

Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 45
Insolvability of quintics

Welcome back we are, we have proved that there if a degree 5 polynomial has Galois group S_5 or A_5 ; then it is not solvable. We we are yet to produce examples of such polynomials, but before we do that I want to reprove this statement.

(Refer Slide Time: 00:36)

Theorem: $F \subseteq \mathbb{C}$, $f \in F[X]$ $\deg f = 5$. Suppose the Galois gp 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 $D = \text{Disc}(f)$
 $G = \text{Gal}(K/F) = \text{Gal}(f)$ $I = \sqrt{D} \in K$

Since $\text{Gal}(f) \not\subseteq A_5$, $S_5 \not\subseteq A_5 \Rightarrow [F(D):F] = 2$
 $\therefore \text{Gal}(K/F(D)) = A_5 \Rightarrow$ Galois gp of f over $F(D)$ is A_5 .
 $\Rightarrow f$ is not solvable over $F(D)$
 $\Rightarrow f$ is not solvable over F .

This will follow by considering the A_5 case.

Because as promised I want to give you two different proofs of that statement; so, let me prove the following. So, this is a result that we already know, but it is a different proof; so let us take a degree 5 polynomial. So, suppose the Galois group of f is S_5 or A_5 , then f is not solvable. Remember, we did prove this because the Galois group f is solvable, if and only if Galois group is solvable. And the Galois group is by hypothesis either S_5 or A_5 ; so it is not solvable by group theoretic arguments. So, f itself is not solvable.

But, here I do not want to introduce solvable groups; this is a self contained proof that will work; only using that A_5 is simple. So, that only thing we need; so let us start the proof. So, suppose G is S_5 , so let G be the Galois group, first suppose G is S_5 . So, I do not argue that I can assume G is A_5 and then that will also solve the case for S_5 . So, then let K be the splitting field of F over K

over F ; so, the G is the Galois group of K over F by definition. So, you have K and you have F to begin with so this is S_5 ; the Galois group is S_5 . But, now first add let D be the discriminant of f , and Δ is the square root of the discriminator.

Since, Galois of f is not contained in A_5 , we know that Δ is not in K ; Δ is not in F . This is something we have shown; discriminant is square if and only if the Galois group is contained in the alternating group. So, this is in fact a degree 2 extension; it is either degree 2 extension or degree 1 extension. But, if it is degree 1 extension, Δ will be in F ; so that is not possible. So, this is degree 2 and Galois of course and this is the Galois group A_5 ; that is the only group if you think about this of order 2, order index 2.

So, this must be; so this implies the Galois group only group of index 2 is S_5 is A_5 . So, this must be a group of index 2; because this is 2 so that is A_5 . So, Galois group of f over $F(\Delta)$ is A_5 . So, suppose that we have shown that Galois group if the Galois group is A_5 , then the polynomial is not solvable; then f is not solvable over $F(\Delta)$. So, so this implies f is not solvable; because if it if the roots cannot be expressed as radicals with coefficients in $F(\Delta)$, they cannot be expressed as using radicals in F . So, if it is not solvable over a bigger field; it is not solvable over a smaller field.

So, this is what I will show; this this will follow. So, if we prove the A_5 case, that means forget S_5 for the moment. So, if we showed that if Galois group is A_5 , then F is not solvable. Then, applying the theorem Galois group of small f over $F(\Delta)$ is A_5 ; so it is not solvable over $F(\Delta)$. It will follow in turn that it is not solvable over F .

(Refer Slide Time: 05:50)

This will follow by considering the A_5 case.
 $\Rightarrow f$ is not solvable over F .
 So it suffices to consider the case $\text{Gal}(f) = A_5$.
 Let $G = \text{Gal}(f) = A_5$.
 Our goal: f is not solvable over F .
 $K \supset A_5$
 F



Let $G = \text{Gal}(f) = A_5$.
 Our goal: f is not solvable over F .
 Suppose it is. Let $\alpha \in K$ be a root of f . So α is solvable over F .
 F



So, it suffices it to consider the case Galois f is A_5 ; because if I proved that case this implication will follow. So, now we are in business, so we assume; so let G is a Galois group of f which is A_5 . So, suppose so now I am done with this discriminant business; so now I have my situation is K over F . This is A_5 and it is supposed to be not solvable; so, K is a splitting field of small f over capital F . So, if so our goal f is not solvable over capital F .

Suppose now or suppose it is: Suppose it is solvable over capital F ; that means let α be a root of small f in capital K . So, α is, so this is going to be our assumption and we hoped to get a

contradiction. Suppose its roots are solvable, so I will take one root; alpha is solvable over solvable over F.

(Refer Slide Time: 07:34)

hence: \exists a tower of extns which cyclic of prime degree:
 $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_r$; $\alpha \in F_r$ & F_i/F_{i-1} is Galois
 & $[F_i:F_{i-1}]$ is prime.

Thm: Let $F \subseteq \mathbb{C}$; let $\alpha \in \mathbb{C}$ be a root of a polynomial $f(x) \in F[x]$.
 (1) α 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 & $\alpha \in F_r$.
 (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)
 (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)

So, there exist a tower of extensions which are cyclic of prime degree like this. So, what I want to do is F which is F0 contained in F1 contained in Fr; and alpha is in Fr, and each is cyclic of prime degree. And Fi contained in Fi minus 1, so need to say Fi over Fi minus 1 is Galois; and the index of this or the degree of this extension is prime. So, now radical is equivalent to being radical is equivalent to existence of such a tower with abelian extensions, or cyclic extensions; or

refining further cyclic of prime degree. So, I added this additional condition to you to the theorem that we did; so I will just show it to you.

Remember we originally want to 3, but then later I added third a fourth condition; because it is going to come up later, and it comes up now. So, there exists a tower like this, where each extensions is cyclic of prime order; so it is Galois and its Galois group is a prime number, is a cyclic group of prime order. And it is a triviality to go from 3 to 4, because also you have a cyclic extension; you can take a subgroup which is of prime index; go modulo that and so on. And so, 3 to 4 is a triviality; so I just added that after we prove this theorem. And we are going to just now use 4 directory; so we have such a situation. So, now what I will do is the following.

(Refer Slide Time: 09:47)

Lemma: Let F'/F be a Galois ext st $[F':F]$ is prime. Let K' be the sp fld of f over F' . Then $\text{Gal}(K'/F') \cong A_5$.

Diagram:

```

    K
    / \
   F'  F
  
```

$K = \text{sp fld of } f \text{ over } F$
 $K' = \text{sp fld of } f \text{ over } F'$

Conditions:

- K sp fld h
- $1 \leq 24$
- $L = \text{sp fld of } g$
- $1 \leq 24$
- F

Red box text:

If $\text{Gal}(G) = A_5$ or S_5 then f is irreducible.
 Ex: $f = gh$
 $\deg g \leq 4$
 $\deg h \leq 4$
 $5 \mid |\text{Gal}(K'/F)|$
 but if f is red, then 5 can't divide $|\text{Gal}(K'/F)|$

Now, I have a small claim, which is actually the main ingredient in the proof; so, let me prove that as a lemma. Let F' prime over F be again a Galois extension, such that the degree of this extension is prime number, is a prime number. Let K prime be the splitting field of small f over capital F , F' prime; K prime is a splitting field of small f over F' prime. Then, I claim Galois group of K prime over F' prime is also isomorphic to A_5 ; so that is the lemma. And this lemma is all that we required; so the main ingredient is that lemma. So, let us carefully prove this. So, the picture is the following.

So, you have I will draw this picture a few times; so you have F to F' prime, so F to F' prime. And we have also K , remember K is the splitting field of small f over capital F . And we have K

prime, which is a splitting field of f over capital F prime; so, now let us just see what these are. So, first of all K is equal to F adjoint $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$; so as a small exercise, I did not say that f is an irreducible polynomial in theorem. But, if Galois group of f is A_5 or S_5 , then f is irreducible; this is an exercise for you. Because if it is not irreducible, then it factors as gh , where degree of g and degree of h are less than or equal to 4.

So, the Galois group cannot be S_5 or A_5 . So, because K will be, so basically what we know is that Galois group of K over F is the order of that is divisible by 5. Because it is either 60 or 120; in either case 5 divides this. But if f is reducible, then 5 cannot divide; so I will leave that as an exercise, maybe I will do this in the exercise session later on. So, f is irreducible in order for to have the right Galois group A_5 or S_5 . Because if its degree 4, so it is a product of small degree polynomials; it can be when you attach roots of g , you will have L . This degree is less than equal to 24; and then you will have another.

So, this is the splitting field of g which is degree 4, and then you will have splitting field of h . So, that is also less than equal to 24; in fact if its degree, I mean it will be much less than that. But, I do not care, but the total can be 5 cannot be divide the total product. So, anyway this is triviality, but I wanted to record that; and I wanted to state a stronger theorem. So, stronger looking theorem, so I do not want to assume f is irreducible. So, let me record bit here, f must be irreducible with this hypothesis.

(Refer Slide Time: 14:05)

The slide contains handwritten notes and a diagram. The diagram shows a field extension K/F with an intermediate field F' . The extension F'/F is labeled with P . Below the diagram, it is noted that K is the splitting field of f over F and K' is the splitting field of f over F' . To the right, the Galois group $\text{Gal}(F'/F) \cong \mathbb{Z}/p\mathbb{Z}$ is stated, followed by the observation that F'/F has no proper intermediate fields. Further down, it is noted that F' is the splitting field of a polynomial $g \in F[X]$. On the far right, a red box contains the following text: "deg $g = 1$, deg $h \leq 4$, $5 \nmid |\text{Gal}(K/F)|$, but if f is red, then 5 can't divide $|\text{Gal}(K/F)|$ ".



So, the conclusion that f must be irreducible says that α_1, α_2 are 5 distinct elements. So, that is something that I note, and what is F prime; so this is what we have. F Galois group, let say this is P , so prime say P ; some prime number P is isomorphic to $\mathbb{Z} \bmod P$. So, it is the splitting field of some polynomial and we know that has no proper intermediate fields. It has no proper intermediate fields because it is a prime number. If you have an intermediate field here that must be either equal to F or F prime; because P cannot be factored as product of two smaller numbers. This we also know that F prime is the splitting field of a polynomial.

(Refer Slide Time: 15:31)

Then g must be irreducible: $g = h \cdot h'$ $\deg h > 0, \deg h' > 0$.
 can also assume $\deg h > 1, \deg h' > 1$.
 $(h, h') = 1$
 $\gcd = 1$

Then

$F' = F(\text{roots of } g)$
 \vdots
 $F(\text{roots of } h)$
 \vdots
 F

(Exercise)

$g = h \cdot (x-a)$
 $a \in F$
 $F = \text{sp field of } h$
 $\text{sp field of } g$

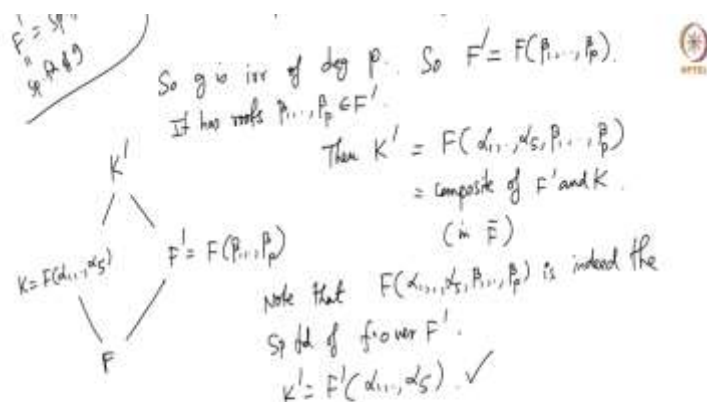
We claimed that g must be reducible. And the reason is similar to above. So, it is the splitting field of a polynomial, because F prime is Galois; any Galois extension is splitting field of a polynomial. In this case separable is automatically there, so I just not mentioned that. Because if g is some h times h prime with both h and h prime being positive degree polynomials. Then, we have F prime which is F adjoint roots of g , and you can have intermediate field here; F adjoint roots of h and F .

So, this if this is a proper decomposition, I can also assume that; because if they are not degree 1 if any other miss degree 1, I can drop it and take that as g . If g is h times x minus a , then a is in F ; so f prime will be splitting field of h . F prime is a priory splitting field of g , but I do not get anything extra by attaching another linear factor. So, I can remove all the linear factors that g

may contain. Then if it is not irreducible, it will factored as the reducible polynomials of degree greater than 1, so at least 2.

So, this is not an equality and this is not an equality; because h prime cannot be contain roots of h prime cannot be here. Because they are co-prime that means they have no common roots; h and h prime are co-prime. Because they are too reducible, they can further factor; but I assume that GCD is 1. So, I understand that this is all a bit of work; I mean this is not such a triviality as I am trying to suggest. But, this is an exercise, so take this as an exercise and show that g is a irreducible polynomial. So, because you can conclude that these two must be unequal. So, now what we have is g is an irreducible polynomial.

(Refer Slide Time: 18:23)




So, g is irreducible of degree P . Of course, it has to be P because you take any root, its irreducible polynomial is g ; and the degree of extension is P . So, this tells me that F prime is F adjoint some β_1 through β_P . So, it has roots, so it splits completely in F prime; so the roots are β_1 through β_P . So, now I am going to rewrite our picture. So, K is equal to F α_1 through α_5 and F prime is F β_1 through β_P .


Now, let us take K to be let K prime to be F adjoint all of them; so K prime is the composite. So, I use the composite of F prime and K obviously that is a smallest field, let say in \bar{F} . I need to talk composites are really make them meaningful only in a bigger field. I can take it to be in \bar{F} .

Because that is any field that contained both K and F prime, must contain α_1 through α_5 , β_1 through β_P ; and this is the smallest such field.

And now note that K prime have used earlier and they it is not accident that; so I should not really talk about a new K prime new K prime is not being defined for the first time. But, I will simply wrote that α_1 through α_5 , β_1 through β_P is indeed the splitting field of f over F prime. Because this field K prime is generated over F prime by the roots; so, K prime is F prime adjoint α_1 through α_5 . So, F splits completely in K prime and it is generated over the roots over F prime by the roots; so that is the splitting field of small f over F prime. So, now this is our picture.

(Refer Slide Time: 21:08)





Every extn in this picture is Galois


Claim: $H \cong A_5$. (This is what we want to prove)

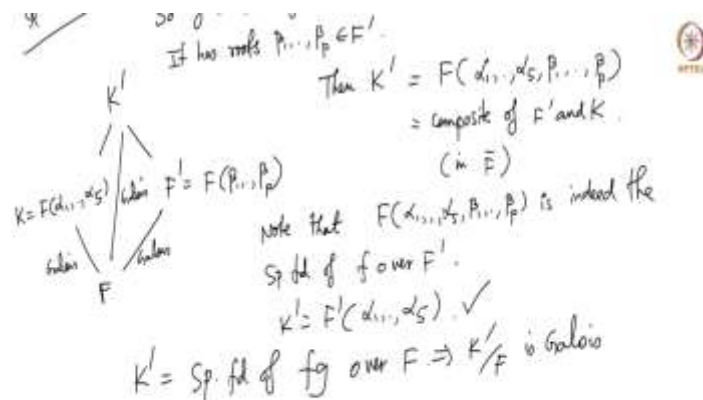
$N := \text{Gal}(K'/F)$

Then:

- $H \leq N, H' \leq N$ are normal subgroups
- $N/H \cong G' \text{ \& \; } N/H' \cong G$

(from Main Theorem)





So, K prime F sorry K prime K , F , F prime. And this I am going to write now instead of the degree I am going to write the Galois groups here. Let us call this Galois group G , let us call this Galois group G prime, let us call this H , and let us call this H prime. And what is our claim? Our claim is that Galois group of K prime over F prime is $K5$; so, claim H is isomorphic to $A5$, so this is what we want to prove. And I am just introducing the new H prime here that is a Galois group of this. So, everything here is every extension here is Galois, because K is Galois; because that is a splitting field.

F is Galois over F prime, F prime is Galois over F prime by hypothesis; and K prime is the splitting field of actually fg over capital F . Because the roots of fg are α_1 through α_5 and β_1 through β_p are more directly this is Galois; and this is Galois, so the composite is Galois I am saying. So, now let N be the Galois group of K prime over F ; let N be the Galois group of K prime over F . So, now I am going to do some serious group theory; so what do I do?

And we have so then let us list down all the statements. So, H and H prime are normal subgroups; because these extensions are Galois. And G or $N \bmod H$ is isomorphic to G prime, and $N \bmod H$ prime is isomorphic to G ; this is from main theorem of Galois Theory so far so good, so there is nothing serious yet. This is N modulo H is G prime; this N modulo H prime is G .

(Refer Slide Time: 24:00)

Every extn in this picture is Galois (from Main Theorem)

claim: $H \cap H' = \{1\}$

pf: $\sigma \in H' = \text{Gal}(K'/K) = \{F\text{-auto of } K' \text{ that fix } \alpha_1, \dots, \alpha_5\}$

$\sigma \in H = \text{Gal}(K'/F) = \{F\text{-auto of } K' \text{ that fix } \beta_1, \dots, \beta_p\}$

$\therefore \sigma \in H \cap H' \Rightarrow \sigma$ is an F-auto of K' that fixes $\alpha_1, \dots, \alpha_5, \beta_1, \dots, \beta_p$

But $K' = F(\alpha_1, \dots, \alpha_5, \beta_1, \dots, \beta_p)$. So $\sigma = 1$.



So, now consider the first we claim that $H \cap H'$ is identity; so the proof is simple here. Suppose σ is in H , what does this mean? σ is in H means what is H ? H is the Galois group of K' over K . So, these are automorphisms, automorphisms of K' that fixed K , which is generated by α_1 through α_5 . So, σ is in H means σ fixes α_1 through α_5 . σ in H' means H' is the Galois group of K' over F ; so these are automorphisms of K' that fix everything in F . H is the Galois, H' is the Galois; let me write it H' here, let me write H here.

H' is the Galois group of K' over K ; so automorphisms that consists of automorphisms of K' that fix K , in particular α_1 through α_5 . So, let me say F automorphisms of; because F is fixed and then α_1 through α_5 is fixed. That means that is equivalent to saying it fixes K . Here these are F automorphisms of K' that fix β_1 through β_p . So, if σ fixes $\sigma \in H \cap H'$ implies σ is an F automorphisms of K' that fixes all the α_i 's and all the β_j 's.

But, K' is generated by those; so σ is identity. So, it fixes F , it fixes α_1 through α_5 and it fixes β_1 through β_p ; so, it better be identity. So, $H \cap H'$ is identity, so that is good.

(Refer Slide Time: 26:23)

$$\begin{aligned}
 &\text{Consider the canonical map: } \varphi: N \rightarrow N/H \cong G'. \\
 &H' \leq N \quad \text{Restrict to } H': \quad \varphi|_{H'}: H' \rightarrow N/H \\
 &\quad \ker(\varphi|_{H'}) = (\ker \varphi) \cap H' = H \cap H' = \{1\} \\
 &\Rightarrow \varphi|_{H'}: H' \rightarrow G' \cong \mathbb{Z}/p\mathbb{Z} \text{ is injective.}
 \end{aligned}$$



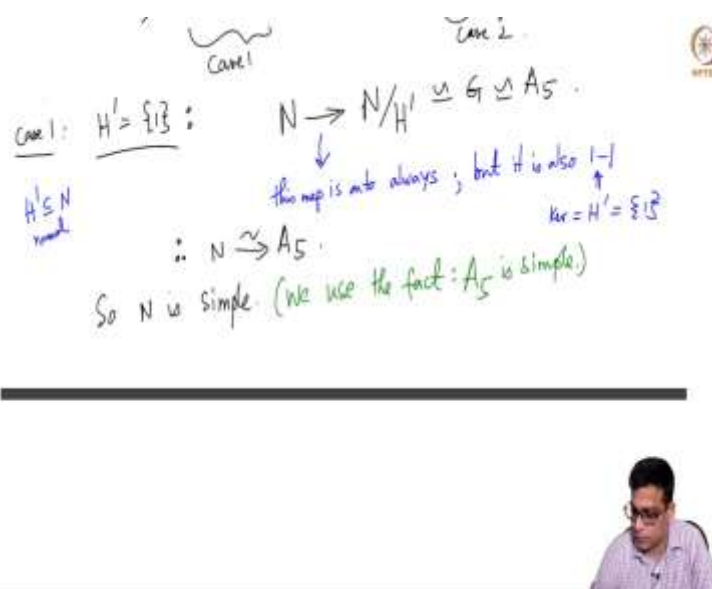
$$\begin{aligned}
 &\Rightarrow \varphi|_{H'}: H' \rightarrow G' \cong \mathbb{Z}/p\mathbb{Z} \\
 &\text{Hence: } H' \text{ is iso to a subgroup of } \mathbb{Z}/p\mathbb{Z} \quad (H' \hookrightarrow \mathbb{Z}/p\mathbb{Z}) \\
 &\Rightarrow \underbrace{H' = \{1\}}_{\text{Case 1}} \quad \text{OR} \quad \underbrace{H' \cong \mathbb{Z}/p\mathbb{Z}}_{\text{Case 2}}
 \end{aligned}$$



So, now consider the canonical map, I want to call this φ from N to $N \bmod H$; which we know is isomorphic to G prime. Canonical of this map is H , so restrict to φ , restrict to H prime; because H prime is in N , so H prime to $N \bmod H$. So, kernel of the restriction is the kernel of the original map intersected with H prime. Obviously, when you are restrict, it is all the things that go to u identity that are in H prime; but, this is $H \cap H$ prime. So, this means this is identity by the claim there. So, this implies φ restricted to H prime is a function from H prime to G prime, which is isomorphic to $\mathbb{Z} \bmod p \mathbb{Z}$ is injective.

Remember G prime is $\mathbb{Z} \bmod P \mathbb{Z}$, so $N \bmod H$ is isomorphic to G prime. So, H prime to that there is an injective homomorphism; hence we have 2 cases. H prime is the so H prime is isomorphic to a subgroup of $\mathbb{Z} \bmod P \mathbb{Z}$; this implies H prime is either $\mathbb{Z} \bmod P \mathbb{Z}$ is the group of order P , which is a prime number. So, it has only 2 subgroups; either H is trivial or H is equal to, or H prime is trivial or H prime is isomorphic to $\mathbb{Z} \bmod P \mathbb{Z}$. So, there are 2 cases; so this is case 1, this is case 2. So, H is either H prime is either trivial, so H prime sits inside $\mathbb{Z} \bmod P \mathbb{Z}$; so, that means H prime is either trivial or $\mathbb{Z} \bmod P \mathbb{Z}$.

(Refer Slide Time: 28:41)



So, case 1: H prime is trivial; if H prime is trivial, then let us look at this map. N to $N \bmod H$ prime which is G , which is by hypothesis A_5 ; so, now what can you say about this map? So, this map is onto always. This is the canonical map from a group to that group mod normal subgroup. So, this is onto, but it is also 1-1; why is this? This is because kernel is H prime which is identity. Kernel of this canonical map is H prime which is identity; that is the case that we are taking. So, we an onto map and which is injective map; so N is isomorphic to the alternating group A_5 , so N is simple. So, here we have to use the fact that which we have not proved; I have to prove this later with that A_5 is simple.

(Refer Slide Time: 30:08)

N does have a normal subgroup H s.t. $N/H \cong \mathbb{Z}/p\mathbb{Z}$.

$|H| \neq 1$
 $\neq 60$

$|N| = 60$
 $|N/H| = P \Rightarrow |H| = \frac{60}{P}$

So H is a proper, non-trivial normal subgroup of $N \cong A_5$.

This violates the fact that A_5 is simple.

So $H \not\cong \mathbb{Z}/p\mathbb{Z}$.

Cor 2: $H \cong \mathbb{Z}/p\mathbb{Z}$: $|N| = |G||H'| = 60P \Rightarrow |H| = 60$.

$G \cong A_5$
 $G \cong \mathbb{Z}/p\mathbb{Z}$

But, I claim that this is a problem because N does have a simple group, normal subgroup H . H is a normal subgroup of N , such that this H ; so maybe just I should draw the picture again here. So, you have K prime, K , F prime, F and this is N , this is H , this H prime; this is G which is A_5 , this is G prime which is $\mathbb{Z} \bmod P$ \mathbb{Z} really an isomorphism. So, N does have a subgroup, normal subgroup such that so H is not trivial obviously; because N is N has 60 elements.

So, kernelity of N is 60 and kernelity of is P ; so this implies kernelity of H is 60 by P . But, 60 by P is less than 60 and bigger than 1; so kernelity of H is not 1 and not 60. So, H is a proper non-trivial normal subgroup of N , which is A_5 . But, this violates the fact that A_5 is simple; simple means it has no non-trivial proper normal subgroups. But, N does not have a non-trivial proper normal subgroups; so, this case cannot occur, so H prime cannot be 1. Correct, so I hope this is clear; see H prime is trivial then you violated the simplicity of A_5 .

(Refer Slide Time: 32:23)

$$\begin{array}{l}
 N/H \cong G \\
 N/H \cong G \\
 \text{Now consider the canonical map: } N \xrightarrow{\psi} N/H \cong G. \\
 N \xrightarrow{\psi} G \quad \text{Ker}(\psi|_H) = (\text{Ker } \psi) \cap H = H' \cap H = \{1\} \\
 \begin{array}{c}
 H \\
 \downarrow \psi|_H \\
 H
 \end{array}
 \end{array}$$

$|H|/|G| = 1$
 $\therefore H$ is iso to a subgroup of G .
 But $|H| = 60 = |G|$



So, case 2 is H prime is $\mathbb{Z} \text{ mod } P \mathbb{Z}$; that means this $\mathbb{Z} \text{ mod } P \mathbb{Z}$. So, in this case we conclude that H must be $\mathbb{Z} \text{ mod } P \mathbb{Z}$. So, now let us just do some simple group theory. So, we know that order of N is order of H ; so because $N \text{ mod } H$ prime is isomorphic to G and $N \text{ mod } H$ is isomorphic to G prime. So, at the same this is order of H times order of G prime, this is what we have. And now this H prime by hypothesis is G is 60 because G is A_5 ; and H prime by this assumption is P , this is 60 times P . H is whatever it is and what is G prime? This is H prime; and G prime is $\mathbb{Z} \text{ mod } P \mathbb{Z}$ so this is P . So, G prime is $\mathbb{Z} \text{ mod } P \mathbb{Z}$; so this is P and this is H , these are equal.

So, this implies order of H is 60, so you have subgroup of N of order 60; and now we have done almost. So, now consider the canonical map N going to $N \text{ mod } H$ prime which is isomorphic to G ; so, $N \text{ mod } H$ prime is isomorphic to G . So, when we have N going to G ; I will omit that it is surjective, surjective; let me write onto. And now we have a subgroup H here and this goes to this. What is the so this is ψ and this is ψ restricted to H . What is the kernel of ψ ? So, this is ψ ; I do not need that onto but ψ .

So, what is the kernel of ψ restricted to H ? This is kernel of ψ restricted to H ; this is H prime intersected H this is 1. So, this is 1 minus 1, so ψ restricted to H just like in previous case; there we looked at N to $N \text{ mod } H$. And restricted to H prime and concluded that it is injective; so it is isomorphic to $\mathbb{Z} \text{ image } \mathbb{Z} \text{ mod } P \mathbb{Z}$. Here it is image is G . So, H is isomorphic to subgroup G . But,

what are the orders of this group? Order of H is 60 by just what we concluded here; which is also of course order of G because G is A5.

(Refer Slide Time: 35:30)

$$\begin{array}{ccc} H & \xrightarrow{1-1} & G \\ 60 & & 60 \end{array} \Rightarrow H \cong G \cong A_5. \quad \square$$

Let α be a root of f that is solvable over F :



So, you have an injective map from G to H to G, and both have order 60; so, this implies H is isomorphic to G as required. So, this is the claim that we made which is the claim that I have wrote here. For any Galois extension which is a prime whose degree is a prime number, if the K prime is the splitting field; then the Galois group is A5. Now, so this you may have forgotten the original situation what is it that we have? We want to prove that F is not solvable. We assumed to the contrary that F is solvable and we have this tower; so, let us now copy this tower. So, so if alpha is in K is a root of f that is solvable; so for a contradiction we assumed this. So, we have a tower like this, so I am going to write it like this.



So, you have F, F_1, F_2, F_3, F_r minus 1, F_r ; so this is the tower we have. And this is prime Galois and the degree is prime, Galois and the degree is prime, Galois and the degree is prime, this is Galois and degree is prime, Galois and degree is prime. This is now equivalence of the 4 characterization of radical extensions. If α is radical we can construct such a thing. Now, we have K which is the splitting field; so this is the splitting field of f over capital F . And this by hypothesis degree Galois is A5. Now, by the claim we have K_1 and what is this? This is a splitting field of f over F_1 ; so this is this picture here.

I am applying with F prime equal to F_1 and K as it is F as it is; and I have K prime which will be now called K_1 . So, this is a splitting field of the same polynomial over this larger field. But, this is A_5 , this statement is from by the claim; now let see where we are. Now, you forget the original situation K over F you forget; so you forget this part. F from is a field small f is a polynomial over that field; splitting field has Galois group A_5 and we took again Galois extension with F prime degree. That is important here, so this is a Galois extension F prime degree. So, we take the splitting field, so this is the splitting field of f over F_1 or F_2 now over F_2 now.

And by by the same claim that is A_5 ; so you can keep going like this. So, you have K_3 here and this was F_3 that would be K_3 ; and you have K_r minus 1 here; that will be A_5 also, and this will be A_5 also. At each stage we have a Galois extension with prime degree, Galois extension with prime degree. So, by repeatedly applying the claim, we get A_5 ; and finally we get K_r . So, just to make it abundantly clear K_r is the splitting field of f over F_r . And this is A_5 , because of the claim; so the claim is applied to this square.

Because f is a polynomial over capital F of minus 1 whose Galois group is A_5 , we took a Galois extension of F prime degree, took the splitting field of f over that extension; and what you get is F degree A_5 extension. But, this is now a problem, why is this a problem? This is a problem because so maybe I will write or write it here. Because f splits in F_r , because it has a root; the whole tower was constructed, so that the last field in the tower contains a root. So, f splits in that field, so f has a root in that field. So, it does not split completely; so all I will says that f is not irreducible in F_r . So, f is not irreducible in F_r because it has a root.

So, the Galois group of f , so that means we have f equals x minus α times f prime; where f prime is in F_r , and degree f prime is 4. So, the Galois is a splitting field of f over capital F_r minus F_r , which is of course K_r is the splitting field of. So, maybe I will rewrite it here.

(Refer Slide Time: 42:33)

$K_r = \text{sp fld of } f \text{ over } F_r = \text{sp fld of } f' \text{ over } F_r \dots$
 $f = (x - \alpha)f'$
 $\alpha \in F_r$
 $\Rightarrow \text{Gal}(K_r/F_r) \leq S_4$
 $\Rightarrow |\text{Gal}(K_r/F_r)| \leq 24$
 But $\text{Gal}(K_r/F_r) = A_5$, so has order 60.
 This is the contradiction we are looking for!
 Hence f is NOT solvable over F \square

So, K_r which is a splitting field of F_r of f over F_r is actually the splitting field of f prime over F_r . Because f 's factors as f times f prime x minus α times f prime; α is already in F_r . So, in order to attach all the roots of small f ; you just need to attach the roots of f prime. But, this means Galois K_r over F_r is a subgroup of S_4 ; because it is splitting field of a degree 4 polynomial, so it must be a subgroup of S_4 . This in particular means its degree its order is less than or equal to 24; but, we already established the Galois K_r over F_r is A_5 . So, has order 60, so this is the contradiction we need, we are looking for.

So, because f already has a root, you do not need a degree 60 extension to get all the other roots; in fact, you need at most a degree 24 for extension. So, if this is A_5 , this is A_5 , this is A_5 , this is A_5 , this will be A_5 ; so there is no tower like this. The conclusion is there is no tower like this and hence f is not solvable over capital F . If there is a tower like this F, F_1, F_2, F_3, F_r minus 1, F_r we are obtaining a contradiction; that is not solvable.

So, this completes the proof that any degree 5 polynomial whose Galois group is S_5 or A_5 is not solvable. So, we sort of take care of this; so we proved that we proved star here in a separate way. And the next we will address the question of whether, in fact they do exist such a polynomials or not. And next there are lot of such a polynomial will do that, and then we will start doing some problems.

So, this completes the proof that there are if, so I should not say there are quintics that are not solvable. But, it completes the proof that if there is a quintic polynomial whose Galois group is S_5 or A_5 . It cannot be solvable over that base field; so let me stop this here. In the next class we will see such examples of quintics whose Galois group is S_5 or A_5 . And thereby producing quintics that are not solvable and then we will go to some problem session. Thank you.