4/17

Wednesday, April 17, 2019 11:25

G - solvable

$H \leq G$, last time we claimed that $\exists$ a subnormal series

$H \trianglelefteq \cdots \trianglelefteq G$. But this is <u>wrong</u>!

eg: $G = S_3$, $H = \langle (1,2) \rangle$. $H \ntrianglelefteq G$, but there are no subgroups in between!

<u>Also claimed</u>:

E/F - Galois, $Gal(E/F) = G$ is polycyclic,

$F \subseteq K \subseteq E \Rightarrow K$ is a tower of simple cyclic extensions:

$K = L_n / L_{n-1} / \cdots / L_0 = F$

But this is also wrong!

<u>Correction</u> (New definition): K/F is <u>polycyclic</u> if it is a tower of simple cyclic extensions.

This implies that if E = galois closure of K/F, then E is also polycyclic (so solvable).

Remark: char $F > n \Rightarrow$ everything is separable automatically.

We need to adjoin $\overset{\omega}{\overset{\shortparallel}{\sqrt[n]{1}}}$ for some n.

We can adjoin this by adjoining roots of smaller degrees: i.e. $\sqrt[3]{1} = \frac{-1+\sqrt{-3}}{2}$, so adjoining $\sqrt{-3}$ is the same. (But who cares? - Leibman).

Corollary any pol-l of degree ≤ 4 is solvable in radicals. The general polynomial of degree ≥ 5 is not.

Proof If $\deg f = n$, $Gal(f) \leq S_n$

S_2, S_3, S_4 are solvable, S_5 is not.

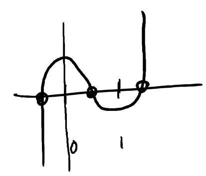
(neither is S_n for $n > 5$). $\quad 1 \triangleleft \underset{\substack{\uparrow \\ \text{simple} \\ \text{group,} \\ \text{not abelian.}}}{A_5} \triangleleft S_5$

General pol-l of degree n has $Gal \cong S_n$.

Example: $x^5 - 4x + 2 = f(x)$.

Claim: $f(x)$ is irreducible, has 3 real roots & 2 non-real roots.

$f'(x) = 5x^4 - 4$, has 2 zeroes.

$f =$ 

$f(0) = 2$, $f(1) < 0$, $f(+\infty) = +\infty$

Let K be the splitting field of f.

then $5 \mid [K:F]$.

So $5 \mid |G|$ where $G = Gal(K/\mathbb{Q})$.

So G contains a 5-cycle.

also, complex conjugation is in G & acts as transposition of 2 non-real roots of f.

If p is prime, $G \leq S_p$ that contains p-cycle & transposition, then $G = S_p$.

So $G = \mathrm{Gal}(f) \cong S_5$ which is not solvable, so f isn't solvable by radicals.

For the same reason, if p is prime & $f \in \mathbb{Q}[x]$ is of deg. p and has exactly 2 non-real roots, then $\mathrm{Gal}(f) \cong S_p$.

<u>Claim</u>: $\forall n$, $\exists f \in \mathbb{Q}[x]$ s.t. $\mathrm{Gal}(f) \cong S_n$.

$K = F(x_1, \dots, x_n)$, $L = \mathrm{Fix}(G)$, then $\mathrm{Gal}(K/L) = G$

$G \leq S_n$

<u>Conjecture</u>: $\forall$ finite gp G, $\exists f \in \underline{\underline{\mathbb{Q}}}[x]$ s.t. $\mathrm{Gal}(f) \cong G$.

G - solvable, finite

$1 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$

$\uparrow$ cyclic factors.

tower of cyclic extensions = radical extensions.

S_3, S_4. $\forall n$, $A_n \trianglelefteq S_n$, $|S_n : A_n| = 2$.

So $\forall f \in F[x]$, if K is the splitting field of f,

Let $G = Gal(f) = Gal(K/F) \leq S_n$.

If $G \not\leq A_n$, then $G \cap A_n$ has

index 2 in G, so $\exists$ $L \subseteq K$

s.t. $[L : F] = 2$.

$L = F(\delta)$, $\delta^2 \in F$.

Let $\alpha_1, \ldots, \alpha_n \in K$ be the roots of f.

δ is fixed by A_n, and $\forall$ odd $\sigma \in S_n$, $\sigma(\delta) = -\delta$.

$$\delta = \prod_{i<j} (\alpha_j - \alpha_i) = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)\cdots(\alpha_n - \alpha_1)(\alpha_3 - \alpha_2)\cdots(\alpha_n - \alpha_{n-1}).$$

$D = \delta^2 = \prod_{i<j} (\alpha_j - \alpha_i)^2$ is symmetric in αs,

So it is a pol-l in the coeffs of f. So $D \in F$.

($f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

then $a_k = \pm S_k(\alpha_1, \ldots, \alpha_n)$

$\uparrow$

k^{th} symmetric pol-l. $a_k \in F$. So $D \in F$.)

D is called Discriminant of f.

i.e. $n = 2$, $f = x^2 + ax + b$, α_1, α_2 - roots.

$$D = (\alpha_2 - \alpha_1)^2 = (\alpha_2 + \alpha_1)^2 - 4\alpha_1\alpha_2$$

$$= a^2 - 4b$$

$(s_1 = -a, \ s_2 = b)$

$n = 3$, $f = x^3 + ax^2 + bx + c$

$$D = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2$$

$y = x + \frac{a}{3} \Rightarrow f = y^3 + py + q$ for some p, q.

$D = D$, $D = -4p^3 - 27q^2$.

$n = 4$, we can do this, the formula is long.

For $n = 2$, $A_2 = 1$.

So either G is trivial (if $\sqrt{D} \in F$)

or $G \cong \mathbb{Z}_2$ (if $\sqrt{D} \notin F$).

Splitting field is $F(\sqrt{D})$.

roots are $\alpha = \frac{-a \pm \sqrt{D}}{2}$

In general, $Gal(f) \leq A_n$ iff $\sqrt{D} = \delta \in F$.

If $G = \mathrm{Gal} \leq A_n$ then G fixes $\sqrt{D}$ so $\sqrt{D} \in F$.

If $G \not\leq A_n$, then any odd $\sigma \in G$ maps $\sqrt{D} \mapsto -\sqrt{D}$.

$D = \prod_{j<i} (\alpha_i - \alpha_j)^2 \neq 0$ if f is separable