Pol eqs $\quad x^2+ax+b=0$

Cardano, Ferrari $\begin{cases} x^3+ax^2+bx+c=0 \\ x^4+\dots \end{cases}$

$x^5+\dots$

<u>Def</u> E/F is an extension by radicals if $\exists$ chain of subfields

$$F=F_0\subset F_1\subset\cdots\subset F_r=E$$

such that $F_i=F_{i-1}(\alpha_i)$, $\alpha_i^{n_i}\in F_{i-1}$ for some $n_i>0$.

<u>Note</u> If all $n_i=2$, then

$$(\alpha_1,\alpha_2,\dots,\alpha_r)$$

is a square-root sequence.

<u>Def</u> A pol $f(x)\in F[x]$ is solvable by radicals if the splitting field of $f(x)$ is contained in a field extension of F by radicals.

<u>Ex</u> $f(x)=x^n-1\in\mathbb{Q}[x]$ is solvable by radicals since $E=F(\zeta_n)$ is the splitting field and $F\subset F(\zeta_n)$, $\zeta_n^n=1\in F$ shows E/F is an extension by radicals.

Ex (General Pol Eqs).

$n=2$. F field, s,t indeterminates

$F(s,t) = \operatorname{Frac} F[s,t]$

The general quadratic pol is

$$f(x) = x^2 + sx + t$$

$f(x)$ is irr over $F(s,t)$ by RRT, Gauss:

($\pm 1, \pm t$ only divisors of t)

Let $E = F(s,t)(\alpha,\beta)$ be the splitting field: $x^2+sx+t = (x-\alpha)(x-\beta)$

$$\Rightarrow \quad -\alpha-\beta = s \qquad \text{(symmetric in } \alpha,\beta!)$$
$$\alpha\beta = t$$

So $\exists \sigma \in Gal(E/F(s,t))$. $\sigma(\alpha)=\beta$, $\sigma(\beta)=\alpha$, $\sigma|_{F(s,t)} = Id$

$[E : F(s,t)] = 2 \Rightarrow Gal(E/F(s,t)) \cong S_2$

$$\gamma = \alpha + \frac{s}{2} \Rightarrow \gamma^2 = \underbrace{\alpha^2 + s\alpha}_{=-t} + \frac{s^2}{4} = \frac{s^2-4t}{4}$$

Shows $F(s,t) \subset E = F(s,t)(\gamma)$ is an extension by radicals.

In general:

$$f(x) = x^n + s_1 x^{n-1} + \dots + s_n \in \overbrace{F(s_1,\dots,s_n)}^{\mathbb{F}}[x]$$

E = splitting field. $Gal(E/\mathbb{F}) \cong S_n$

Def A finite group G is <u>solvable</u> if $\exists$ seq of subgroups

$$1 = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_n = G$$

such that

i) $H_{i-1} \trianglelefteq H_i$ for $i = 1, 2, \ldots, n$ (Subnormal)

ii) H_i/H_{i-1} are abelian.

Remark In ii) "abelian" can be replaced by "cyclic": If H_i/H_{i-1} are all abelian, the seq can refined to a seq $1 = K_0 \leq \cdots \leq K_N = G$ s.t. K_j/K_{j-1} are all <u>cyclic</u>.

Examples. S_n is solvable $1 \leq n \leq 4$

$n = 3$: $\quad 1 \leq \langle (123) \rangle \leq S_3$

$$\langle (123) \rangle / 1 \cong \mathbb{Z}_3 \qquad S_3 / \langle (123) \rangle \cong \mathbb{Z}_2$$

$n = 4$:

$$\begin{array}{ccccccccc} 1 & \leq & \langle (12)(34) \rangle & \leq & N & \leq & A_4 & \leq & S_4 \\ 1 & & 2 & & 4 & & 12 & & 24 \end{array}$$

$$N = \{ (1), (12)(34), (13)(24), (14)(23) \} \trianglelefteq A_4$$
$$\cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

S_5 is NOT solvable:
$$1 \trianglelefteq A_5 \trianglelefteq S_5$$
A_5 simple and non-abelian!

<u>Lemma</u> Let F be a field of char $F = 0$. Let E be the splitting field of $f(x) = x^n - a \in F[x]$. Then $Gal(E/F)$ is solvable.

<u>Proof</u> The roots of $f(x)$ are
$$\sqrt[n]{a}, \ \sqrt[n]{a}\,\omega, \ \ldots, \sqrt[n]{a}\,\omega^{n-1}$$
where ω is a primitive n:th root of unity. $E = F(\sqrt[n]{a}, \omega)$

<u>Case 1</u>: $\omega \in F$. Claim: $Gal(E/F)$ is <u>abelian</u>. Let $\sigma, \tau \in Gal(E/F)$. Then
$$\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\,\omega^i, \quad \text{some } i$$
$$\tau(\sqrt[n]{a}) = \sqrt[n]{a}\,\omega^j, \quad \text{some } j$$
$$\sigma\tau(\sqrt[n]{a}) = \sigma(\sqrt[n]{a}\,\omega^j) \underset{\sigma|_F = id}{=} \sigma(\sqrt[n]{a})\,\omega^j = \sqrt[n]{a}\,\omega^{i+j}$$
Similarly $\tau\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\cdot\omega^{i+j}$. $\Longrightarrow \underline{\underline{\sigma\tau = \tau\sigma}}$

<u>Case 2</u>: $\omega \notin F$. Let $M = F(\omega)$.
$$F \subset M \subset E$$
Then M is the splitting field of $x^n - 1$.

So $\sigma, \tau \in Gal(E/F)$ permute the roots of $x^n - 1$:

$$\sigma(\omega) = \omega^i, \quad \tau(\omega) = \omega^j$$

Check $\sigma\tau(\omega) = \tau\sigma(\omega) \Rightarrow Gal(M/F)$ is abelian.

$$1 \leq Gal(E/M) \leq Gal(E/F)$$

$Gal(E/M)$ is abelian by previous argument ($\omega \in M$). And

$$\frac{Gal(E/F)}{Gal(E/M)} \underset{\substack{\uparrow \\ \text{Fund Th. Gal Th.}}}{\cong} Gal(M/F) \text{ abelian.}$$

$\Rightarrow Gal(E/F)$ is solvable.

Lemma F field, char $F = 0$. Let

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E$$

be a radical extension. Then there is a radical extension

$$F = K_0 \subset K_1 \subset \cdots \subset K_r = K$$

such that $K \supset E$ and K_i / K_{i-1} is Galois.

Thm Let $f(x) \in F[x]$, char $F = 0$. If $f(x)$ is solvable by radicals then $Gal(E/F)$ is solvable (E is the splitting field).

[**Remark**: Converse also holds.]

Proof Let

$$F = F_0 \subset F_1 \subset \cdots \subset F_n = E$$

be an extension by radicals. By Lemma, can assume E is the splitting field of $f(x)$ and F_i/F_{i-1} is Galois. By Fund Th. of Galois Theory $Gal(E/F_i) \trianglelefteq Gal(E/F_{i-1})$. So we get subnormal series

$$1 \leq Gal(E/F_{n-1}) \leq \cdots \leq Gal(E/F_1) \leq Gal(E/F).$$

and

$$Gal(E/F_{i-1})/Gal(E/F_i) \cong Gal(F_i/F_{i-1})$$

By lemma, $Gal(F_i/F_{i-1})$ is solvable. After refining (if nec.), we conclude $Gal(E/F)$ is solvable. ∎

Cor General quintic is not solvable by radicals, since its Galois grp is S_5.