  $A_3$  and the differentiating feature of these 2 is in one case, you have odd permutations in the other case, you do not have odd permutations.

So, let me just summarize what I have degree 3,  $f$  as above so that means irreducible degree 3. Then  $\delta$  is square root of  $d$ . Then the first part is  $\delta$  is in  $F$ , if and only if Galois group is  $A_3$  and of course in that case  $K:G$  is 3. In the second case  $\delta$  is not in  $F$ , that means  $G$  is equal to  $S_3$  and in the case  $K:G$  is 6. So, these are the 2 features of the Galois 2 cases for the Galois group of an irreducible polynomial.

So, let me quickly give you a couple of examples covering both cases. So, let us say  $f$  is  $X$  cube minus  $3x$  plus  $1$ . So, then as an exercise use Eisenstein after substituting  $X$  minus  $1$  for  $x$ . Of course, you cannot apply Eisenstein right away. So, you have to change the variable to conclude  $f$  is irreducible. So, that I will let you do this. Of course, it is in the rational polynomial ring. So, this is a irreducible polynomial.

(Refer Slide Time: 39:49)

(ii)  $S \nmid F \Rightarrow G = S_3$  and  $[K:F] = 6$ .

Examples: (i)  $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$ . Ex: Use Eisenstein (after  $X \rightarrow X-1$ ) to conclude  $f$  is irr  $\mathbb{Q}[X]$ .

$\text{Disc}(f) = 3^4$  is a square in  $\mathbb{Q}$ . <sup>use the earlier formula</sup>

Hence  $[K:F] = 3$  and Galois group of  $f$  is  $A_3$ . <sup>2/32</sup>

(ii)  $f = X^3 + 3X + 1$  (again:  $f$  is irr,  $X \rightarrow X-1$ )

$\text{Disc}(f) = -53$  is not a square in  $\mathbb{Q}$ .

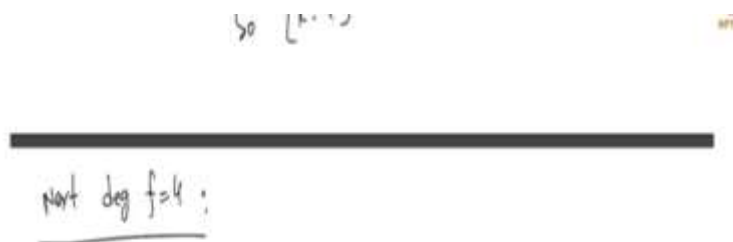
So  $[K:F] = 6$  and Galois group of  $f = S_3$ .

So, what is the discriminant of this? So, this is more or less the only place I will use the formula that I wrote earlier. Very messy formula but you can compute it and I will simply say that it is so equal to this. So, I simply say that use the formula. There is not much theory here, so this is not just it is a computation because it is not just the computation. So, this is not a square in  $\mathbb{Q}$ . Of course, it is not a square in  $\mathbb{Q}$ . For one thing, it is a negative number. So, hence  $K$  colon  $F$  is  $3$ . The Galois group  $f$  is  $A_3$ . So, some calculations of the discriminant tell you immediately what it happens. So, in the other case, we get  $x$  cubed plus  $3x$  plus  $1$  plus  $3x$  plus  $1$ .

So again, this is irreducible. Use the same I think change of variable and use Eisenstein. In this case, discriminant of  $f$  turns out to be  $3$  power  $4$  is a square in, I am sorry, so I think I wrote something wrong here. So, this is  $3$  power  $4$ , I am sorry is a square, about that. So,  $x$  cube minus  $3x$  plus  $1$  is  $3$  power  $4$ , I do not want to do the calculation in the video. It is a waste of time because you can use the formula here. So, just apply the formula and you make sure that I did everything correctly here. So, here is a square.

So, the Galois group is  $A_3$  and in this case it is the other one. So, minus 5 times 3 cubed is not the square so  $K:F$  is 6 and Galois group is  $S_3$ . So, in this case, you have a degree 6 extension with Galois group  $S_3$ . Here you have a Galois degree 3 extension, Galois group  $A_3$  which is of course isomorphic to  $\mathbb{Z}/3\mathbb{Z}$ . So, now also I think this is a polynomial that I said earlier has 3 real root. One can check its graph, looks like this. So, just to remind you that that is the polynomial that we considered earlier. So, now that leaves for me to prove the theorem in the degree 4 case.

(Refer Slide Time: 42:40)



Next, let me stop the class here. I will do degree 4 in the next class and that finishes the proof of the theorem which says that any polynomial of degree less than or equal to 4 is solvable over base field  $F$ . Thank you.