From now on: $\mathrm{char}(F)=0$

Lemma 16.6. Let $b\in F$ and let E be the splitting field of $x^n-b\in F[x]$. Then $G(E/F)$ is solvable.

Proof. Let $w\in F$ be a primitive n-th root of unity and let $\alpha\in E$ be a root of x^n-b. Then $\alpha, w\alpha, \dots, w^{n-1}\alpha$ are all the roots of x^n-b. Assume first that $w\in F$. Then $E=F(\alpha)$. Let $\sigma_1,\sigma_2\in G(F(\alpha)/F)$. Clearly $\sigma_1(\alpha)$ and $\sigma_2(\alpha)$ are also roots of x^n-b and so $\sigma_1(\alpha)=w^i\alpha$, $\sigma_2(\alpha)=w^j\alpha$ for some $0\le i,j\le n-1$. Then

$$\sigma_1\sigma_2(\alpha)=\sigma_1(w^j\alpha)=\sigma_1(w)^j\sigma_1(\alpha)=w^j w^i\alpha=w^{j+i}\alpha=w^{i+j}\alpha=\sigma_2\sigma_1(\alpha).$$

Since $\sigma_1|_F=\mathrm{id}_F=\sigma_2|_F$ and $\sigma_1\sigma_2: F(\alpha)\to F(\alpha)$, we conclude that $\sigma_1\sigma_2=\sigma_2\sigma_1$ and so $G(E/F)$ is abelian. Hence $G(E/F)$ is solvable by Example 16.2(1).

Now assume that $w\notin F$. Since E is the splitting field of x^n-b, we have that $\alpha, w\alpha\in E$. Hence $w=w\alpha\alpha^{-1}\in E$. Since

$$F\subseteq F(w)\subseteq E$$

and $F\subseteq F(w)$ is normal (as the splitting field of $x^n-1\in F[x]$) and $F\subseteq E$ is Galois (since $\mathrm{char}(F)=0$), by FTGT(5) we obtain that $G(E/F(w))\lhd G(E/F)$. Since E is the splitting field of $x^n-a\in F(w)[x]$, we have by the first case that $G(E/F(w))$ is abelian. On the other hand, by FTGT(6) we have

$$G(E/F)/G(E/F(w))\cong G(F(w)/F)\overset{\text{Theorem 14.12(4)}}{\cong}\mathbb{Z}_n^\times$$

is abelian. We have shown that $G(E/F(w))\lhd G(E/F)$ and both $G(E/F(w))$ and $G(E/F)/G(E/F(w))$ are abelian and so solvable by Example 16.2(1). By Example 16.2(2) it follows that $G(E/F)$ is solvable. $\square$

Theorem 16.7. The following are equivalent.
(1) $f(x) \in F[x]$ is solvable by radicals.
(2) The Galois group of f is solvable.

Proof. Let E be the splitting field of f over F. Since $\mathrm{char}(F)=0$, F is perfect and so $F \subseteq E$ is Galois. It follows by FTGT(3) that $[E:F] = |G(E/F)|$ is finite, say $G := G(E/F) = \{\sigma_1, \dots, \sigma_n\}$.

(2) $\Rightarrow$ (1): Assume first that F contains a primitive n-th root of unity, say w. Then if $n = km$ we have that $w^k \in F$ is a primitive m-th root of unity. Since G is solvable, there exists a sequence

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\}$$

such that G_{i-1}/G_i is a cyclic group for $1 \le i \le r$. By FTGT there exist field extensions

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

such that $E_{G_i} = F_i$ and $G(E/F_i) = G_i$. Moreover, $G_1 \lhd G_0$ implies $F = F_0 \subseteq F_1$ is a normal extension. Since E is also the splitting field of $f(x) \in F_1[x]$, the extension $F_1 \subseteq E$ is also Galois. By induction, it follows that each extension $F_i \subseteq F_{i+1}$ is normal for $0 \le i \le r-1$. By FTGT(6) we have

$$G_{i-1}/G_i = G(E/F_{i-1})/G(E/F_i) \cong G(F_i/F_{i-1})$$

and since G_{i-1}/G_i is cyclic, $F_{i-1} \subseteq F_i$ is a cyclic extension. Let $m_i = [F_i : F_{i-1}]$. Then $[F_i : F_{i-1}] \mid [E:F]$ and so $m_i \mid n$. Since $F_i \supseteq F$ has a primitive m_i-th root of unity, we can apply Theorem 15.4 to obtain that F_i is the splitting field of an irreducible polynomial $x^{n_i} - b_i \in F_{i-1}[x]$ and $F_i = F_{i-1}(\alpha_i)$, where $\alpha_i^{n_i} = b_i \in F_{i-1}$. Hence

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = E$$
$$F_0(\alpha_1) \quad F_1(\alpha_2) \quad F_{r-1}(\alpha_r)$$

and $a_i^{n_i} \in F_{i-1}$ for $1 \le i \le r$, so f is solvable by radicals.
Now assume that F does not contain a primitive n-th root of unity. Let $w \in \overline{E}$ be a primitive n-th root of unity. Then $E(w)$ is the splitting field of $f(x) \in F(w)[x]$. Hence $F(w) \subseteq E(w)$ is a Galois extension. Consider the map

$$G(E(w)/F(w)) \longrightarrow G(E/F)$$
$$\sigma \longmapsto \sigma|_E.$$

This is well-defined by Theorem 8.5(3). Moreover, it is clearly a group homomorphism. Finally, it is injective since if $\sigma|_E = \tau|_E$ for $\sigma, \tau \in G(E(w)/F(w))$, then $\sigma|_{F(w)} = id_{F(w)} = \tau|_{F(w)}$ implies $\sigma(w) = w = \tau(w)$ and so σ and τ are equal in $E(w)$. Then $G(E(w)/F(w))$ is isomorphic to a subgroup of $G(E/F)$. Since subgroups of solvable groups are solvable (exercise) we conclude that $G(E(w)/F(w))$ is solvable. By the first case we have that $F(w) \subseteq E(w)$ is a radical extension. Since $F \subseteq F(w)$ is a pure extension, we conclude that $F \subseteq F(w) \subseteq E$ is a radical extension. Since $E \subseteq E(w)$, the claim follows.
(1) $\Rightarrow$ (2): We have that there exists a radical extension $F \subseteq E_r$ and $E \subseteq E_r$. Using Lemma 16.4, we may assume that we have a radical extension

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r$$

such that E_i is the splitting field of $x^{n_i} - b_i \in E_{i-1}[x]$ for $1 \le i \le r$, and $F \subseteq E_r$ is a normal extension. By FTGT we obtain

$$\{e\} \trianglelefteq G(E_r/E_{r-1}) \trianglelefteq \cdots \trianglelefteq G(E_r/F).$$

Moreover, for $1 \le i \le r$ FTGT(6) gives

$$G(E_r/E_{r-i})/G(E_r/E_{r-i+1}) \cong G(E_{r-i+1}/E_{r-i}),$$

which is solvable by Lemma 16.6. Applying repeatedly Example 16.2(2), we obtain that $G(E_r/E_i)$ is solvable for $1 \le i \le r$. In particular, $G(E_r/F)$ is solvable. But $F \subseteq E \subseteq E_r$ implies that

$$G(E/F) \cong G(E_r/F)/G(E_r/E)$$

and so $G(E/F)$ is the quotient of a solvable group. Since quotients of solvable groups are solvable (exercise), we have that $G(E/F)$ is solvable. □

Remark 16.8. Let $f(x) \in F[x]$ be a polynomial with Galois group equal to S_n for $n \geq 5$. Then f is not solvable by radicals. Such polynomials exist.

Definition 16.9 Let $H \leq S_n$ be a subgroup of S_n. We say that H is *transitive* if for all $i, j \in \{1, \dots, n\}$ there exists $\sigma \in H$ with $\sigma(i) = j$.

Theorem 16.10. Let $p \geq 2$ be prime and $H \leq S_p$ be transitive. If $\exists$ transposition $(a, b) \in H$, then $H = S_p$.

Proof. After relabelling we may assume $(1, 2) \in H$. For $i, j \in \{1, 2, \dots, p\}$ define $i \sim j \iff (i, j) \in H$. Clearly $\sim$ is an equivalence relation. Now let $\varphi \in H$ and let $\varphi(1) = i$. We obtain a map

$$\varphi : \bar{1} = \{j \in \{1, 2, \dots, p\} \mid (1, j) \in H\} \longrightarrow \bar{i} = \{j \in \{1, 2, \dots, p\} \mid (i, j) \in H\}$$

$$j \longmapsto \varphi(j)$$

which is a bijection since $(i, j) \in H \iff (i, \varphi(j)) = (\varphi(1), \varphi(j)) = \varphi \circ (1, j) \circ \varphi^{-1} \in H$.

Hence $|\bar{1}| = |\bar{2}| = \cdots = |\bar{p}| = k$ and so $\sim$ partitions $\{1, 2, \dots, p\}$ in sets of the same cardinality k. Hence $k \mid p$ and so $k = 1$ or $k = p$. Since $1, 2 \in \bar{1}$, we have $|\bar{1}| = |\bar{2}| = \cdots = |\bar{p}| = p$. But then all transpositions belong to H and so $H = S_p$.