I.J. Solvable groups and radical extensions

Let G be a group. In the event that it is a Galois group, we want criteria that will correspond to being able to build up the field extension by adjoining a sequence of roots, in order to solve the corresponding polynomial equations by radicals.

Normal and derived series.

I.J.1. DEFINITION. (i) A **normal series** for G is a sequence of subgroups of the form

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_m = \{1\}.$$

(Warning: $G_0 \geq G_2$ etc. need not be normal.)

(ii) G is **solvable** (or **soluble**) if it has a normal series with abelian quotients G_i/G_{i+1}.

I.J.2. EXAMPLES.

(A) Any finitely generated abelian group.

(B) Dihedral groups D_n: use $D_n \triangleright \mathbb{Z}_n \triangleright \{1\}$.

(C) p-groups: by [**Algebra I**, II.L.8], G has an index p normal subgroup G_1, the quotient by which is $\mathbb{Z}_p$. Iterate this observation.

(D) $\mathfrak{S}_3$ and $\mathfrak{S}_4$ are solvable: use the normal series

$$\mathfrak{S}_3 \triangleright \mathfrak{A}_3 \, (\cong \mathbb{Z}_3) \triangleright \{1\} \text{ and } \mathfrak{S}_4 \triangleright \mathfrak{A}_4 \triangleright V_4 \triangleright \{1\}.$$

(E) $\mathfrak{S}_5$ is *not*, because $\mathfrak{A}_5$ is its only normal subgroup, and $\mathfrak{A}_5$ itself is simple[30] and nonabelian. That $\mathfrak{S}_n$ is also non-solvable for $n \geq 6$ is then an immediate consequence of part (i) of the next result, since it has $\mathfrak{S}_5$ as a subgroup.

I.J.3. THEOREM. (i) *If G is solvable and $H \leq G$, then H is solvable.*

(ii) *Given $H \trianglelefteq G$, G is solvable $\iff$ H and G/H are solvable.*

Before we prove this, let's record some bits of the first and second isomorphism theorems that we will want to invoke: given groups

[30] This was [**Algebra I**, II.I.13].

$\mathsf{G}' \trianglelefteq \mathsf{G}$ and $\mathsf{H} \leq \mathsf{G}$, we have

$$\text{(I.J.4)} \qquad \mathsf{G}' \cap \mathsf{H} \trianglelefteq \mathsf{H} \;\text{ and }\; \mathsf{H}/(\mathsf{G}' \cap \mathsf{H}) \cong \mathsf{G}'\mathsf{H}/\mathsf{G}';$$

while if also $\mathsf{G}' \leq \mathsf{H}$ and $\mathsf{H} \trianglelefteq \mathsf{G}$, then

$$\text{(I.J.5)} \qquad \mathsf{G}' \trianglelefteq \mathsf{H}, \;\; \mathsf{H}/\mathsf{G}' \trianglelefteq \mathsf{G}/\mathsf{G}', \;\text{ and }\; (\mathsf{G}/\mathsf{G}')/(\mathsf{H}/\mathsf{G}') \cong \mathsf{G}/\mathsf{H}.$$

PROOF OF I.J.3(i). Start with a normal series for G, with terms $G_i \trianglelefteq G_{i-1}$. Setting $H_i := H \cap G_i$, we have

$$H_i = H \cap G_{i-1} \cap G_i = H_{i-1} \cap G_i \trianglelefteq H_{i-1}$$

by (I.J.4) (take $\mathsf{G} = G_{i-1}$, $\mathsf{G}' = G_i$, and $\mathsf{H} = H_{i-1}$), which also gives

$$H_{i-1}/H_i \cong H_{i-1}/(H_{i-1} \cap G_i) \cong G_i H_{i-1}/G_i \leq G_{i-1}/G_i.$$

Since G_{i-1}/G_i is abelian, so is H_{i-1}/H_i. □

The proof of part (ii) gets a little messy without introducing the **derived series** of G, which I'll do now.

I.J.6. DEFINITION. The **derived group** DG of G is the subgroup generated by all commutators $[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2$.

Here are some brief remarks on properties of derived groups:

- Of course, if G is abelian, then $DG = \{1\}$.
- Any homomorphism $\eta\colon G \to H$ restricts to a homomorphism $\eta|_{DG}\colon DG \to DH$ of derived groups, since η must send commutators to commutators. Clearly, if η is surjective, then $\eta(DG) = DH$.
- In particular, automorphisms of G restrict to automorphisms of DG; this implies that $DG \trianglelefteq G$, but if G has nontrivial outer automorphisms, this is a stronger statement than normality.
- Moreover, given a normal subgroup $K \trianglelefteq G$, we may restrict inner automorphisms (conjugation by elements) to K, obtaining a composition $\mathrm{Inn}(G) \to \mathrm{Aut}(K) \to \mathrm{Aut}(DK)$ which exhibits DK as a normal subgroup of G.
- In particular, taking $K = DG$, we get that $D^2G := D(DG)$ is normal in DG and G. Iteratively defining $D^kG := D(D^{k-1}G)$ gives a sequence of normal subgroups (in each other and in G).

I.J.7. DEFINITION. The **derived series** of G is

$$G \rhd DG \rhd D^2G \rhd D^3G \rhd \cdots .$$

That the successive quotients $D^kG/D^{k+1}G$ are abelian follows from the

I.J.8. LEMMA. *G/DG is abelian. In fact, DG is the intersection of all $K \trianglelefteq G$ for which G/K is abelian.*

PROOF. Given $g, h \in G$ and $K \trianglelefteq G$, we have

$$[gK, hK] = (gK)^{-1}(hK)^{-1}(gK)(hK) = [g,h]K.$$

Thus $DG \leq K \iff [g,h] \in K\,(\forall g,h) \iff [g,h]K = K\,(\forall g,h) \iff [gK, hK] = K\,(\forall g,h) \iff D(G/K) = \{1\} \iff G/K$ abelian. $\square$

While normal series sometimes have abelian quotients and always terminate at $\{1\}$, the derived series always has abelian quotients and sometimes terminates at $\{1\}$. The latter "sometimes" is the key to our whole problem:

I.J.9. PROPOSITION. *G is solvable $\iff$ $D^nG = \{1\}$ for some $n \geq 1$.*

PROOF. $\underline{(\Longleftarrow)}$: if some $D^nG = \{1\}$, then the derived series is a normal series (with abelian quotients). So G is solvable.

$\underline{(\Longrightarrow)}$: given $G = G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{1\}$ with abelian factors, we have $G_{k+1} \geq DG_k$ $(\forall k)$ by applying Lemma I.J.8 to subgroups of G_k (take $K = G_{k+1}$). So $G_2 \geq DG_1 = DG$, and inductively

$$G_k \geq D^{k-1}G \quad \Longrightarrow \quad G_{k+1} \geq DG_k \geq D(D^{k-1}G) = D^kG$$

for all k. But then $D^{m-1}G \leq G_m = \{1\}$. $\square$

We are ready to prove I.J.3(ii), and to give a shorter proof of (i):

PROOF OF THM. I.J.3. (i) If $H \leq G$, then $D^iH \leq D^iG$ $(\forall i)$. If G is also solvable, then $D^nG = \{1\}$ for some n and hence $D^nH = \{1\}$. Apply I.J.9.

(ii) $\underline{(\Longrightarrow)}$: If G is solvable, then H is by (i). Consider $\eta\colon G \twoheadrightarrow G/H$; applying the remarks after I.J.6, we have $\eta(DG) = D(G/H)$, and by iteration $\eta(D^kG) = D^k(G/H)$ $(\forall k)$. By I.J.8, for some n $\{1\} = \eta(\{1\}) = \eta(D^nG) = D^n(G/H)$, and thus G/H is solvable.

$\underline{(\Longleftarrow)}$: Again we just use I.J.9. If G/H is solvable, then for some k we have $D^k(G/H) = \{1\}$, and

$$\eta(D^kG) = D^k(G/H) = \{1\} \quad \Longrightarrow \quad D^kG \leq \ker(\eta) = H.$$

If H is also solvable, there exists an ℓ for which $\{1\} = D^\ell H \geq D^\ell(D^kG) = D^{\ell+k}G$, and G is solvable. □

Root towers.

It is now time to reveal the relation to field theory. Let L/K be an extension.

I.J.10. DEFINITION. (a) $\alpha \in L$ is **radical** over K if, for some n, α^n belongs to K.

(b) L/K is an **extension by radicals** (or **root tower**) if there is a sequence $L = L_s \supset \cdots \supset L_1 \supset L_0 = K$ such that $L_i = L_{i-1}(\alpha_i)$ $(\forall i)$, where α_i is radical over L_{i-1}. The minimal n_i for which $\alpha_i^{n_i} \in L_{i-1}$ are called the **orders** of the extension.

(c) A polynomial $f \in K[x]$ is **solvable by radicals** if there is an extension by radicals L/K over which f splits. (This could be bigger than a splitting field extension.) As in (b), we can speak of the *orders* of the radicals involved.

I.J.11. THEOREM. *Suppose $f \in K[x]$ is separable with solvable Galois group $\mathrm{Gal}_K(f)$, and that $\mathrm{char}(K) \not| \, |\mathrm{Gal}_K(f)|$. Then f is solvable by radicals.*

PROOF. Put $d := |\mathrm{Gal}_K(f)|$, let M/K be a SFE for $g := x^d - 1$, and write $\zeta \in M$ for a primtive d^{th} root of unity.[31] Since d is nonzero modulo $\mathrm{char}(K)$, $g' = dx^{d-1}$ and g are coprime, and (by I.E.3) the roots $1, \zeta, \zeta^2, \ldots, \zeta^{d-1}$ of g in M are distinct. This is the first step in our extension by radicals.

Let L/M be a SFE for f, and write $\mathcal{R}_f$ for the roots of f in L. Then $L = M(\mathcal{R}_f)$, and $L_0 := K(\mathcal{R}_f)$ is a splitting field for f over K. (Since

[31] Of course, if $K \subset \mathbb{C}$ then it's just $M = K(\zeta_d)$ and $\zeta = \zeta_d$.

both f and g are separable, L/K and all intermediate extensions are separable.) This is exactly the setting of the Theorem on Natural Irrationalities I.G.30 (with the simplification I.G.31 due to separability of f), which presents $\mathrm{Gal}_M(f) = \mathrm{Aut}(L/M)$ as a subgroup of $\mathrm{Gal}_K(f) = \mathrm{Aut}(L_0/K)$.

Since $\mathrm{Gal}_K(f)$ is solvable, so is $G := \mathrm{Gal}_M(f)$ by I.J.3. So we have a normal series

$$\{1\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_0 = G$$

with abelian quotients. In fact, by the FTFGAG (structure theorem) we may assume that the G_i/G_{i+1} are *cyclic*. By the Galois correspondence, applying Inv produces a tower

$$L = L_r \supset L_{r-1} \supset \cdots \supset L_0 = M$$

with

$$\mathrm{Aut}(L/L_j) = G_j \lhd G_{j-1} = \mathrm{Aut}(L/L_{j-1}).$$

Applying I.G.22(iv-v)[32] yields that L_j/L_{j-1} is a normal (hence Galois) extension with $\mathrm{Aut}(L_j/L_{j-1}) \cong G_{j-1}/G_j$ cyclic.

At this point it remains to show, for each j, that L_j may be obtained by adjoining a radical to L_{j-1}. Henceforth we fix any j and do just that. Write $\delta := |G_{j-1}/G_j| = [L_j{:}L_{j-1}|$, note that $\delta \mid d$ and $G_j/G_{j-1} = \langle \sigma \rangle \cong \mathbb{Z}_\delta$, and let $\omega \in M$ be a power of ζ which is a primitive δ^{th} root of 1.

Let $r \leq \delta$ be the smallest integer for which there exists a linear dependency $\sum_{k=1}^r \ell_k \sigma^{i_k}(\beta) = 0$ ($\ell_k \in L_j$, $0 \leq i_1 < \cdots < i_r < \delta$) valid for all $\beta \in L_j$. (Clearly $r \geq 2$.) Choose $\beta_0 \in L_j$ for which $\sigma^{i_1}(\beta_0) \neq \sigma^{i_r}(\beta_0)$, and take the difference of $\sum_{k=1}^r \ell_k \sigma^{i_k}(\beta\beta_0) = 0$ and $\sum_{k=1}^r \ell_k \sigma^{i_k}(\beta)\sigma^{i_r}(\beta_0) = 0$. The r^{th} terms of the sums cancel and we are left with a dependency (valid for all β) with fewer than r terms, contradicting the minimality of r.

So there is no such dependency, and there must exist $\beta \in L_j$ for which $\alpha := \sum_{i=0}^{\delta-1} \omega^i \sigma^i(\beta) \in L_j$ is nonzero. I claim that this is the

[32] We can replace "$H \trianglelefteq G$" there by $G_j \trianglelefteq G_{j-1}$, since L/L_{j-1} is Galois.

desired radical. First, notice that $\sigma(\alpha) = \sum_{i=0}^{\delta-1} \omega^i \sigma^{i+1}(\beta) = \omega^{-1}\alpha$ by reindexing. Hence $\sigma(\alpha^\delta) = \alpha^\delta \implies a := \alpha^\delta \in L_{j-1} \implies \alpha$ is indeed radical over L_{j-1}.

Observe next that $x^\delta - a = \prod_{i=0}^{\delta-1}(x - \omega^i \alpha)$ has splitting field $L_{j-1}(\alpha)$ over L_{j-1}. This factorization has to work because the $\{\omega^i\alpha\}$ are all roots, and distinct. But $1, \sigma, \ldots, \sigma^{\delta-1}$ are also distinct, and belong to $\mathrm{Aut}(L_{j-1}(\alpha)/L_{j-1})$, making

$$[L_{j-1}(\alpha){:}L_{j-1}] = |\mathrm{Aut}(L_{j-1}(\alpha)/L_{j-1})| \geq \delta.$$

Hence $L_{j-1}(\alpha) = L_j$ and we are done. □

Composition series.

That was a long proof, but I thought it important to see some light at the end of the tunnel. To get a shorter proof of this Theorem, as well as its converse, we need to introduce one more group theory concept (which also has a module-theoretic version that is used in commutative algebra and representation theory).

I.J.12. DEFINITION. A **composition series** for G is a normal series such that each G_{i+1} is *maximal* normal in G_i: that is, there does not exist H with $G_i \triangleright H \triangleright G_{i+1}$ and $H \neq G_{i+1}, G_i$. Equivalently (by (I.J.5)), each **composition factor** G_i/G_{i+1} is simple.

Let G be a finite group. Then a composition series certainly exists by taking successive maximal proper normal subgroups.

I.J.13. THEOREM (Jordan-Hölder). *If $\{G_i\}_{i=0}^s$ and $\{H_j\}_{j=0}^t$ are two composition series for G, then they have the same set of composition factors, up to isomorphism and reordering.*

PROOF. Induce on $|G|$. Call two CS *equivalent* if the statement of the Theorem holds (because it's an equivalence relation!). Note that $G_0 = G = H_0$. If $G_1 = H_1$ we are done by induction.

So assume $G_1 \neq H_1$. Clearly neither can contain the other, by *maximal* normality of G_1, H_1 in G. Together with $G_1, H_1 \leq G_1H_1 \trianglelefteq G$, this maximality forces $G_1H_1 = G$. By (I.J.4),

$$G/G_1 = G_1H_1/G_1 \cong H_1/(G_1 \cap H_1) \text{ and} \\ G/H_1 = G_1H_1/H_1 \cong G_1/(G_1 \cap H_1)\,; \tag{I.J.14}$$

and by (I.J.5), this gives that $K_2 := G_1 \cap H_1$ is maximal normal in H_1 and in G_1. Writing (I.J.14) in the form

$$G_0/G_1 \cong H_1/K_2 \;\text{ and }\; H_0/H_1 \cong G_1/K_2, \tag{I.J.15}$$

and appending to these a CS for K_2, yields two CS for G (both of the same length u) — in addition to the original $\{G_i\}$ and $\{H_j\}$.

Now $G_0 \rhd G_1 \rhd K_2 \rhd \cdots K_u = \{1\}$ and $G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_s = \{1\}$ have the same G_1, and these CS are equivalent by induction. The same goes for $H_0 \rhd H_1 \rhd K_2 \rhd \cdots K_u = \{1\}$ and $H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_s = \{1\}$. Finally, $G_0 \rhd G_1 \rhd K_2 \rhd \cdots K_u = \{1\}$ and $H_0 \rhd H_1 \rhd K_2 \rhd \cdots K_u = \{1\}$ are equivalent because the first two composition factors satisfy (I.J.15), and the later ones K_i/K_{i+1} are the same. By transitivity, $\{G_i\}$ and $\{H_j\}$ are equivalent. □

So we can speak unambiguously of *the* composition factors of a finite group.

I.J.16. THEOREM. *G is solvable $\iff$ its composition factors are cyclic of prime order.*

PROOF. $\underline{(\implies)}$: If G is solvable, so are its subquotients; in particular, the composition factors G_i/G_{i+1} in a CS are solvable. By definition, they are also simple, and so their only normal series is the trivial one $G_i/G_{i+1} \rhd \{1\}$. So if they are solvable, they must be abelian. But then, if they are simple, by the p-primary version of the FTFGAG [**Algebra I**, IV.C.13] they must have prime order.

$\underline{(\impliedby)}$: Obviously cyclic groups of order p are abelian. □

Galois's Theorem.

Let $f \in K[x]$ be a separable polynomial of degree n, with splitting field extension L_0/K of degree d not divisible by $\text{char}(K)$. The latter is Galois, so $\text{Gal}_K(f) = \text{Aut}(L_0/K)$ has fixed field K, and

$|\mathrm{Gal}_K(f)| = [L_0{:}K] =: d$. Moreover, through its action on $\mathcal{R}_f$, we may regard $\mathrm{Gal}_K(f)$ as a subgroup of $\mathfrak{S}_n$, which is transitive if f is irreducible. We are going to show that solubility of $\mathrm{Gal}_K(f)$ is equivalent to solubility of f by radicals, with some added caveats in positive characteristic.

It is useful to adopt the terminology that a Galois extension is **abelian** [resp. **cyclic**] if its automorphism group is. For instance, the next statement makes precise the notion that "cyclotomic extensions are abelian".[33]

I.J.17. LEMMA. *Let* $f := x^n - 1$ *and* K *be a field. Then* $\mathrm{Gal}_K(f) \leq \mathbb{Z}_n^*$*; in particular, the SFE is abelian.*

PROOF. First assume $\mathrm{char}(K) \nmid n$. We then have $\gcd(f, f') \sim 1$, so the roots $\mathcal{R}_f = \{\zeta^j\}_{j=0}^{n-1} \subset L_0 = K(\zeta)$ are distinct; and $\mathbb{Z}_n \cong \mathcal{R}_f \leq K(\zeta)^*$ as groups $\implies \mathrm{Gal}_K(f) \leq \mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ by I.G.26.

If $\mathrm{char}(K) = p \mid n$, then write $n = p^k m$ $(p \nmid m)$ and $f = (x^m - 1)^{p^k} =: g^{p^k}$. Then we are back in the above case (with f, n replaced by g, m). Obviously f is separable; and $\mathbb{Z}_m^*$ is a subgroup of $\mathbb{Z}_n^*$. □

I.J.18. LEMMA. *Suppose* K *contains* n *distinct* n^{th} *roots of* 1*, and* $a \in K^*$*. Then* $f := x^n - a$ *is separable/*K *with* $\mathrm{Gal}_K(f) \cong \mathbb{Z}_m$ *for some* $m \mid n$ *(with* $m = n \iff f$ *irreducible/*K*). In particular, the SFE is cyclic.*

PROOF. Write $\langle\zeta\rangle \subset K$ for the n^{th} roots of 1, whose existence imply $\mathrm{char}(K) \nmid n$ ($\implies f$ separable), and $\alpha \in L_0$ for an n^{th} root of a. Then $\mathcal{R}_f = \langle\zeta\rangle\alpha \subset L_0 \implies L_0 = K(\alpha) \implies \sigma \in \mathrm{Aut}(L_0/K)$ is determined by $\sigma(\alpha) = \zeta^{j(\sigma)}\alpha$. This presents $\mathrm{Aut}(L_0/K)$ as a subgroup of $\mathbb{Z}_n$, hence cyclic of order $m \mid n$. By I.G.17, f is irreducible $\iff \mathrm{Aut}(L_0/K)$ acts transitively on the roots $\iff m = n$. □

The next result gives a sort of converse. Its proof demonstrates that the construction of the radicals in the proof of I.J.11 above simplifies greatly when δ is a prime p.

[33] I should add that it is important in number theory (esp. class field theory) that *all* abelian extensions of $\mathbb{Q}$ are contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$; this is the *Kronecker-Weber theorem.*

I.J.19. LEMMA. *Suppose a field K contains p distinct p^{th} roots of* 1, *and L/K is cyclic* (*Galois*) *of degree p. Then $L = K(\alpha)$, with $\alpha^p \in K$.*

PROOF. Write $\{\zeta^i\}_{i=0}^{p-1} \subset K$ for the p^{th} roots. Any $\beta \in L \setminus K$ gives $K(\beta) = L$ since $[L{:}K]$ is prime. Set $\alpha_i := \sum_{j=0}^{p-1} \zeta^{ij}\sigma^j(\beta)$, and note that $\sigma(\alpha_i) = \zeta^{-i}\alpha_i$. So $\sigma(\alpha_i^p) = \alpha_i^p \implies \alpha_i^p \in K$ $(\forall i)$.

Notice that the matrix (ζ^{ij}) relating the $\{\sigma^j(\beta)\}$ and $\{\alpha_i\}$ has (Vandermonde) determinant $\prod_{0\leq i<j<p}(\zeta^j - \zeta^i) \neq 0$, so is invertible. Thus we can write β as a K-linear combination of the $\{\alpha_i\}$, which means that *some* $\alpha_{i_0} =: \alpha \notin K$. Clearly, $K(\alpha) = L$. □

I.J.20. LEMMA. *Let L/K be a finite separable extension, L^c a normal closure. Then the conjugates $\{\sigma(L) \mid \sigma \in \mathrm{Aut}(L^c/K)\}$ generate L^c/K.*

PROOF. Let L' be the subfield of L^c they generate. It is closed under $\mathrm{Aut}(L^c/K)$. Since the fixed field of $\mathrm{Aut}(L^c/K)$ is K, the fixed field of $\mathrm{Aut}(L^c/K)|_{L'} \leq \mathrm{Aut}(L'/K)$ is also K, and so L'/K is normal. Conclude that $L' = L^c$. □

I.J.21. LEMMA. *Let L/K be a separable extension by radicals. Then L^c is an extension by radicals, whose orders equal or divide those of L/K.*

PROOF. In the notation of I.J.10, we have $L = K(\alpha_0, \ldots, \alpha_{s-1})$. By I.G.20, $L^c = K(\{\sigma(\alpha_0), \ldots, \sigma(\alpha_{s-1})\}_{\sigma\in\mathrm{Aut}(L^c/K)})$. Adjoining all the $\sigma(\alpha_0)$'s (one by one), then the $\sigma(\alpha_1)$'s, and so forth, we obtain the desired root tower. □

I.J.22. GALOIS'S THEOREM. *Given a polynomial $f \in K[x]$:*

(A) *If f is solvable by radicals of orders*[34] *coprime to* $\mathrm{char}(K)$, *then* $\mathrm{Gal}_K(f)$ *is solvable* (*and f is separable*).

(B) *If f is separable/K,* $\mathrm{char}(K) \not| |\mathrm{Gal}_K(f)|$, *and* $\mathrm{Gal}_K(f)$ *is solvable, then f is solvable by radicals* (*of orders coprime to* $\mathrm{char}(K)$).

[34] Note that "orders" are the powers of the radicals that belong to the previous step in the root tower, not necessarily the degree of the field extension it yields. This distinction really matters for roots of 1, and is why we don't get $\mathrm{char}(K) \not| |\mathrm{Gal}_K(f)|$ in (A).

PROOF. **(A)** We are given a root tower L/K, containing a splitting field L_0 for f, that arises by adjoining roots of orders δ_i not divisible by $p := \mathrm{char}(K)$. These extensions are obviously separable, and thus so is the whole tower. (Clearly, f is separable$/K$ because it splits over a separable extension of K.) Writing $\delta := \mathrm{lcm}(\{\delta_i\})$, $x^\delta - 1$ is also separable (as $p \nmid \delta$) and we may assume the tower "begins" by adjoining δ distinct δ^{th} roots of 1. Finally, by Lemma I.J.21, we may assume that L/K is Galois.

Now observe that each step in the tower is abelian and normal by Lemmas I.J.17-I.J.18. (Clearly, it's crucial that we add the roots of 1 *first*!) So under the Galois correspondence (applying $\mathrm{Aut}(L/\cdot)$), the successive subgroups are normal, with abelian quotients, proving that $\mathrm{Aut}(L/K)$ is solvable. Since L_0/K is normal (being a SFE), we have $\mathrm{Aut}(L/L_0) \trianglelefteq \mathrm{Aut}(L/K)$, and according to I.J.3 $\mathrm{Aut}(L_0/K) \cong \mathrm{Aut}(L/K)/\mathrm{Aut}(L/L_0)$ is also solvable.

(B) Begin as in the proof of I.J.11: put $d := |\mathrm{Gal}_K(f)|$ and $p := \mathrm{char}(K) \nmid d$. Let M/K be obtained by adjoining a primitive d^{th} root of unity ζ (where we recall that ζ has d distinct powers since $p \nmid d$). Then let L [resp. $L_0 \subset L$] be a SFE for f over M [resp. K]. Again I.G.30 $\implies$ $\mathrm{Gal}_M(f) \leq \mathrm{Gal}_K(f)$ $\implies$ $G := \mathrm{Gal}_M(f)$ solvable of order dividing d. Now comes the simplification.

Invoking I.J.16, G has a composition series with cyclic factors of prime orders p_i dividing d. Applying Inv yields a tower of cyclic (Galois) extensions of degrees p_i. Since powers of ζ furnish the required p_i^{th} roots of 1, I.J.19 says that the i^{th} step in the tower is obtained by adjoining a p_i^{th} root. Hence f is solvable by radicals of orders coprime to p. □

I.J.23. COROLLARY. *If* $\mathrm{char}(K) = 0$, *then* $f \in K[x]$ *is solvable by radicals* $\iff$ $\mathrm{Gal}_K(f)$ *is solvable.*

To state the obvious, this means that any cubic or quartic polynomial over $\mathbb{Q}$ is solvable by radicals, but a quintic with Galois group $\mathfrak{S}_5$ or $\mathfrak{A}_5$ is not.

I.J.24. REMARK. To see how I.J.22(B) might fail in positive characteristic without the extra conditions, consider $f(x) = x^p - x - t \in K[x]$ where $K = \mathbb{Z}_p(t)$. This is obviously separable (consider f'); and by the same argument as in I.H.10, f is irreducible, is split by adjoining a single root β (then $\mathcal{R}_f = \beta + \mathbb{Z}_p \subset L_0 = K(\beta)$), and has $\text{Gal}_K(f) \cong \mathbb{Z}_p$. But the characteristic does divide the order of the Galois group (they're equal), and f actually fails to be solvable by radicals!

How can that be? Well, we need to fit a degree-p extension inside a root tower. You can separate root towers into prime-order ones by adjoining successively smaller powers of your root. By the Tower Law, one of these steps must have order p. In fact, it must be an "order p" step that splits f: in the tower there must be $J(\alpha) \supset J$ with $\alpha^p \in J$, such that $J \cap L_0 = K$ and $J(\alpha) \supset L_0$. But this is impossible: β would have to take the form $h(\alpha)$, $h \in J(x)$; and then $\beta = \beta^p - t = h(\alpha)^p - t = \phi(h)(\alpha^p) - t \in J$, a contradiction.

For this reason, in characteristic-p root-towers a special allowance is sometimes made for the extensions generated by this sort of polynomial, called *Artin-Schreier extensions*. On the other hand, there is no reason to do this over finite fields. If K is finite, then *any* $f \in K[x]$ *is solvable by radicals*, because (as we know) any extension of finite fields is cyclic.