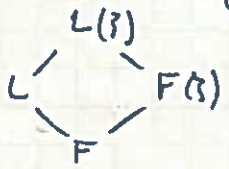
Solvable extensions, solvable groups.

Assumption All fields have char 0.

For $m \in \mathbb{Z}^+$, field L, $x^m - 1$ is separable with roots $1, \zeta, \dots, \zeta^{m-1}$ forming a cyclic group of order m. The splitting field is $L(\zeta)$, and $L(\zeta)/L$ is Galois and $\mathrm{Gal}(L(\zeta)/L)$ is Abelian. (Indeed, σ determined by $\sigma(\zeta) \in \{1, \dots, \zeta^{m-1}\}$.)

Consider



Lemma If L/F is Galois, then $L(\zeta)/F$ and $L(\zeta)/F(\zeta)$ are also Galois, and

$$\mathrm{Gal}(L/F) \text{ is solvable} \iff \mathrm{Gal}(L(\zeta)/F) \text{ is solvable} \iff \mathrm{Gal}(L(\zeta)/F(\zeta)) \text{ is solvable.}$$

Pf Check $L(\zeta)/F$ Galois (exc). so $L(\zeta)/F(\zeta)$ is Galois as well. For first equiv, get $\mathrm{Gal}(L(\zeta)/L) \trianglelefteq \mathrm{Gal}(L(\zeta)/F)$ with quotient $\cong \mathrm{Gal}(L/F)$. ↑ Abelian, hence solvable.

Thus $\mathrm{Gal}(L(\zeta)/F)$ solvable $\iff \mathrm{Gal}(L/F)$ solvable. ✓

Similarly, $\mathrm{Gal}(F(\zeta)/F) \cong \mathrm{Gal}(L(\zeta)/F) / \mathrm{Gal}(L(\zeta)/F(\zeta))$.

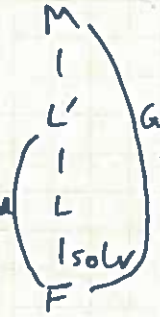
↑ Abelian, hence solvable, so $\mathrm{Gal}(L(\zeta)/F)$ solv $\iff$ ↑ solv. □

Lemma Suppose M/K Galois with $\mathrm{Gal}(M/K) \cong C_p$, p prime. If K contains a primitive p-th root of unity ζ, then $\exists \alpha \in M$ s.t. $M = K(\alpha)$ and $\alpha^p \in K$.

Pf Later if time. Read on p. 203.

Thm. L/F Galois. Then L/F solvable iff $\mathrm{Gal}(L/F)$ solvable

Pf ($\Rightarrow$) Reduce to the radical case:



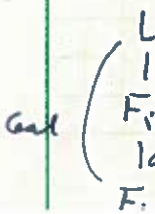
Suppose $\mathrm{Gal}(M/F)$ solvable. Then $\mathrm{Gal}(L/F)$ is a solvable gp since it's isomorphic to $\mathrm{Gal}(M/F)/\mathrm{Gal}(M/L)$. Thus it suffices to show $\mathrm{Gal}(M/F)$ solvable, i.e. we may assume L/F radical and Galois.

If we adjoin a primitive m-th root of unity ζ to F and L, get $L(\zeta)/F(\zeta)$ radical and Galois. Showing $\mathrm{Gal}(L(\zeta)/F(\zeta))$ solvable will imply $\mathrm{Gal}(L/F)$ solvable. So WLOG, F contains any m-th root of unity we want.

Take $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n = L$ witnessing L/F radical: $F_i = F_{i-1}(\gamma_i)$ with $\gamma_i^{m_i} \in F_{i-1}$. May assume F contains prim m_i-th root of unity, $i = 1, \ldots, n$. Claim F_i/F_{i-1} Galois with cyclic Galois group.

$\gamma_i, \zeta_i\gamma_i, \ldots, \zeta_i^{m_i-1}\gamma_i$ are the distinct roots of $x^{m_i} - \gamma_i^{m_i} \in F_{i-1}[x]$. Since $\zeta_i \in F \subseteq F_{i-1}$, we have $F_{i-1}(\gamma_i, \zeta_i\gamma_i, \ldots, \zeta_i^{m_i-1}\gamma_i) = F_{i-1}(\gamma_i) = F_i$, so F_i/F_{i-1} Galois. For $\sigma \in \mathrm{Gal}(F_i/F_{i-1})$, $\exists!\, 0 \le \ell \le m_i - 1$ s.t. $\sigma(\gamma_i) = \zeta_i^{\ell}\gamma_i$. For $C_{m_i} = \langle g \rangle$, $\sigma \mapsto g^{\ell}$ defines an injective hom $\mathrm{Gal}(F_i/F_{i-1}) \hookrightarrow C_{m_i}$. ~~$[F_i : F_{i-1}] = m_i$, so~~ Thus $\mathrm{Gal}(F_i/F_{i-1})$ is cyclic.

Now prove $\mathrm{Gal}(L/F)$ solvable. Let $G_i = \mathrm{Gal}(L/F_i) \le \mathrm{Gal}(L/F)$. Get $1 = \mathrm{Gal}(L/L) = \mathrm{Gal}(L/F_n) = G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = \mathrm{Gal}(L/F)$



$\Rightarrow G_i \trianglelefteq G_{i-1}$ with $G_{i-1}/G_i = \mathrm{Gal}(L/F_{i-1})/\mathrm{Gal}(L/F_i) \cong \mathrm{Gal}(F_i/F_{i-1})$, cyclic hence Abelian.

Cor of G solv $\Leftrightarrow$ $H, G/H$ solv is that filtration quotients solvable $\Rightarrow$ G solvable, so $\mathrm{Gal}(L/F)$ is solvable.

($\Leftarrow$) Let L/F be Galois with solvable Galois group.

Special case: F contains a primitive p-th root of unity $\forall$ prime $p \mid |\mathrm{Gal}(L/F)|$.

Now show L/F radical in this case: Take

$1 = G_n \trianglelefteq \cdots \trianglelefteq G_0 = \mathrm{Gal}(L/F)$ witnessing solvability.

Let $F_i = L^{G_i}$ to get

$$F = L^{\mathrm{Gal}(L/F)} = L^{G_0} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n = L^{G_n} = L^1 = L.$$

$G_i \trianglelefteq G_{i-1} \Rightarrow G_{i-1}/G_i \cong \mathrm{Gal}(F_i/F_{i-1}) \cong C_p$ for a prime p. Exc $p \mid |\mathrm{Gal}(L/F)|$. The lemma implies $F_i = F_{i-1}(\alpha)$ for $\alpha^p \in F_{i-1}$. Thus L/F radical.

Now consider the general case:

Let $m = |\mathrm{Gal}(L/F)|$, ζ a prim m-th root of unity. Then $\mathrm{Gal}(L(\zeta)/F(\zeta))$ is solvable.

$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(L(\zeta)/F) / \mathrm{Gal}(L(\zeta)/L))$

induced by $\mathrm{Gal}(L(\zeta)/F) \xrightarrow{\mathrm{res}_L} \mathrm{Gal}(L/F)$

$\uparrow$

$\mathrm{Gal}(L(\zeta)/F(\zeta))$ $\xrightarrow{\mathrm{res}_L}$ $\ker = 1$ b/c elts of ker are id on $LF(\zeta) = L(\zeta)$.

Thus $m = |\mathrm{Gal}(L(\zeta)/F(\zeta))| \mid \mathrm{Gal}(L/F)$. Take prime $p \mid m$. Then $\zeta^{m/p}$ is a primitive p-th root of unity, and $\zeta^{m/p} \in F(\zeta)$ so $L(\zeta)/F(\zeta)$ is in the special case, hence a radical extn. $F(\zeta)/F$ is radical, so $L(\zeta)/F$ is radical $\Rightarrow$ L/F solvable. $\square$

Cor L/F Galois of deg n, solvable, ζ a prim n-th root of 1. Then

Pf Lemma Take $\langle\sigma\rangle = Gal(M/K) \cong C_p$. Fix $\beta \in M \setminus K$.

Then for $i = 0, \dots, p-1$, consider the Lagrange resolvent

$$\alpha_i = \beta + \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta).$$

Then $\zeta^{-i}\sigma(\alpha_i) = \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta) + \underbrace{\zeta^{-ip}\sigma^p(\beta)}_{\beta}$

$\Rightarrow \zeta^{-i}\sigma(\alpha_i) = \alpha_i$

$\Rightarrow \sigma(\alpha_i) = \zeta^i \alpha_i$

$\Rightarrow \sigma(\alpha_i^p) = \zeta^{ip}\alpha_i^p = \alpha_i^p$.

$\Rightarrow \alpha_i^p \in M^{Gal(M/K)} = K$. Also $\alpha_0 \in K$.

Case 1 $\exists\ 1 \le i \le p-1$ s.t. $\alpha_i \neq 0$. Then $\zeta^i \neq 1$ so $\zeta^i \alpha_i \neq \alpha_i$

so $\sigma(\alpha_i) \notin \alpha_i$ so $\alpha_i \notin K$. Since $[M:K]$ prime, get

$M = K(\alpha_i)$ ✓

Case 2 $\alpha_i = 0$ for $1 \le i \le p-1$. Then

$$\alpha_0 = \alpha_0 + \alpha_1 + \cdots + \alpha_{p-1}$$

$$= \cdots\cdots = p\beta.$$

So $\beta = \alpha_0/p \in$ since $\alpha_0 \in K$, $\beta \notin K$. Thus we're always in case 1. □