Content:

Theorem	Galois Criterion. Let F be a field of characteristic 0 and $f \in F[x]$. Then f is solvable by radicals $\Leftrightarrow$ Gal(f/F) is solvable.
Definition	radical extension
Definition	solved by radicals
Definition	solvable group
Example	(1) Any abelian group is solvable. (2) S_3 is solvable.
Example	Determine Gal$(x^5 - 6x + 3/\mathbb{Q})$.
Lemma	Assume char $F = 0$, $\alpha \in F$, α is a primitive nth root of unity. If u is a root of $x^n - c$ in some extension of F, then $F(u)$ is normal over F and Gal$(F(u)/F)$ is abelian.

Theorem **Galois Criterion** Let F be a field of characteristic 0 and $f \in F[x]$. Then f is solvable by radicals $\Leftrightarrow$ Gal(f/F) is solvable.

Proof:
Assume f is solvable by radicals. Then ∃ a radical extension F ⊆ E such that the splitting field for f is contained in E.
Goal 1: Show ∃ a normal radical extension.
Goal 2: $F \subseteq K \subseteq E \Rightarrow$ Gal(E/F) is solvable.

Definition A field K is said to be a radical estension of F is there is a chain of fields $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = K$ such that $F_i = F_{i-1}(\sqrt[n_i]{u_i})$ for some $u_i \in F_{i-1}$.

Definition A polynomial $f(x) \in F[x]$ can be solved by radical if there is a radical extension of f that contains a splitting field for $f(x)$.

Definition A group G is solvable if there exists a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_n = \langle e \rangle$ such that $G_i \lhd G_{i-1}$ and G_{i-1}/G_i is abelian.

Example (1) Any abelian group is solvable.

Proof:
G abelian and $G \lhd \langle e \rangle \Rightarrow G$ is solvable.

(2) S_3 is solvable.

Proof:
$S_3 \lhd A_3 \lhd \langle e \rangle$.
$S_3/A_3 \cong Z_2$, which is abelian.
$A_3/\langle e \rangle \cong A_3$ which is abelian.
$\therefore$ S_3 is solvable.

Note This would not work for S_5 as A_5.

Example Let $f(x) = x^5 - 6x + 3$
Find Gal $(f/\mathbb{Q})$.

Gal$(f/\mathbb{Q}) \leq S_5$. Recall S_5 is generated by a 2-cycle and a 5-cycle.
Let α be a root of f. Let K be the splitting field for f.
Then $[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]$. And $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$. So $5 \mid |\text{Gal}(f/\mathbb{Q})|$
By Cauchy, $\exists\, \sigma \in \text{Gal}(f/\mathbb{Q})$ such that $\circ(\sigma) = 5$.
Since $\sigma \in S_5$ abd $\circ(\sigma) = 5$, then σ must be a 5-cycle.
You can show f has 3 real roots and 2 complex roots.
So $\exists\, \varphi \in \text{Gal}(\mathbb{C}/\mathbb{R})$ such that $\varphi(a + bi) = a - bi$.

Is $\varphi|_K \in \text{Gal}(K/\mathbb{Q})$? Is $\varphi|_K$ a 2-cycle?
$\varphi \in \text{Gal}(\mathbb{C}/\mathbb{R}) \Rightarrow \varphi: \mathbb{C} \to \mathbb{C}$ and $\circ(\varphi) = 2$ in Aut$(\mathbb{C})$.
In the proof of the FTGT we showed if $F \lhd K$, then $\varphi(K) = K$.
Thus $\exists\, \tau \in \text{Gal}(K/\mathbb{Q})$ such that τ is a transposition equal to $\varphi|_K$.
$\therefore$ Gal$(K/\mathbb{Q})$ contains a 2-cycle and a 5-cycle. So Gal$(K/\mathbb{Q}) \cong S_5$.

We need to show S_5 is not solvable.
Suppose it is.
Then $\langle e \rangle = G_n \lhd \cdots \lhd G_1 \lhd G_0 = S_5$ such that G_{i-1}/G_i is abelian.
If G/N is abelian, then
$g_1Ng_2N = g_2Ng_1N \Rightarrow g_1g_2N = g_2g_1N \Rightarrow g_1g_2g_1^{-1}g_2^{-1} \in N$.
Let (rst) and (uv) be disjoint cycles in S_5.
We know S_n/G is abelian, so
$(rst) = (tus)(srv)(tus)^{-1}(srv)^{-1} \in G_1$.
We proved G_1 contains all 3-cycles. Then since G_1/G_2 is abelian,
$(rst) = (tus)(srv)(tus)^{-1}(srv)^{-1} \in G_2$.
Continuing, we show G_n contains all 3-cycles,
but $G_n = \langle e \rangle$, clearly a contradiction.

We have shown S_n is not solvable for $n \geq 5$.

Lemma Assume char $F = 0$, $\alpha \in F$, α is a primitive nth root of unity.
If u is a root of $x^n - c$ in some extension of F, then $F(u)$ is normal over F
and Gal$(F(u)/F)$ is abelian.