9.0 Solvable Groups

What other properties fit into our dictionary between intermediate fields and subgroups of a Galois group? Today we explore a property of groups.

9.0.0 Definition. A finite group G is *solvable* if there are subgroups

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$

such that, for all $1 \leqslant j \leqslant n$, the subgroup G_j is normal in G_{j-1} and the index $[G_{j-1} : G_j]$ is prime.

The index condition is equivalent to the quotient group $G_{j-1} \big/ G_j$ being a cyclic group of prime order.

9.0.1 Remark. The chain $\langle \mathrm{id}_{[3]} \rangle \subset A_3 \subset \mathfrak{S}_3$ of subgroups shows that $\mathfrak{S}_3$ is solvable, because each subgroup is normal in the next, and the indices are $[A_3 : \langle \mathrm{id}_{[3]} \rangle] = 3$, and $[\mathfrak{S}_3 : A_3] = 2$.

9.0.2 Proposition. *Every subgroup of a solvable finite group is solvable.*

Proof. Let G be solvable finite group. There exists subgroups

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$

such that, for all $1 \leqslant j \leqslant n$, G_j is normal in G_{j-1} and $[G_{j-1} : G_j]$ is prime. For each subgroup $H \subseteq G$, set $H_j \coloneqq G_j \cap H$. In particular, we have $H_0 = G \cap H = H$, and $H_n = \{e\} \cap H = \{e\}$. The composition of the inclusion and the quotient map is the group homomorphism $\pi \colon H_{j-1} \to G_{j-1} \big/ G_j$ defined by $h \mapsto hG_j \in G_{j-1} \big/ G_j$ for all $h \in H_{j-1}$. An element $h \in H_{j-1}$ belongs to $\operatorname{Ker}(\pi)$ if and only if $hG_j = G_j$ or equivalently $h \in H_{j-1} \cap G_j = (G_{j-1} \cap H) \cap G_j = H \cap G_j = H_j$. It follows that $\operatorname{Ker}(\pi) = H_j$ and H_j is a normal subgroup in H_{j-1}. The First Isomorphism Theorem gives

$$H_{j-1} \big/ H_j = H_{j-1} \big/ \operatorname{Ker}(\pi) \cong \operatorname{Im}(\pi) \subseteq G_{j-1} \big/ G_j \,.$$

Since $G_{j-1} \big/ G_j$ is cyclic of prime order, we see that $H_{j-1} \big/ H_j$ is either trivial or isomorphic to $G_{j-1} \big/ G_j$. It follows that either $H_{j-1} = H_j$ or $[H_{j-1} : H_j]$ is prime. By discarding any duplicates, the subgroups

$$\{e\} = H_n \subset H_{n-1} \subset \cdots \subset H_1 \subset H_0 = H$$

show that H is solvable. □

9.0.3 Theorem. *Let G be a finite group and let H be a normal subgroup. The group G is solvable if and only if H and $G \big/ H$ are solvable.*

Proof. Suppose that the finite group G is solvable. The previous proposition establishes that H is solvable. Moreover, there exists subgroups $\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$ such that, for all $1 \leqslant j \leqslant n$, G_j is normal in G_{j-1} and $[G_{j-1} : G_j]$ is prime. Let $\pi \colon G \to G \big/ H$ be the quotient map, and set $\widetilde{G}_j \coloneqq \pi(G_j)$ for all $0 \leqslant j \leqslant n$. Observe that $\widetilde{G}_0 = G \big/ H$ because $G_0 = G$. Similarly, $G_n = \{e\}$ implies that $\widetilde{G}_n = \{H\}$, where the coset $H = eH$ is the identity in $G \big/ H$. Since G_j is normal in G_{j-1}, the Correspondence Theorem shows that $\widetilde{G}_j$ is normal in $\widetilde{G}_{j-1}$. Moreover, the Induced Map Lemma shows that the map $G_{j-1} \big/ G_j \to \widetilde{G}_{j-1} \big/ \widetilde{G}_j$ defined by

$gG_j \mapsto \pi(g)\widetilde{G}_j$ is a well-defined surjective group homomorphism. The hypothesis that $G_{j-1} \big/ G_j$ is a group of prime order implies that $\widetilde{G}_{j-1} \big/ \widetilde{G}_j$ is either trivial or has prime order, so either $\widetilde{G}_{j-1} = \widetilde{G}_j$ or $[\widetilde{G}_{j-1} : \widetilde{G}_j]$ is prime. By discarding duplicates, the subgroups

$$\{H\} = \widetilde{G}_n \subset \widetilde{G}_{n-1} \subset \cdots \subset \widetilde{G}_1 \subset \widetilde{G}_0 = G \big/ H$$

show that $G \big/ H$ is solvable.

Conversely, suppose that H and $G \big/ H$ are solvable. There exists subgroups $\{H\} = \widetilde{G}_n \subset \widetilde{G}_{n-1} \subset \cdots \subset \widetilde{G}_1 \subset \widetilde{G}_0 = G \big/ H$ such that, for all $1 \leqslant j \leqslant n$, $\widetilde{G}_j$ is normal in $\widetilde{G}_{j-1}$ and $[\widetilde{G}_{j-1} : \widetilde{G}_j]$ is prime. Let $\pi \colon G \to G \big/ H$ be a the quotient map. By the Correspondence Theorem, the preimages are subgroups of G such that

$$H = \pi^{-1}(\{H\}) \subset \pi^{-1}(\widetilde{G}_{n-1}) \subset \cdots \subset \pi^{-1}(\widetilde{G}_1) \subset \pi^{-1}(G \big/ H) = G$$

where, for all $1 \leqslant j \leqslant n$, the subgroup $\pi^{-1}(\widetilde{G}_j)$ is normal in $\pi^{-1}(\widetilde{G}_{j-1})$ and $[\pi^{-1}(\widetilde{G}_{j-1}) : \pi^{-1}(\widetilde{G}_j)] = [\widetilde{G}_{j-1} : \widetilde{G}_j]$. Since H is solvable, there also exists subgroups $\{e\} = H_m \subset H_{m-1} \subset \cdots \subset H_1 \subset H_0 = H$ such that, for all $1 \leqslant k \leqslant m$, H_{m-1} is normal in H_m and $[H_{m-1} : H_m]$ prime. Concatenation gives

$$\{e\} \subset H_{m-1} \subset \cdots \subset H_1 \subset H \subset \pi^{-1}(\widetilde{G}_{n-1}) \subset \cdots \subset \pi^{-1}(\widetilde{G}_1) \subset G$$

which demonstrates that G is solvable. □

9.0.4 Corollary. *Every finite abelian groups is solvable.*

Proof. Let G be a finite abelian group. We proceed by induction on $|G|$. The base case $|G| = 1$ is trivial. Assume that $|G| > 1$. Let p be a prime divisor of $|G|$. When $p = |G|$, the group G is cyclic of order p and thereby solvable as witnessed by $\{e\} \subset G$. If $P < |G|$, then Cauchy's Theorem for group theory implies that there exists $g \in G$ of order p. Let $H := \langle g \rangle$. Since G is abelian, H is normal. In this case, the orders of H and $G \big/ H$ are stictly smaller than $|G|$. The induction hypothesis ensures that H and $G \big/ H$ are solvable. Thus, today's theorem implies that G is solvable. □

9.1 Radical and Solvable Extensions

What is the field-theoretic counterpart to solvable groups?

9.1.0 Definition. A field extension $K \subseteq K$ is *radical* if there exist intermediate fields $K = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = L$ where, for all $1 \leqslant j \leqslant n$, there exists $\gamma_j \in K_j$ such that $K_j = K_j(\gamma_j)$ and $\gamma_j^{m_j} \in K_{j-1}$ for some positive $m_j \in \mathbb{N}$.

9.1.1 Remark. Setting $b_j := \gamma_j^{m_j} \in K_{j-1}$, we see that γ_j is an m_jth root of b_j, so $\gamma_j = \sqrt[m_j]{b_j}$ and $K_j = K_{j-1}(\sqrt[m_j]{b_j})$ where $b_j \in K_{j-1}$. Thus, radical extensions are obtained by adjoining successive radicals.

9.1.2 Remark. Consider the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2+\sqrt{2}})$. Let $\gamma_1 := \sqrt{2}$ and $\gamma_2 := \sqrt{2+\sqrt{2}}$. It follows that

$$\mathbb{Q} \subset \mathbb{Q}(\gamma_1) = \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \gamma_2) = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})\,.$$

where $\gamma_1^2 = 3 \in \mathbb{Q}$ and $\gamma_2^2 = 2 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Hence, the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is radical.

9.1.3 Remark. Let L be a splitting field of $f := x^3+x^2-2x-1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. Since $f(1) = -1$ and $f(-1) = 1$, this polynomial has no rational roots and is irreducible. Its discriminant is

$$\begin{aligned}\Delta(f) &= (1)^2(-2)^2 + 18(1)(-2)(-1) - 4(-2)^3 - 4(1)^3(-1) - 27(-1)^2 \\ &= 49 = 7^2 > 0\,,\end{aligned}$$

so the roots of f are all real and $L \subset \mathbb{R}$. Since $\Delta(f)$ is a square, the field extension $\mathbb{Q} \subset L$ is Galois of degree 3. Moreover, Cardano's formulas imply that $\mathbb{Q} \subset L$ is contained in a radical extension.

However, we claim that the field extension $\mathbb{Q} \subset L$ is not radical. If $\mathbb{Q} \subset L$ were radical, then $[L : \mathbb{Q}] = 3$ would imply that $L = \mathbb{Q}(\gamma)$ where $\gamma^m \in \mathbb{Q}$ for some $m \geqslant 3$. The minimal polynomial f of γ over $\mathbb{Q}$ would divide $x^m - \gamma^m$ and have degree $[L : \mathbb{Q}] = 3$. Since $\mathbb{Q} \subset L$ is Galois, f would split completely over $\mathbb{Q}(\gamma)$, so three of $\gamma, \zeta\gamma, \zeta^2\gamma, \ldots, \zeta^{m-1}\gamma$ would like in L, where ζ is a primitive mth root of unity. However, this is impossible because $L \subset \mathbb{R}$.

This example motivates the following definition.

9.1.4 Definition. A field extension $K \subseteq L$ is *solvable* if there exists a field extension $L \subseteq M$ such that $K \subseteq M$ is radical.

9.1.5 Remark. When L is a splitting field of $x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$, the field extension $\mathbb{Q} \subset L$ is solvable.

9.1.6 Definition. For all subfields K_1, K_2 of field L, their *compositum* K_1K_2 is the smallest subfield of L containing K_1 and K_2.

9.1.7 Lemma. *The compositum of two subfields always exists. Moreover, the compositum of*

$$M_1 = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq L \quad \textit{and} \quad M_2 = K(\beta_1, \beta_2, \ldots, \beta_m) \subseteq L$$

is $M_1M_2 = K(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m)$.

Sketch of Proof. The intersection of any collection of subfields of L is again a subfield of L. Thus, M_1M_2 is the intersection of all subfields of L containing both M_1 and M_2.

The field $K(\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m)$ contains M_1 and M_2, so

$$M_1M_2 \subseteq K(\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m) .$$

For the reverse inclusion, the compositum M_1M_2 contains M_1 and M_2, so it contains K and the elements $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m$. Hence, we deduce that

$$K(\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m) \subseteq M_1M_2 . \qquad \square$$

9.1.8 Proposition. *For any intermediate field M of a Galois extension $K \subseteq L$, the Galois closure of $K \subseteq M$ is the compositum of all conjugate fields of M in L.*

Proof. By the Theorem of the Primitive Element, there exists $\alpha \in L$ such that $M = K(\alpha)$. Since $K \subseteq L$ is Galois, the minimal polynomial $p \in K[x]$ of α is separable and splits completely over L, which means $p = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$ where $\alpha_1 = \alpha$. It follows that $K(\alpha_1, \alpha_2, \dots, \alpha_r)$ is a Galois extension of K containing M. The conjugate fields of M in L are $K(\alpha_j)$, for all $1 \leqslant j \leqslant r$, and the lemma implies that $K(\alpha_1)K(\alpha_2)\cdots K(\alpha_r) = K(\alpha_1, \alpha_2, \dots, \alpha_r) = M$. $\square$

9.1.9 Lemma. *When $K \subseteq M$ and $M \subseteq L$ are radical, then $K \subseteq L$ is radical. Moreover, given $K \subseteq M_1 \subseteq L$ and $K \subseteq M_2 \subseteq L$ such that $K \subseteq M_1$ is radical, the field extension $M_2 \subseteq M_1M_2$ is radical. Thirdly, given $K \subseteq M_1 \subseteq L$ and $K \subseteq M_2 \subseteq L$ such thatt $K \subseteq M_1$ and $K \subseteq M_2$ are radical, the field extension $K \subseteq M_1M_2$ is radical.*

Sketch of Proof. Concatenate the sequence of subfields that show $K \subseteq M$ and $M \subseteq L$ are radical extensions.

Since $K \subseteq M_1$ is radical, there exists $K = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = M$ where $K_j = K_j(\gamma_j)$ and ${\gamma_j}^{m_j} \in K_{j-1}$. Set $K_0' := M_2$ and $K_j' := K_{j-1}'(\gamma_j)$ for all $1 \leqslant j \leqslant n$. Verify that $K_j \subseteq K_j'$ and ${\gamma_j}^{m_j} \in K_{j-1} \subseteq K_{j-1}'$. Hence, the sequence $M_2 = K_0' \subset \cdots \subset K_n'$ is radical, and one confirms that $K_n' = M_1M_2$.

The second part shows that $M_2 \subseteq M_1M_2$ is radical. Since $K \subseteq M_2$ is radical, the first part shows that $K \subseteq M_1M_2$ is radical. $\square$

9.1.10 Theorem. *For every field extension $K \subseteq L$ that is separable and radical, its Galois closure is also radical.*

Proof. From the existence of Galois closures, there exists a field extension $L \subseteq L'$ such that $K \subseteq L'$ is Galois. Given $\sigma \in \mathrm{Gal}(L'/K)$, we get the conjugate field $K \subseteq \sigma(M) \subseteq L$. Applying σ to the sequence of fields that establish that $M \subseteq L$ is radical shows that $\sigma(M) \subseteq L$ is also radical. Since each conjugate field over K is radical, the Lemma shows that their compositum is also radical over K. This compositum is the Galois closure, which completes the proof. $\square$

9.1.11 Corollary. *Let K be a field of characteristic 0. The Galois closure of a solvable finite field extension $K \subseteq L$ is also solvable.*

Proof. Since $K \subseteq L$ is solvable, there is a field L' such that $K \subseteq L \subseteq L'$ and $K \subseteq L'$ is radical. Working in characteristic 0 ensures that $K \subseteq L'$ is separable. Hence, there exists a Galois closure $K \subseteq L' \subseteq M$. By Theorem 9.1.10, the field extension $K \subseteq M$ is radical.

Now consider $K \subseteq L \subseteq M$. Since $K \subseteq M$ is Galois, it contains the Galois closure of $K \subseteq L$. Thus, the Galois closure lies in the radical extension $K \subseteq M$, so the Galois closure is solvable. $\square$

9.2 Roots and Radicals

When is a finite field extension $K \subseteq L$ solvable? Given a positive integer m and a field L of characteristic 0, consider the splitting field of $f := x^m - 1$ over L. As $(-1)f + \left(\frac{1}{m}x\right)f' = 1$, we have $\gcd(f, f') = 1$ and the polynomial f is separable and has m distinct roots. An *mth primitive roots of unity* ζ has two properties: the m distinct roots of $x^m - 1$ are $1, \zeta, \zeta^2, \ldots, \zeta^{m-1}$ and the splitting field of $x^m - 1$ is $L(\zeta)$.

9.2.0 Lemma. *Let L be a field of characteristic zero. For every primitive mth root ζ of unity, the field extension $L \subseteq L(\zeta)$ is Galois and the Galois group $\mathrm{Gal}\big(L(\zeta)/L\big)$ is abelian.*

Proof. The field extension $L \subseteq L(\zeta)$ is Galois because $L(\zeta)$ is the splitting field of the separable polynomial $x^m - 1 \in L[x]$. Consider $\sigma, \tau \in \mathrm{Gal}\big(L(\zeta)/L\big)$. Since the image of root must be a root, we see that $\sigma(\zeta) = \zeta^j$ and $\tau(\zeta) = \zeta^k$ for some $j, k \in \mathbb{Z}$. It follows that

$$(\sigma \circ \tau)(\zeta) = \sigma(\zeta^k) = \sigma(\zeta)^k = \zeta^{jk} = \tau(\zeta)^j = \tau(\zeta^j) = (\tau \circ \sigma)(\zeta)\,.$$

We deduce that $\sigma \circ \tau = \tau \circ \sigma$ because the elements of $\mathrm{Gal}\big(L(\zeta)/L\big)$ are uniquely determined by their values on ζ. We conclude that $\mathrm{Gal}\big(L(\zeta)/L\big)$ is abelian. □

9.2.1 Lemma. *Assume that the field K has characteristic zero. Let $K \subseteq L$ be a Galois field extension. For every primitive mth root ζ of unity, the field extensions $K \subseteq L(\zeta)$ and $K(\zeta) \subseteq L(\zeta)$ are also Galois. Moreover, the following are equivalent:*

(a) *The group $\mathrm{Gal}(L/K)$ is solvable.*

(b) *The group $\mathrm{Gal}\big(L(\zeta)/K\big)$ is solvable*

(c) *The group $\mathrm{Gal}\big(L(\zeta)/K(\zeta)\big)$ is solvable.*

Proof. Since the field extension $K \subseteq L$ is Galois, the larger field L is the splitting field of a separable polynomial $f \in K[x]$ over K. The hypothesis that ζ is a primitive mth root of unity implies that $L(\zeta)$ is the splitting field of $x^m - 1 \in L[x]$ over L. It follows that $L(\zeta)$ is the splitting field of the product $(x^m - 1)f \in K[x]$ over K. Hence, the field extension $K \subseteq L(\zeta)$ is also Galois.

We next prove the equivalence between **(a)** and **(b)**. Since $K \subseteq L(\zeta)$ and $K \subseteq L$ are Galois, the group $\mathrm{Gal}\big(L(\zeta)/L\big)$ is a normal subgroup of $\mathrm{Gal}\big(L(\zeta)/K\big)$ such that

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}\big(L(\zeta)/K\big) \Big/ \mathrm{Gal}\big(L(\zeta)/L\big)\,.$$

The first lemma shows that $\mathrm{Gal}\big(L(\zeta)/L\big)$ is abelian and therefby solvable. Thus, Monday's Theorem establishes that $\mathrm{Gal}\big(L(\zeta)/K\big)$ is solvable if and only if $\mathrm{Gal}(L/K)$ is.

It remains to prove the equivalence between **(b)** and **(c)**. The first lemma shows that $K \subseteq K(\zeta)$ is Galois, we have

$$\mathrm{Gal}\big(K(\zeta)/K\big) \cong \mathrm{Gal}\big(L(\zeta)/K\big) \Big/ \mathrm{Gal}\big(L(\zeta)/K(\zeta)\big)\,.$$

As above, the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is abelian and thereby solvable. Thus, Monday's Theorem establishes that $\mathrm{Gal}\big(L(\zeta)/K\big)$ is solvable if and only if $\mathrm{Gal}\big(L(\zeta)/K(\zeta)\big)$ is. □

Our third lemma will play a crucial role in our analysis of solvable extensions.

9.2.2 Lemma. *Assume that the field K has characteristic zero. Let $K \subseteq L$ be a Galois field extension with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/\langle p \rangle$ for some prime $p \in \mathbb{Z}$. When K contains a primitive pth roots of unity ζ, there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^p \in K$.*

Proof. By hypothesis, $\mathrm{Gal}(L/K)$ is cycle of order p. Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator, and fix $\beta \in L \setminus K$. For each $1 \leqslant j \leqslant p-1$, consider the *Lagrange resolvent* defined by

$$\alpha_j := \beta + \zeta^{-j}\sigma(\beta) + \sigma^{-2j}\sigma^2(\beta) + \cdots + \zeta^{-j(p-1)}\sigma^{p-1}(\beta)\,.$$

It follows that

$$\zeta^{-j}\sigma(\alpha_j) = \zeta^{-j}\sigma(\beta) + \sigma^{-2j}\sigma^2(\beta) + \cdots + \zeta^{-j(p-1)}\sigma^{p-1}(\beta) + \zeta^{-jp}\sigma^p(\beta)\,.$$

The identities $\zeta^p = 1$ and $\sigma^p = \mathrm{id}_L$ give $\zeta^{-j}\sigma(\alpha_j) = \alpha_j$ or equivalently $\sigma(\alpha_j) = \zeta^j\alpha_j$. Since $\zeta \in K$ and $\zeta^p = 1$, we obtain $\sigma(\alpha_j^p) = \alpha_j^p$. This shows that α_j^p is fixed by $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Hence, $\alpha_j^p \in K$ because $K \subseteq L$ is Galois. When $j = 0$, we have $\sigma(\alpha_0) = \alpha_0$, so $\alpha_0 \in K$.

Suppose that there exists an index $1 \leqslant j \leqslant p-1$ such that $\alpha_j \neq 0$. For these indices, we also have $\zeta^j \neq 1$ and $\zeta^j\alpha_j \neq \alpha_j$. Combined with $\sigma(\alpha_j) = \zeta^j\alpha_j$, we deduce that $\sigma(\alpha_j) \neq \alpha_j$, so $\alpha_j \notin K$. It follows that $L = K(\alpha_j)$ because $[L : K]$ is prime. In particular, the element $\alpha := \alpha_j$ has the desired properties.

It remains to consider what happens if $\alpha_j = 0$ for all $1 \leqslant j \leqslant p-1$. In this case, we have the sum

$$\begin{aligned}
\alpha_0 &= \alpha_0 + \alpha_1 + \cdots + \alpha_{p-1} \\
&= \bigl(\beta + \sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{p-1}(\beta)\bigr) \\
&\quad + \bigl(\beta + \zeta^{-1}\sigma(\beta) + \zeta^{-2}\sigma^2(\beta) + \cdots + \zeta^{-(p-1)}\sigma^{p-1}(\beta)\bigr) + \cdots \\
&\quad\quad + \bigl(\beta + \zeta^{-(p-1)}\sigma(\beta) + \zeta^{-2(p-1)}\sigma^2(\beta) + \cdots + \zeta^{-(p-1)(p-1)}\sigma^{p-1}(\beta)\bigr) \\
&= p\beta + \bigl(1 + \zeta^{-1} + \zeta^{-2} + \cdots + \zeta^{-(p-1)}\bigr)\sigma(\beta) \\
&\quad + \bigl(1 + \zeta^{-2} + \zeta^{-4} + \cdots + \zeta^{-2(p-1)}\bigr)\sigma^2(\beta) + \cdots \\
&\quad\quad + \bigl(1 + \zeta^{-(p-1)} + \zeta^{-2(p-1)} + \cdots + \zeta^{-(p-1)(p-1)}\bigr)\sigma^{p-1}(\beta)\,.
\end{aligned}$$

Since $1 + \zeta^{-j} + \zeta^{-2j} + \cdots + \zeta^{-(p-1)j} = 0$ for all $1 \leqslant j \leqslant p-1$, it follows that $\alpha_0 = p\beta$. However, this contradicts the relations $\alpha_0 \in K$ and $\beta \notin K$. Thus, at least one of the $\alpha_1, \alpha_2, \ldots, \alpha_{p-1}$ is nonzero. □

9.2.3 Theorem. *Let $K \subseteq L$ be a Galois field extension. The Galois group $\mathrm{Gal}(L/K)$ is solvable if and only if the field extension $K \subseteq L$ is solvable.*

Comment on the Proof. Using the lemmata from today, the prove of the theorem will be discussed next class. □