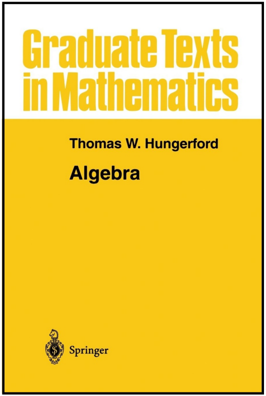
# Modern Algebra

## Chapter V. Fields and Galois Theory

V.9. Radical Extensions—Proofs of Theorems



# Table of contents

# Lemma V.9.3

**Lemma V.9.3.** If $F$ is a radical extension of $K$ and $N$ is a normal closure of $F$ over $K$ (see Theorem V.3.16 on page 265), then $N$ is a radical extension of $K$.

**Proof.** The proof is based on two claims.

# Lemma V.9.3

**Lemma V.9.3.** If $F$ is a radical extension of $K$ and $N$ is a normal closure of $F$ over $K$ (see Theorem V.3.16 on page 265), then $N$ is a radical extension of $K$.

**Proof.** The proof is based on two claims.

**Claim 1.** If $F$ is any finite dimensional extension of $K$ (not necessarily a radical extension) and $N$ is the normal closure of $F$ over $K$, then $N$ is the composite field $E_1 E_2 \cdots E_r$ (that is, the subfield of $N$ generated by $E_1 \cup E_2 \cup \cdots \cup E_r$) where each $E_i$ is a subfield of $N$ generated by $E_1 \cup E_2 \cup \cdots \cup E_r$) where each $E_i$ is a subfield of $N$ which is $K$-isomorphic to $F$.

# Lemma V.9.3

**Lemma V.9.3.** If $F$ is a radical extension of $K$ and $N$ is a normal closure of $F$ over $K$ (see Theorem V.3.16 on page 265), then $N$ is a radical extension of $K$.

**Proof.** The proof is based on two claims.
**Claim 1.** If $F$ is any finite dimensional extension of $K$ (not necessarily a radical extension) and $N$ is the normal closure of $F$ over $K$, then $N$ is the composite field $E_1E_2 \cdots E_r$ (that is, the subfield of $N$ generated by $E_1 \cup E_2 \cup \cdots \cup E_r$) where each $E_i$ is a subfield of $N$ generated by $E_1 \cup E_2 \cup \cdots \cup E_r$) where each $E_i$ is a subfield of $N$ which is $K$-isomorphic to $F$.

Proof 1. Since we hypothesize that $F$ is a finite dimensional extension of $K$, let $\{w_1, w_2, \ldots, w_n\}$ be a basis of $F$ over $K$ and let $f_i$ be the irreducible polynomial of $w_i$ over $K$ (finite dimensional extensions are algebraic extensions by Theorem V.1.11).

# Lemma V.9.3

**Lemma V.9.3.** If $F$ is a radical extension of $K$ and $N$ is a normal closure of $F$ over $K$ (see Theorem V.3.16 on page 265), then $N$ is a radical extension of $K$.

**Proof.** The proof is based on two claims.
**Claim 1.** If $F$ is any finite dimensional extension of $K$ (not necessarily a radical extension) and $N$ is the normal closure of $F$ over $K$, then $N$ is the composite field $E_1 E_2 \cdots E_r$ (that is, the subfield of $N$ generated by $E_1 \cup E_2 \cup \cdots \cup E_r$) where each $E_i$ is a subfield of $N$ generated by $E_1 \cup E_2 \cup \cdots \cup E_r$) where each $E_i$ is a subfield of $N$ which is $K$-isomorphic to $F$.
Proof 1. Since we hypothesize that $F$ is a finite dimensional extension of $K$, let $\{w_1, w_2, \ldots, w_n\}$ be a basis of $F$ over $K$ and let $f_i$ be the irreducible polynomial of $w_i$ over $K$ (finite dimensional extensions are algebraic extensions by Theorem V.1.11).

# Lemma V.9.3 (continued 1)

**Proof (continued).** Since $N$ is the normal closure of $F$ over $K$ then as shown in the proof of Theorem V.3.16(i) $N$ is a splitting field of $\{f_1, f_2, \ldots, f_n\}$ over $K$. For a given $f_j$, let $v$ be any root of $f_j \in K[x]$ in $N$. By Theorem V.1.8(ii), since $w_i$ is also a root of $f_j \in K[x]$, then the identity $\iota : K \to K$ extends to an isomorphism $\sigma : K(w_j) \to K(v)$ such that $\sigma(w_j) = v$ (here we let $L = K$ in Theorem V.1.8(ii); that is, $\sigma$ is a $K$-isomorphism mapping $K(w_j) \to K(v)$ where $\sigma(w_j) = v$. By Theorem V.3.8 (with $L = K$, $S = \{f_i\}$, $S' = \{\sigma f_i\} = \{f_i\}$, and $F = M = N$) $\sigma$ extends to a $K$-automorphism $\tau$ of $N$.

# Lemma V.9.3 (continued 1)

**Proof (continued).** Since $N$ is the normal closure of $F$ over $K$ then as shown in the proof of Theorem V.3.16(i) $N$ is a splitting field of $\{f_1, f_2, \ldots, f_n\}$ over $K$. For a given $f_j$, let $v$ be any root of $f_j \in K[x]$ in $N$. By Theorem V.1.8(ii), since $w_i$ is also a root of $f_j \in K[x]$, then the identity $\iota : K \to K$ extends to an isomorphism $\sigma : K(w_j) \to K(v)$ such that $\sigma(w_j) = v$ (here we let $L = K$ in Theorem V.1.8(ii); that is, $\sigma$ is a $K$-isomorphism mapping $K(w_j) \to K(v)$ where $\sigma(w_j) = v$. By Theorem V.3.8 (with $L = K$, $S = \{f_i\}$, $S' = \{\sigma f_i\} = \{f_i\}$, and $F = M = N$) $\sigma$ extends to a $K$-automorphism $\tau$ of $N$. Since $F$ is a subfield of $N$ which is isomorphic to $F$ (i.e., $\tau(F) \cong F$) and $w_j \in F$ then $\tau(w_j) = \sigma(w_j) = v \in \tau(F)$. In this way we can find for every root $v$ of every $f_i$ a subfield $E$ of $N$ such that $v \in E$ and $E$ is $K$-isomorphic to $F$ (the $K$-isomorphism if $\tau$, as constructed above).

# Lemma V.9.3 (continued 1)

**Proof (continued).** Since $N$ is the normal closure of $F$ over $K$ then as shown in the proof of Theorem V.3.16(i) $N$ is a splitting field of $\{f_1, f_2, \ldots, f_n\}$ over $K$. For a given $f_j$, let $v$ be any root of $f_j \in K[x]$ in $N$. By Theorem V.1.8(ii), since $w_i$ is also a root of $f_j \in K[x]$, then the identity $\iota : K \to K$ extends to an isomorphism $\sigma : K(w_j) \to K(v)$ such that $\sigma(w_j) = v$ (here we let $L = K$ in Theorem V.1.8(ii); that is, $\sigma$ is a $K$-isomorphism mapping $K(w_j) \to K(v)$ where $\sigma(w_j) = v$. By Theorem V.3.8 (with $L = K$, $S = \{f_i\}$, $S' = \{\sigma f_i\} = \{f_i\}$, and $F = M = N$) $\sigma$ extends to a $K$-automorphism $\tau$ of $N$. Since $F$ is a subfield of $N$ which is isomorphic to $F$ (i.e., $\tau(F) \cong F$) and $w_j \in F$ then $\tau(w_j) = \sigma(w_j) = v \in \tau(F)$. In this way we can find for every root $v$ of every $f_i$ a subfield $E$ of $N$ such that $v \in E$ and $E$ is $K$-isomorphic to $F$ (the $K$-isomorphism if $\tau$, as constructed above).

# Lemma V.9.3 (continued 2)

**Proof (continued).** If $E_1, E_2, \ldots, E_r$ are the subfields so obtained, then the subfield of $N$ generated by $E_1 \cup E_2 \cup \cdots \cup E_r$ (that is, the "composite field" $E_1 E_2 \cdots E_r$) contains all the roots of $f_1, f_2, \ldots, f_n$. That is, $E_1 E_2 \cdots E_r$ is a splitting field for $\{f_1, f_2, \ldots, f_n\}$ and so by Theorem V.3.14 (the (ii)$\Rightarrow$(i) part) field $E_1 E_2 \cdots E_r \subset N$ is normal over $K$. When we have the case $v = w_j$ then the $K$-isomorphism $\tau : N \to N$ is then identity (since the corresponding $\sigma : K(w_j) \to K(v)$ is the identity) and in this case $\tau(F) = F$ and $F$ is a subfield of the corresponding $E_j$. So $F$ is a subfield of the composite field $E_1 E_2 \cdots E_r \subset N$. But by Theorem V.3.16(ii), no proper subfield of $N$ containing $F$ is normal over $K$, so it must be that $N = E_1 E_2 \cdots E_r$, proving Claim 1.

# Lemma V.9.3 (continued 2)

**Proof (continued).** If $E_1, E_2, \ldots, E_r$ are the subfields so obtained, then the subfield of $N$ generated by $E_1 \cup E_2 \cup \cdots \cup E_r$ (that is, the "composite field" $E_1 E_2 \cdots E_r$) contains all the roots of $f_1, f_2, \ldots, f_n$. That is, $E_1 E_2 \cdots E_r$ is a splitting field for $\{f_1, f_2, \ldots, f_n\}$ and so by Theorem V.3.14 (the (ii)$\Rightarrow$(i) part) field $E_1 E_2 \cdots E_r \subset N$ is normal over $K$. When we have the case $v = w_j$ then the $K$-isomorphism $\tau : N \to N$ is then identity (since the corresponding $\sigma : K(w_j) \to K(v)$ is the identity) and in this case $\tau(F) = F$ and $F$ is a subfield of the corresponding $E_j$. So $F$ is a subfield of the composite field $E_1 E_2 \cdots E_r \subset N$. But by Theorem V.3.16(ii), no proper subfield of $N$ containing $F$ is normal over $K$, so it must be that $N = E_1 E_2 \cdots E_r$, proving Claim 1.

# Lemma V.9.3 (continued 3)

**Proof (continued).**
**Claim 2.** If $E_1, E_2, \ldots, E_r$ are each radical extensions of $K$, then the composite field $E_1 E_2 \cdots E_r$ is a radical extension of $K$.
Proof 2. If $E_k$ is a radical extension of $K$ then (by definition) $E_k = K(u_1^k, u_2^k, \ldots, u_{n_k}^k)$ where some power of $u_i^k$ lies in $K$ and for each $i \geq 2$, some power of $u_i^k$ lies in $K(u_1^k, u_2^k, \ldots, u_{i-1}^k)$. Then $E_1 E_2 \cdots E_r = K(u_1^1, 2_2^1, \ldots, u_{n_1}^1, u_1^2, u_2^2, \ldots, u_{n_2}^2, u_1^3, u_2^3, \ldots, u_{n_r}^r)$ is "clearly" a radical extension of $K$, proving Claim 2.

# Lemma V.9.3 (continued 3)

**Proof (continued).**
**Claim 2.** If $E_1, E_2, \ldots, E_r$ are each radical extensions of $K$, then the composite field $E_1 E_2 \cdots E_r$ is a radical extension of $K$.
Proof 2. If $E_k$ is a radical extension of $K$ then (by definition) $E_k = K(u_1^k, u_2^k, \ldots, u_{n_k}^k)$ where some power of $u_i^k$ lies in $K$ and for each $i \geq 2$, some power of $u_i^k$ lies in $K(u_1^k, u_2^k, \ldots, u_{i-1}^k)$. Then $E_1 E_2 \cdots E_r = K(u_1^1, 2_2^1, \ldots, u_{n_1}^1, u_1^2, u_2^2, \ldots, u_{n_2}^2, u_1^3, u_2^3, \ldots, u_{n_r}^r)$ is "clearly" a radical extension of $K$, proving Claim 2.
**Proof of Lemma.** Since by definition, a radical extension is a finite extension, Claim 1 implies that $N = E_1 E_2 \cdots E_r$ where each $E_i$ is a subfield of $N$ which is $K$-isomorphic to $F$. Since $F$ is hypothesized to be a radical extension of $K$, then each $E_i$ is a radical extension of $K$.

# Lemma V.9.3 (continued 3)

**Proof (continued).**

**Claim 2.** If $E_1, E_2, \ldots, E_r$ are each radical extensions of $K$, then the composite field $E_1 E_2 \cdots E_r$ is a radical extension of $K$.

Proof 2. If $E_k$ is a radical extension of $K$ then (by definition) $E_k = K(u_1^k, u_2^k, \ldots, u_{n_k}^k)$ where some power of $u_i^k$ lies in $K$ and for each $i \geq 2$, some power of $u_i^k$ lies in $K(u_1^k, u_2^k, \ldots, u_{i-1}^k)$. Then $E_1 E_2 \cdots E_r = K(u_1^1, 2_2^1, \ldots, u_{n_1}^1, u_1^2, u_2^2, \ldots, u_{n_2}^2, u_1^3, u_2^3, \ldots, u_{n_r}^r)$ is "clearly" a radical extension of $K$, proving Claim 2.

**Proof of Lemma.** Since by definition, a radical extension is a finite extension, Claim 1 implies that $N = E_1 E_2 \cdots E_r$ where each $E_i$ is a subfield of $N$ which is $K$-isomorphic to $F$. Since $F$ is hypothesized to be a radical extension of $K$, then each $E_i$ is a radical extension of $K$. By Claim 2, $N = E_1 E_2 \cdots E_r$ is a radical extension of $K$. □

# Lemma V.9.3 (continued 3)

**Proof (continued).**
**Claim 2.** If $E_1, E_2, \ldots, E_r$ are each radical extensions of $K$, then the composite field $E_1 E_2 \cdots E_r$ is a radical extension of $K$.
Proof 2. If $E_k$ is a radical extension of $K$ then (by definition) $E_k = K(u_1^k, u_2^k, \ldots, u_{n_k}^k)$ where some power of $u_i^k$ lies in $K$ and for each $i \geq 2$, some power of $u_i^k$ lies in $K(u_1^k, u_2^k, \ldots, u_{i-1}^k)$. Then $E_1 E_2 \cdots E_r = K(u_1^1, 2_2^1, \ldots, u_{n_1}^1, u_1^2, u_2^2, \ldots, u_{n_2}^2, u_1^3, u_2^3, \ldots, u_{n_r}^r)$ is "clearly" a radical extension of $K$, proving Claim 2.
**Proof of Lemma.** Since by definition, a radical extension is a finite extension, Claim 1 implies that $N = E_1 E_2 \cdots E_r$ where each $E_i$ is a subfield of $N$ which is $K$-isomorphic to $F$. Since $F$ is hypothesized to be a radical extension of $K$, then each $E_i$ is a radical extension of $K$. By Claim 2, $N = E_1 E_2 \cdots E_r$ is a radical extension of $K$. □

# Theorem V.9.4

**Theorem V.9.4.** If $F$ is a radical extension field of $K$ and $E$ is an intermediate field, then $\mathrm{Aut}_K(E)$ is a solvable group.

**Proof.** Let $K_0$ be the fixed subfield of $E$ relative to $\mathrm{Aut}_K E$ (so $K \subset K_0 \subset E$). Then $\mathrm{Aut}_{K_0} E = \mathrm{Aut}_K E$ and the fixed field of $\mathrm{Aut}_{K_0} E$ is $K_0$ so $E$ is Galois over $K_0$.

# Theorem V.9.4

**Theorem V.9.4.** If $F$ is a radical extension field of $K$ and $E$ is an intermediate field, then $\mathrm{Aut}_K(E)$ is a solvable group.

**Proof.** Let $K_0$ be the fixed subfield of $E$ relative to $\mathrm{Aut}_K E$ (so $K \subset K_0 \subset E$). Then $\mathrm{Aut}_{K_0} E = \mathrm{Aut}_K E$ and the fixed field of $\mathrm{Aut}_{K_0} E$ is $K_0$ so $E$ is Galois over $K_0$. By Exercise V.9.1, $F$ is a radical extension of $K_0$ (since $K \subset K_0 \subset E \subset F$; $F$ is radical over $K$ and so is radical over intermediate fields by the Exercise). By the definition of radical extension, $F$ is then algebraic over $K_0$ and so $E$ is algebraic over $K$. Our goal is to show that $\mathrm{Aut}_K E$ is a solvable group.

# Theorem V.9.4

**Theorem V.9.4.** If $F$ is a radical extension field of $K$ and $E$ is an intermediate field, then $\mathrm{Aut}_K(E)$ is a solvable group.

**Proof.** Let $K_0$ be the fixed subfield of $E$ relative to $\mathrm{Aut}_K E$ (so $K \subset K_0 \subset E$). Then $\mathrm{Aut}_{K_0} E = \mathrm{Aut}_K E$ and the fixed field of $\mathrm{Aut}_{K_0} E$ is $K_0$ so $E$ is Galois over $K_0$. By Exercise V.9.1, $F$ is a radical extension of $K_0$ (since $K \subset K_0 \subset E \subset F$; $F$ is radical over $K$ and so is radical over intermediate fields by the Exercise). By the definition of radical extension, $F$ is then algebraic over $K_0$ and so $E$ is algebraic over $K$. Our goal is to show that $\mathrm{Aut}_K E$ is a solvable group. However, $\mathrm{Aut}_K E = \mathrm{Aut}_{K_0} E$ where $E$ is algebraic and Galois over $K_0$; so WLOG we can assume that $E$ is algebraic and Galois over $K$ to begin with.

# Theorem V.9.4

**Theorem V.9.4.** If $F$ is a radical extension field of $K$ and $E$ is an intermediate field, then $\text{Aut}_K(E)$ is a solvable group.

**Proof.** Let $K_0$ be the fixed subfield of $E$ relative to $\text{Aut}_K E$ (so $K \subset K_0 \subset E$). Then $\text{Aut}_{K_0} E = \text{Aut}_K E$ and the fixed field of $\text{Aut}_{K_0} E$ is $K_0$ so $E$ is Galois over $K_0$. By Exercise V.9.1, $F$ is a radical extension of $K_0$ (since $K \subset K_0 \subset E \subset F$; $F$ is radical over $K$ and so is radical over intermediate fields by the Exercise). By the definition of radical extension, $F$ is then algebraic over $K_0$ and so $E$ is algebraic over $K$. Our goal is to show that $\text{Aut}_K E$ is a solvable group. However, $\text{Aut}_K E = \text{Aut}_{K_0} E$ where $E$ is algebraic and Galois over $K_0$; so WLOG we can assume that $E$ is algebraic and Galois over $K$ to begin with.

Let $N$ be a normal closure of $F$ over $K$. By Lemma V.9.3, $N$ is a radical extension of $K$. Since $K \subset E \subset F$ where $E$ is algebraic and Galois over $K$ (WLOG as above), then by Lemma V.2.13, $E$ is stable (relative to $F$ and $K$). That is, every $K$-automorphism in $\text{Aut}_K F$ maps $E$ to itself.

# Theorem V.9.4

**Theorem V.9.4.** If $F$ is a radical extension field of $K$ and $E$ is an intermediate field, then $\mathrm{Aut}_K(E)$ is a solvable group.

**Proof.** Let $K_0$ be the fixed subfield of $E$ relative to $\mathrm{Aut}_K E$ (so $K \subset K_0 \subset E$). Then $\mathrm{Aut}_{K_0} E = \mathrm{Aut}_K E$ and the fixed field of $\mathrm{Aut}_{K_0} E$ is $K_0$ so $E$ is Galois over $K_0$. By Exercise V.9.1, $F$ is a radical extension of $K_0$ (since $K \subset K_0 \subset E \subset F$; $F$ is radical over $K$ and so is radical over intermediate fields by the Exercise). By the definition of radical extension, $F$ is then algebraic over $K_0$ and so $E$ is algebraic over $K$. Our goal is to show that $\mathrm{Aut}_K E$ is a solvable group. However, $\mathrm{Aut}_K E = \mathrm{Aut}_{K_0} E$ where $E$ is algebraic and Galois over $K_0$; so WLOG we can assume that $E$ is algebraic and Galois over $K$ to begin with.

Let $N$ be a normal closure of $F$ over $K$. By Lemma V.9.3, $N$ is a radical extension of $K$. Since $K \subset E \subset F$ where $E$ is algebraic and Galois over $K$ (WLOG as above), then by Lemma V.2.13, $E$ is stable (relative to $F$ and $K$). That is, every $K$-automorphism in $\mathrm{Aut}_K F$ maps $E$ to itself.

# Theorem V.9.4 (continued 1)

**Proof (continued).** Consequently, for any $\sigma \in \mathrm{Aut}_K N$ we can restrict $\sigma$ to $E$ (i.e., $\sigma|_E$) to produce an element of $\mathrm{Aut}_K E$. Let $\theta : \mathrm{Aut}_K N \to \mathrm{Aut}_K E$ be defined as $\theta(\sigma) = \sigma|_E$. Then $\theta$ is a homomorphism because $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|_E = \sigma_1|_E\sigma_2|_E = \theta(\sigma_1)\theta(\sigma_2)$. Now since $N$ is normal over $K$, then $N$ is a splitting field over $K$ by Theorem V.3.14 (the (i)⇒(ii) part), and so $N$ is a splitting field over $E$. Now for $\sigma \in \mathrm{Aut}_K E$ we know that $\sigma : E \to E$ is an isomorphism and since $N$ is a splitting field of $E$, then by Theorem V.3.8, $\sigma$ can be extended to an isomorphism mapping $N \to N$. That is, $\sigma$ extends to a $K$-automorphism of $N$.

# Theorem V.9.4 (continued 1)

**Proof (continued).** Consequently, for any $\sigma \in \text{Aut}_K N$ we can restrict $\sigma$ to $E$ (i.e., $\sigma|_E$) to produce an element of $\text{Aut}_K E$. Let $\theta : \text{Aut}_K N \to \text{Aut}_K E$ be defined as $\theta(\sigma) = \sigma|_E$. Then $\theta$ is a homomorphism because $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|_E = \sigma_1|_E\sigma_2|_E = \theta(\sigma_1)\theta(\sigma_2)$. Now since $N$ is normal over $K$, then $N$ is a splitting field over $K$ by Theorem V.3.14 (the (i)⇒(ii) part), and so $N$ is a splitting field over $E$. Now for $\sigma \in \text{Aut}_K E$ we know that $\sigma : E \to E$ is an isomorphism and since $N$ is a splitting field of $E$, then by Theorem V.3.8, $\sigma$ can be extended to an isomorphism mapping $N \to N$. That is, $\sigma$ extends to a $K$-automorphism of $N$. Applying homomorphism $\theta$ to the extension of $\sigma$ produces $\sigma \in \text{Aut}_K E$. Since $\sigma$ was an arbitrary element of $\text{Aut}_K E$, then $\theta$ is onto (i.e., an epimorphism). Since the homomorphic image of a solvable group is solvable by Theorem II.7.11(i), if we show that $\text{Aut}_K N$ is solvable then the solvability of $\text{Aut}_K E$ would follow.

# Theorem V.9.4 (continued 1)

**Proof (continued).** Consequently, for any $\sigma \in \mathrm{Aut}_K N$ we can restrict $\sigma$ to $E$ (i.e., $\sigma|_E$) to produce an element of $\mathrm{Aut}_K E$. Let $\theta : \mathrm{Aut}_K N \to \mathrm{Aut}_K E$ be defined as $\theta(\sigma) = \sigma|_E$. Then $\theta$ is a homomorphism because $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|_E = \sigma_1|_E\sigma_2|_E = \theta(\sigma_1)\theta(\sigma_2)$. Now since $N$ is normal over $K$, then $N$ is a splitting field over $K$ by Theorem V.3.14 (the (i)⇒(ii) part), and so $N$ is a splitting field over $E$. Now for $\sigma \in \mathrm{Aut}_K E$ we know that $\sigma : E \to E$ is an isomorphism and since $N$ is a splitting field of $E$, then by Theorem V.3.8, $\sigma$ can be extended to an isomorphism mapping $N \to N$. That is, $\sigma$ extends to a $K$-automorphism of $N$. Applying homomorphism $\theta$ to the extension of $\sigma$ produces $\sigma \in \mathrm{Aut}_K E$. Since $\sigma$ was an arbitrary element of $\mathrm{Aut}_K E$, then $\theta$ is onto (i.e., an epimorphism). Since the homomorphic image of a solvable group is solvable by Theorem II.7.11(i), if we show that $\mathrm{Aut}_K N$ is solvable then the solvability of $\mathrm{Aut}_K E$ would follow.

# Theorem V.9.4 (continued 2)

**Proof (continued).** Let $K_1$ be the fixed subfield of $N$ relative to $\mathrm{Aut}_K N = \mathrm{Aut}_{K_1} N$. Then (by definition) $N$ is a Galois extension of $K_1$ and by Exercise V.9.1, $N$ is a radical extension of $K_1$ since $N$ is a radical extension of $K$ and $K \subset K_1 \subset N$. Hence proving that $\mathrm{Aut}_K E$ is solvable can be accomplished by proving that $\mathrm{Aut}_{K_1} N$ is solvable where $N$ is a radical extension of $K_1$ and $N$ is Galois over $K_1$. So WLOG we may assume that $F$ is a Galois radical extension of $K$.

# Theorem V.9.4 (continued 2)

**Proof (continued).** Let $K_1$ be the fixed subfield of $N$ relative to $\text{Aut}_K N = \text{Aut}_{K_1} N$. Then (by definition) $N$ is a Galois extension of $K_1$ and by Exercise V.9.1, $N$ is a radical extension of $K_1$ since $N$ is a radical extension of $K$ and $K \subset K_1 \subset N$. Hence proving that $\text{Aut}_K E$ is solvable can be accomplished by proving that $\text{Aut}_{K_1} N$ is solvable where $N$ is a radical extension of $K_1$ and $N$ is Galois over $K_1$. So WLOG we may assume that $F$ is a Galois radical extension of $K$.

With $F = K(u_1, u_2, \ldots, u_n)$ with $u_1^{m_1} \in K$ and $u_i^{m_i} \in K(u_1, u_2, \ldots, u_{i-1})$ for $i \geq 2$, where $m_1$ and $m_i$ are chosen to be the smallest power of $u_1$ and $u_i$ in $K(u_1, u_2, \ldots, u_{i-1})$.

# Theorem V.9.4 (continued 2)

**Proof (continued).** Let $K_1$ be the fixed subfield of $N$ relative to $\text{Aut}_K N = \text{Aut}_{K_1} N$. Then (by definition) $N$ is a Galois extension of $K_1$ and by Exercise V.9.1, $N$ is a radical extension of $K_1$ since $N$ is a radical extension of $K$ and $K \subset K_1 \subset N$. Hence proving that $\text{Aut}_K E$ is solvable can be accomplished by proving that $\text{Aut}_{K_1} N$ is solvable where $N$ is a radical extension of $K_1$ and $N$ is Galois over $K_1$. So WLOG we may assume that $F$ is a Galois radical extension of $K$.

With $F = K(u_1, u_2, \ldots, u_n)$ with $u_1^{m_1} \in K$ and $u_i^{m_i} \in K(u_1, u_2, \ldots, u_{i-1})$ for $i \geq 2$, where $m_1$ and $m_i$ are chosen to be the smallest power of $u_1$ and $u_i$ in $K(u_1, u_2, \ldots, u_{i-1})$. We now establish that $\text{char}(K)$ does not divide $m_i$. This is obvious if $\text{char}(K) = 0$. If $\text{char}(K) = p \neq 0$ and $m_i = rp^t$ where $\gcd(r, p) = (r, p) = 1$.

# Theorem V.9.4 (continued 2)

**Proof (continued).** Let $K_1$ be the fixed subfield of $N$ relative to $\text{Aut}_K N = \text{Aut}_{K_1} N$. Then (by definition) $N$ is a Galois extension of $K_1$ and by Exercise V.9.1, $N$ is a radical extension of $K_1$ since $N$ is a radical extension of $K$ and $K \subset K_1 \subset N$. Hence proving that $\text{Aut}_K E$ is solvable can be accomplished by proving that $\text{Aut}_{K_1} N$ is solvable where $N$ is a radical extension of $K_1$ and $N$ is Galois over $K_1$. So WLOG we may assume that $F$ is a Galois radical extension of $K$.

With $F = K(u_1, u_2, \ldots, u_n)$ with $u_1^{m_1} \in K$ and $u_i^{m_i} \in K(u_1, u_2, \ldots, u_{i-1})$ for $i \geq 2$, where $m_1$ and $m_i$ are chosen to be the smallest power of $u_1$ and $u_i$ in $K(u_1, u_2, \ldots, u_{i-1})$. We now establish that $\text{char}(K)$ does not divide $m_i$. This is obvious if $\text{char}(K) = 0$. If $\text{char}(K) = p \neq 0$ and $m_i = rp^t$ where $\gcd(r, p) = (r, p) = 1$. Then $u_i^{m-i} = u_i^{rp^t} \in K(u_1, u_2, \ldots, u_{i-1})$ and, as remarked after Definition V.9.1, $u_i$ is a root of $x^{m_1} - u_i^{m_1} = x_i^{rp^t} - u_i^{rp^t} \in K(u_1, u_2, \ldots, u_{i-1})[x]$.

# Theorem V.9.4 (continued 2)

**Proof (continued).** Let $K_1$ be the fixed subfield of $N$ relative to $\mathrm{Aut}_K N = \mathrm{Aut}_{K_1} N$. Then (by definition) $N$ is a Galois extension of $K_1$ and by Exercise V.9.1, $N$ is a radical extension of $K_1$ since $N$ is a radical extension of $K$ and $K \subset K_1 \subset N$. Hence proving that $\mathrm{Aut}_K E$ is solvable can be accomplished by proving that $\mathrm{Aut}_{K_1} N$ is solvable where $N$ is a radical extension of $K_1$ and $N$ is Galois over $K_1$. So WLOG we may assume that $F$ is a Galois radical extension of $K$.

With $F = K(u_1, u_2, \ldots, u_n)$ with $u_1^{m_1} \in K$ and $u_i^{m_i} \in K(u_1, u_2, \ldots, u_{i-1})$ for $i \geq 2$, where $m_1$ and $m_i$ are chosen to be the smallest power of $u_1$ and $u_i$ in $K(u_1, u_2, \ldots, u_{i-1})$. We now establish that char$(K)$ does not divide $m_i$. This is obvious if char$(K) = 0$. If char$(K) = p \neq 0$ and $m_i = rp^t$ where $\gcd(r, p) = (r, p) = 1$. Then $u_i^{m-i} = u_i^{rp^t} \in K(u_1, u_2, \ldots, u_{i-1})$ and, as remarked after Definition V.9.1, $u_i$ is a root of $x^{m_1} - u_i^{m_1} = x_i^{rp^t} - u_i^{rp^t} \in K(u_1, u_2, \ldots, u_{i-1})[x]$.

# Theorem V.9.4 (continued 3)

**Proof (continued).** But by the Freshman's Dream (Exercise III.1.11), $x_i^{rp^t} - u_i^{rp^t} = (x_i^r - u_i^r)^{p^t}$. So the irreducible polynomial of $u^r \in F$ over $K(u_1, u_2, \ldots, u_{i-1})$ is $(x - u_i^r)^{p^t} = x^{p^t} - i_i^{rp^t} = x^{m_i} - u_i^{m_i}$ (notice that $u_i^{rp^t} = u_i^{m_i} \in K(u_1, u_2, \ldots, u_{i-1})$) and since $m_i$ is the smallest power of $u_i$ in $K(u_1, u_2, \ldots, u_{i-1})$ then $(x - u_i^r)^{p^t}$ is irreducible over $K(u_1, u_2, \ldots, u_{i-1})$; the "constant term" of this polynomial is $\pm$ a power of $u_i$). Therefore, by definition, $u_i^r$ is purely inseparable over $K(u_1, u_2, \ldots, u_{i-1})$. But $F$ is Galois over $K$ (by the WLOG argument above) and so $F$ is separable over $K$ by Theorem V.3.11 (the (i)$\Rightarrow$(ii) part). Whence $F$ is separable over the intermediate field $K(u_1, u_2, \ldots, u_{i-1})$ by Exercise V.3.12.

# Theorem V.9.4 (continued 3)

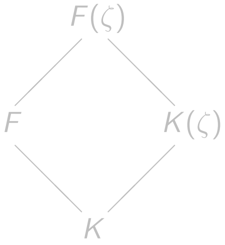
**Proof (continued).** But by the Freshman's Dream (Exercise III.1.11), $x_i^{rp^t} - u_i^{rp^t} = (x_i^r - u_i^r)^{p^t}$. So the irreducible polynomial of $u^r \in F$ over $K(u_1, u_2, \ldots, u_{i-1})$ is $(x - u_i^r)^{p^t} = x^{p^t} - i_i^{rp^t} = x^{m_i} - u_i^{m_i}$ (notice that $u_i^{rp^t} = u_i^{m_i} \in K(u_1, u_2, \ldots, u_{i-1})$) and since $m_i$ is the smallest power of $u_i$ in $K(u_1, u_2, \ldots, u_{i-1})$ then $(x - u_i^r)^{p^t}$ is irreducible over $K(u_1, u_2, \ldots, u_{i-1})$; the "constant term" of this polynomial is $\pm$ a power of $u_i$). Therefore, by definition, $u_i^r$ is purely inseparable over $K(u_1, u_2, \ldots, u_{i-1})$. But $F$ is Galois over $K$ (by the WLOG argument above) and so $F$ is separable over $K$ by Theorem V.3.11 (the (i)$\Rightarrow$(ii) part). Whence $F$ is separable over the intermediate field $K(u_1, u_2, \ldots, u_{i-1})$ by Exercise V.3.12. So $u_i^r$ is both separable and purely inseparable over $K$, and by Theorem V.6.2, $u_i^r \in K(u_1.u_2, \ldots, u_{i-1})$. So we have that $\text{char}(K) = p$ does not divide $m_i$, as claimed.

# Theorem V.9.4 (continued 3)

**Proof (continued).** But by the Freshman's Dream (Exercise III.1.11), $x_i^{rp^t} - u_i^{rp^t} = (x_i^r - u_i^r)^{p^t}$. So the irreducible polynomial of $u^r \in F$ over $K(u_1, u_2, \ldots, u_{i-1})$ is $(x - u_i^r)^{p^t} = x^{p^t} - i_i^{rp^t} = x^{m_i} - u_i^{m_i}$ (notice that $u_i^{rp^t} = u_i^{m_i} \in K(u_1, u_2, \ldots, u_{i-1})$) and since $m_i$ is the smallest power of $u_i$ in $K(u_1, u_2, \ldots, u_{i-1})$ then $(x - u_i^r)^{p^t}$ is irreducible over $K(u_1, u_2, \ldots, u_{i-1})$; the "constant term" of this polynomial is $\pm$ a power of $u_i$). Therefore, by definition, $u_i^r$ is purely inseparable over $K(u_1, u_2, \ldots, u_{i-1})$. But $F$ is Galois over $K$ (by the WLOG argument above) and so $F$ is separable over $K$ by Theorem V.3.11 (the (i)$\Rightarrow$(ii) part). Whence $F$ is separable over the intermediate field $K(u_1, u_2, \ldots, u_{i-1})$ by Exercise V.3.12. So $u_i^r$ is both separable and purely inseparable over $K$, and by Theorem V.6.2, $u_i^r \in K(u_1.u_2, \ldots, u_{i-1})$. So we have that $\text{char}(K) = p$ does not divide $m_i$, as claimed.

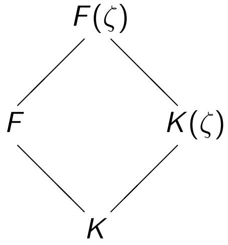
# Theorem V.9.4 (continued 4)

**Proof (continued).** If $m = m_1 m_2 \cdots m_n$ (where the $m_i$ are minimal as required in the previous paragraph) then char$(K)$ (which equals char$(F)$ by considering $1_k = 1_F$ in Theorem III.1.9(ii) for $n > 0$, and the fact that there is no $n \in \mathbb{N}$ such that all $na = 0$ for all $a \in K$ and the fact that $K \subset F$) does not divide $m$. Consider $x^m - 1 \in K[x]$ and let $\zeta$ be a primitive $m$th root of unity (which exists in the algebraic closure of $K$). Then $F(\zeta)$ contains all roots of $x^m - 1$ and hence is a cyclotomic extension of $K$. We have:



# Theorem V.9.4 (continued 4)

**Proof (continued).** If $m = m_1 m_2 \cdots m_n$ (where the $m_i$ are minimal as required in the previous paragraph) then char($K$) (which equals char($F$) by considering $1_k = 1_F$ in Theorem III.1.9(ii) for $n > 0$, and the fact that there is no $n \in \mathbb{N}$ such that all $na = 0$ for all $a \in K$ and the fact that $K \subset F$) does not divide $m$. Consider $x^m - 1 \in K[x]$ and let $\zeta$ be a primitive $m$th root of unity (which exists in the algebraic closure of $K$). Then $F(\zeta)$ contains all roots of $x^m - 1$ and hence is a cyclotomic extension of $K$. We have:



# Theorem V.9.4 (continued 5)

**Proof (continued).** By Theorem V.8.1(ii), $F(\zeta)$ is an abelian extension of $F$ and so (by definition of "abelian extension") is Galois over $F$. By Exercise V.3.15(b), $F(\zeta)$ is Galois over $K$ ($F$ is Galois over $K$ WLOG as argued above, and $F(\zeta)$ is a splitting field of $x^m - 1$ over $F$). By the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) we have that $\text{Aut}_K F \cong \text{Aut}_K F(\zeta)/\text{Aut}_F F(\zeta)$ (in Theorem V.2.5 we take $F = F(\zeta)$, $E = F$, $K = K$). This shows that $\text{Aut}_K F$ is the homomorphic image of $\text{Aut}_K F(\zeta)$ under canonical epimorphism (see page 43 on Section I.5). So to show that $\text{Aut}_K F$ is solvable, it is sufficient by Theorem II.7.11(i) to show that $\text{Aut}_K F(\zeta)$ is solvable.

# Theorem V.9.4 (continued 5)

**Proof (continued).** By Theorem V.8.1(ii), $F(\zeta)$ is an abelian extension of $F$ and so (by definition of "abelian extension") is Galois over $F$. By Exercise V.3.15(b), $F(\zeta)$ is Galois over $K$ ($F$ is Galois over $K$ WLOG as argued above, and $F(\zeta)$ is a splitting field of $x^m - 1$ over $F$). By the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) we have that $\mathrm{Aut}_K F \cong \mathrm{Aut}_K F(\zeta)/\mathrm{Aut}_F F(\zeta)$ (in Theorem V.2.5 we take $F = F(\zeta)$, $E = F$, $K = K$). This shows that $\mathrm{Aut}_K F$ is the homomorphic image of $\mathrm{Aut}_K F(\zeta)$ under canonical epimorphism (see page 43 on Section I.5). So to show that $\mathrm{Aut}_K F$ is solvable, it is sufficient by Theorem II.7.11(i) to show that $\mathrm{Aut}_K F(\zeta)$ is solvable. Observe that $K(\zeta)$ is an abelian (and so by the definition of Galois) extension of $K$ by Theorem V.8.1(ii). Whence by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii) with $F = F(\zeta)$, $E = K(\zeta)$, $K = K$) we have
$\mathrm{Aut}_K K(\zeta) \cong \mathrm{Aut}_K F(\zeta)/\mathrm{Aut}_{K(\zeta)} F(\zeta)$. Since $\mathrm{Aut}_K K(\zeta)$ is abelian then it is solvable trivially (see page 102).

# Theorem V.9.4 (continued 5)

**Proof (continued).** By Theorem V.8.1(ii), $F(\zeta)$ is an abelian extension of $F$ and so (by definition of "abelian extension") is Galois over $F$. By Exercise V.3.15(b), $F(\zeta)$ is Galois over $K$ ($F$ is Galois over $K$ WLOG as argued above, and $F(\zeta)$ is a splitting field of $x^m - 1$ over $F$). By the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) we have that $\mathrm{Aut}_K F \cong \mathrm{Aut}_K F(\zeta)/\mathrm{Aut}_F F(\zeta)$ (in Theorem V.2.5 we take $F = F(\zeta)$, $E = F$, $K = K$). This shows that $\mathrm{Aut}_K F$ is the homomorphic image of $\mathrm{Aut}_K F(\zeta)$ under canonical epimorphism (see page 43 on Section I.5). So to show that $\mathrm{Aut}_K F$ is solvable, it is sufficient by Theorem II.7.11(i) to show that $\mathrm{Aut}_K F(\zeta)$ is solvable. Observe that $K(\zeta)$ is an abelian (and so by the definition of Galois) extension of $K$ by Theorem V.8.1(ii). Whence by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii) with $F = F(\zeta)$, $E = K(\zeta)$, $K = K$) we have
$\mathrm{Aut}_K K(\zeta) \cong \mathrm{Aut}_K F(\zeta)/\mathrm{Aut}_{K(\zeta)} F(\zeta)$. Since $\mathrm{Aut}_K K(\zeta)$ is abelian then it is solvable trivially (see page 102).

# Theorem V.9.4 (continued 6)

**Proof (continued).** By Theorem II.7.11(ii), if we knew that $\mathrm{Aut}_{K(\zeta)}F(\zeta)$ were solvable, then we would know that $\mathrm{Aut}_K F(\zeta)$ is solvable and the proof would be complete. Thus we need only prove that $\mathrm{Aut}_{K(\zeta)}F(\zeta)$ is solvable.

As shown above, $F(\zeta)$ is Galois over $K$ and hence, by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)), over any intermediate field. Let $E_0 = K(\zeta)$ and define $E_i = K(\zeta, u_1, u_2, \ldots, u_i)$ for $i = 1, 2, \ldots, n$ so that $E_n = K(\zeta, u_1, u_2, \ldots, u_n) = F(\zeta)$.

# Theorem V.9.4 (continued 6)

**Proof (continued).** By Theorem II.7.11(ii), if we knew that $\text{Aut}_{K(\zeta)}F(\zeta)$ were solvable, then we would know that $\text{Aut}_K F(\zeta)$ is solvable and the proof would be complete. Thus we need only prove that $\text{Aut}_{K(\zeta)}F(\zeta)$ is solvable.

As shown above, $F(\zeta)$ is Galois over $K$ and hence, by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)), over any intermediate field. Let $E_0 = K(\zeta)$ and define $E_i = K(\zeta, u_1, u_2, \ldots, u_i)$ for $i = 1, 2, \ldots, n$ so that $E_n = K(\zeta, u_1, u_2, \ldots, u_n) = F(\zeta)$. Let $H_i = \text{Aut}_{E_i}F(\zeta)$ be the subgroup of $\text{Aut}_{K(\zeta)}F(\zeta))$ corresponding to field $E_i$ under Galois correspondence in the Fundamental Theorem of Galois Theory (Theorem V.2.5).

# Theorem V.9.4 (continued 6)

**Proof (continued).** By Theorem II.7.11(ii), if we knew that $\text{Aut}_{K(\zeta)}F(\zeta)$ were solvable, then we would know that $\text{Aut}_K F(\zeta)$ is solvable and the proof would be complete. Thus we need only prove that $\text{Aut}_{K(\zeta)}F(\zeta)$ is solvable.

As shown above, $F(\zeta)$ is Galois over $K$ and hence, by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)), over any intermediate field. Let $E_0 = K(\zeta)$ and define $E_i = K(\zeta, u_1, u_2, \ldots, u_i)$ for $i = 1, 2, \ldots, n$ so that $E_n = K(\zeta, u_1, u_2, \ldots, u_n) = F(\zeta)$. Let $H_i = \text{Aut}_{E_i}F(\zeta)$ be the subgroup of $\text{Aut}_{K(\zeta)}F(\zeta))$ corresponding to field $E_i$ under Galois correspondence in the Fundamental Theorem of Galois Theory (Theorem V.2.5).

# Theorem V.9.4 (continued 7)

**Proof (continued).** Schematically we have:

$$\begin{array}{ccccccccc}
H_n & < & H_{n-1} & < \cdots < & H_i & < \cdots < & H_0 \\
\| & & \| & & \| & & \| \\
\{e\} & < & \mathrm{Aut}_{E_{n-1}} F(\zeta) & < \cdots < & \mathrm{Aut}_{E_i} F(\zeta) & < \cdots < & \mathrm{Aut}_{K(\zeta)} F(\zeta) \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\
F(\zeta) = E_n & \subset & E_{n-1} & \subset \cdots \subset & E_i & \subset \cdots \subset & E_0 = K(\zeta)
\end{array}$$

Now $\zeta$ is an $m$th root of unity where $m = m_1 m_2 \cdots m_n$, so by Lemma V.7.10(i), $K(\zeta)$ contains a primitive $m_i$th root of unity for each $i$. Since $u_i^{m_i} \in E_{i-1}$ and $E_i = E_{i-1}(u_i)$, then by Lemma V.7.10(ii) (with $d = m_i$), $E_i$ is a splitting field of $x^{m_i} - 1$ over $E_{i-1}$.

# Theorem V.9.4 (continued 7)

**Proof (continued).** Schematically we have:

$$\begin{array}{ccccccccc} & H_n & < & H_{n-1} & <\cdots< & H_i & <\cdots< & H_0 \\ & \| & & \| & & \| & & \| \\ & \{e\} & < & \mathrm{Aut}_{E_{n-1}}F(\zeta) & <\cdots< & \mathrm{Aut}_{E_i}F(\zeta) & <\cdots< & \mathrm{Aut}_{K(\zeta)}F(\zeta) \\ & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ F(\zeta) = & E_n & \subset & E_{n-1} & \subset\cdots\subset & E_i & \subset\cdots\subset & E_0 = K(\zeta) \end{array}$$

Now $\zeta$ is an $m$th root of unity where $m = m_1 m_2 \cdots m_n$, so by Lemma V.7.10(i), $K(\zeta)$ contains a primitive $m_i$th root of unity for each $i$. Since $u_i^{m_i} \in E_{i-1}$ and $E_i = E_{i-1}(u_i)$, then by Lemma V.7.10(ii) (with $d = m_i$), $E_i$ is a splitting field of $x^{m_i} - 1$ over $E_{i-1}$. By Theorem V.7.11 (the (ii)$\Rightarrow$(i) part), $E_i$ is a cyclic extension of $E_{i-1}$; that is, $\mathrm{Aut}_{E_{i-1}} E_i$ is a cyclic group. By definition of "cyclic extension," $E_i$ is Galois over $E_{i-1}$.

# Theorem V.9.4 (continued 7)

**Proof (continued).** Schematically we have:

$$\begin{array}{ccccccccc} & H_n & < & H_{n-1} & < \cdots < & H_i & < \cdots < & H_0 \\ & \| & & \| & & \| & & \| \\ & \{e\} & < & \mathrm{Aut}_{E_{n-1}} F(\zeta) & < \cdots < & \mathrm{Aut}_{E_i} F(\zeta) & < \cdots < & \mathrm{Aut}_{K(\zeta)} F(\zeta) \\ & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ F(\zeta) = & E_n & \subset & E_{n-1} & \subset \cdots \subset & E_i & \subset \cdots \subset & E_0 = K(\zeta) \end{array}$$

Now $\zeta$ is an $m$th root of unity where $m = m_1 m_2 \cdots m_n$, so by Lemma V.7.10(i), $K(\zeta)$ contains a primitive $m_i$th root of unity for each $i$. Since $u_i^{m_i} \in E_{i-1}$ and $E_i = E_{i-1}(u_i)$, then by Lemma V.7.10(ii) (with $d = m_i$), $E_i$ is a splitting field of $x^{m_i} - 1$ over $E_{i-1}$. By Theorem V.7.11 (the (ii)⇒(i) part), $E_i$ is a cyclic extension of $E_{i-1}$; that is, $\mathrm{Aut}_{E_{i-1}} E_i$ is a cyclic group. By definition of "cyclic extension," $E_i$ is Galois over $E_{i-1}$.

# Theorem V.9.4 (continued 8)

**Theorem V.9.4.** If $F$ is a radical extension field of $K$ and $E$ is an intermediate field, then $\mathrm{Aut}_K(E)$ is a solvable group.

**Proof (continued).** So by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) we have the normal subgroups $J_i \triangleleft H_{i-1}$ (or equivalently, $\mathrm{Aut}_{E_i}F(\zeta) \triangleleft \mathrm{Aut}_{E_{i-1}}F(\zeta)$) and $H_{i-1}/H_i = \mathrm{Aut}_{E_{i-1}}F(\zeta)/\mathrm{Aut}_{E_i}F(\zeta) \cong \mathrm{Aut}_{E_{i-1}}E_i$ (with $F = F(\zeta)$, $E = E_i$, $K = E_{i-1}$ in Theorem V.2.5(ii)). So $H_{i-1}/H_i \cong \mathrm{Aut}_{E_{i-1}}E_i$ is cyclic (and so abelian). Consequently, $\{e\} = H_n < H_{n-1} < \cdots < J_1 < H_0 = \mathrm{Aut}_{K(\zeta)}F(\zeta)$ is a solvable series by definition (see Definition II.8.3). By Theorem II.8.5, $\mathrm{Aut}_{K(\zeta)}F(\zeta)$ is solvable.

# Theorem V.9.4 (continued 8)

**Theorem V.9.4.** If $F$ is a radical extension field of $K$ and $E$ is an intermediate field, then $\mathrm{Aut}_K(E)$ is a solvable group.

**Proof (continued).** So by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) we have the normal subgroups $J_i \triangleleft H_{i-1}$ (or equivalently, $\mathrm{Aut}_{E_i} F(\zeta) \triangleleft \mathrm{Aut}_{E_{i-1}} F(\zeta)$) and $H_{i-1}/H_i = \mathrm{Aut}_{E_{i-1}} F(\zeta)/\mathrm{Aut}_{E_i} F(\zeta) \cong \mathrm{Aut}_{E_{i-1}} E_i$ (with $F = F(\zeta)$, $E = E_i$, $K = E_{i-1}$ in Theorem V.2.5(ii)). So $H_{i-1}/H_i \cong \mathrm{Aut}_{E_{i-1}} E_i$ is cyclic (and so abelian). Consequently, $\{e\} = H_n < H_{n-1} < \cdots < J_1 < H_0 = \mathrm{Aut}_{K(\zeta)} F(\zeta)$ is a solvable series by definition (see Definition II.8.3). By Theorem II.8.5, $\mathrm{Aut}_{K(\zeta)} F(\zeta)$ is solvable. Therefore, this result cascades back through the line of implications and WLOG's to imply that $\mathrm{Aut}_K E$ is solvable. □

# Theorem V.9.4 (continued 8)

**Theorem V.9.4.** If $F$ is a radical extension field of $K$ and $E$ is an intermediate field, then $\text{Aut}_K(E)$ is a solvable group.

**Proof (continued).** So by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) we have the normal subgroups $J_i \lhd H_{i-1}$ (or equivalently, $\text{Aut}_{E_i} F(\zeta) \lhd \text{Aut}_{E_{i-1}} F(\zeta)$) and $H_{i-1}/H_i = \text{Aut}_{E_{i-1}} F(\zeta)/\text{Aut}_{E_i} F(\zeta) \cong \text{Aut}_{E_{i-1}} E_i$ (with $F = F(\zeta)$, $E = E_i$, $K = E_{i-1}$ in Theorem V.2.5(ii)). So $H_{i-1}/H_i \cong \text{Aut}_{E_{i-1}} E_i$ is cyclic (and so abelian). Consequently, $\{e\} = H_n < H_{n-1} < \cdots < J_1 < H_0 = \text{Aut}_{K(\zeta)} F(\zeta)$ is a solvable series by definition (see Definition II.8.3). By Theorem II.8.5, $\text{Aut}_{K(\zeta)} F(\zeta)$ is solvable. Therefore, this result cascades back through the line of implications and WLOG's to imply that $\text{Aut}_K E$ is solvable. □

# Corollary V.9.5

**Corollary V.9.5.** Let $K$ be a field and $f \in K[x]$. If the equation $f(x) = 0$ is solvable by radicals, then the Galois group of $f$ is a solvable group.

**Proof.** If $f(x) = 0$ is solvable by radicals, then by Definition V.9.2, there is a radical extension $F$ of $K$ and a splitting field $E$ of $f$ over $K$ such that $F \supset E \supset K$.

# Corollary V.9.5

**Corollary V.9.5.** Let $K$ be a field and $f \in K[x]$. If the equation $f(x) = 0$ is solvable by radicals, then the Galois group of $f$ is a solvable group.

**Proof.** If $f(x) = 0$ is solvable by radicals, then by Definition V.9.2, there is a radical extension $F$ of $K$ and a splitting field $E$ of $f$ over $K$ such that $F \supset E \supset K$. The Galois group of $f$ is $\mathrm{Aut}_K E$ by Definition V.4.1. By Theorem V.9.4, $\mathrm{Aut}_K E$ is a solvable group. □

# Corollary V.9.5

**Corollary V.9.5.** Let $K$ be a field and $f \in K[x]$. If the equation $f(x) = 0$ is solvable by radicals, then the Galois group of $f$ is a solvable group.

**Proof.** If $f(x) = 0$ is solvable by radicals, then by Definition V.9.2, there is a radical extension $F$ of $K$ and a splitting field $E$ of $f$ over $K$ such that $F \supset E \supset K$. The Galois group of $f$ is $\text{Aut}_K E$ by Definition V.4.1. By Theorem V.9.4, $\text{Aut}_K E$ is a solvable group. □

# Proposition V.9.6

**Proposition V.9.6.** Let $E$ be a finite dimensional Galois extension field of $K$ with solvable Galois group $\mathrm{Aut}_K(F)$. Assume that $\mathrm{char}(K)$ does not divide $[E : K]$. Then there exists a radical extension $F$ of $K$ such that $F \supset E \supset K$.

**Proof.** By the Fundamental Theorem of Galois Theory (theorem V.2.5(i)), $|\mathrm{Aut}_K E| = [E : K]$, so $\mathrm{Aut}_K E$ is a finite solvable group. By Proposition II.8.6, $\mathrm{Aut}_K E$ has a composition series whose factors are cyclic of prime order.

# Proposition V.9.6

**Proposition V.9.6.** Let $E$ be a finite dimensional Galois extension field of $K$ with solvable Galois group $\mathrm{Aut}_K(F)$. Assume that $\mathrm{char}(K)$ does not divide $[E : K]$. Then there exists a radical extension $F$ of $K$ such that $F \supset E \supset K$.

**Proof.** By the Fundamental Theorem of Galois Theory (theorem V.2.5(i)), $|\mathrm{Aut}_K E| = [E : K]$, so $\mathrm{Aut}_K E$ is a finite solvable group. By Proposition II.8.6, $\mathrm{Aut}_K E$ has a composition series whose factors are cyclic of prime order. So there is a normal subgroup $H$ of $\mathrm{Aut}_K E$ of some prime index $p$; that is, $p = |(\mathrm{Aut}_K E)/H| = |\mathrm{Aut}_K E|/|H| = [E : K]/|H|$ and so $[E : K] = p|H|$. Since $\mathrm{char}(K) \nmid [E : K]$ then $\mathrm{char}(K) \nmid p$.

# Proposition V.9.6

**Proposition V.9.6.** Let $E$ be a finite dimensional Galois extension field of $K$ with solvable Galois group $\mathrm{Aut}_K(F)$. Assume that $\mathrm{char}(K)$ does not divide $[E:K]$. Then there exists a radical extension $F$ of $K$ such that $F \supset E \supset K$.

**Proof.** By the Fundamental Theorem of Galois Theory (theorem V.2.5(i)), $|\mathrm{Aut}_K E| = [E:K]$, so $\mathrm{Aut}_K E$ is a finite solvable group. By Proposition II.8.6, $\mathrm{Aut}_K E$ has a composition series whose factors are cyclic of prime order. So there is a normal subgroup $H$ of $\mathrm{Aut}_K E$ of some prime index $p$; that is, $p = |(\mathrm{Aut}_K E)/H| = |\mathrm{Aut}_K E|/|H| = [E:K]/|H|$ and so $[E:K] = p|H|$. Since $\mathrm{char}(K) \nmid [E:K]$ then $\mathrm{char}(K) \nmid p$. Let $N = E(\zeta)$ be a cyclotomic extension of $E$ where $\zeta$ is a primitive $p$th root of unity (which can be done by Theorem V.8.1(i)). Define $M = K(\zeta)$.

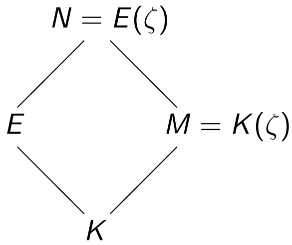
# Proposition V.9.6

**Proposition V.9.6.** Let $E$ be a finite dimensional Galois extension field of $K$ with solvable Galois group $\text{Aut}_K(F)$. Assume that $\text{char}(K)$ does not divide $[E : K]$. Then there exists a radical extension $F$ of $K$ such that $F \supset E \supset K$.

**Proof.** By the Fundamental Theorem of Galois Theory (theorem V.2.5(i)), $|\text{Aut}_K E| = [E : K]$, so $\text{Aut}_K E$ is a finite solvable group. By Proposition II.8.6, $\text{Aut}_K E$ has a composition series whose factors are cyclic of prime order. So there is a normal subgroup $H$ of $\text{Aut}_K E$ of some prime index $p$; that is, $p = |(\text{Aut}_K E)/H| = |\text{Aut}_K E|/|H| = [E : K]/|H|$ and so $[E : K] = p|H|$. Since $\text{char}(K) \nmid [E : K]$ then $\text{char}(K) \nmid p$. Let $N = E(\zeta)$ be a cyclotomic extension of $E$ where $\zeta$ is a primitive $p$th root of unity (which can be done by Theorem V.8.1(i)). Define $M = K(\zeta)$.

# Proposition V.9.6 (continued 1)

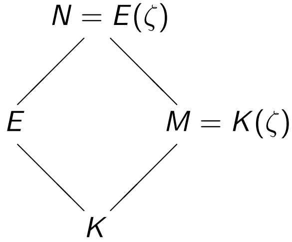
**Proof (continued).** Then we have:




By Theorem V.8.1(ii), $N$ is a finite dimensional abelian extension of $E$ and so, by the definition of "abelian extension," $N$ is Galois over $E$ and, by Exercise V.3.15(b), $N$ is Galois over $K$.

# Proposition V.9.6 (continued 1)

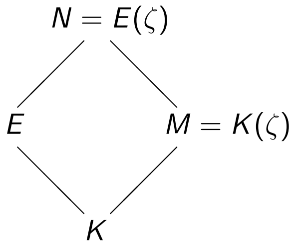
**Proof (continued).** Then we have:




By Theorem V.8.1(ii), $N$ is a finite dimensional abelian extension of $E$ and so, by the definition of "abelian extension," $N$ is Galois over $E$ and, by Exercise V.3.15(b), $N$ is Galois over $K$. Now $M = K(\zeta)$ is clearly a radical extension of $K$. If we can find a radical extension of $M$ that contains $N = E(\zeta)$, then this extension will be radical over $K$ by Exercise V.9.4 (since $M$ is radical over $K$) and this extension will be the desired extension $F$.

# Proposition V.9.6 (continued 1)

**Proof (continued).** Then we have:




By Theorem V.8.1(ii), $N$ is a finite dimensional abelian extension of $E$ and so, by the definition of "abelian extension," $N$ is Galois over $E$ and, by Exercise V.3.15(b), $N$ is Galois over $K$. Now $M = K(\zeta)$ is clearly a radical extension of $K$. If we can find a radical extension of $M$ that contains $N = E(\zeta)$, then this extension will be radical over $K$ by Exercise V.9.4 (since $M$ is radical over $K$) and this extension will be the desired extension $F$.

# Proposition V.9.6 (continued 2)

**Proof (continued).** First, observe that $E$ is a stable intermediate field between $N$ and $K$ by Lemma V.2.13 (since $E$ is Galois over $K$ and algebraic over $K$ by Theorem V.1.11). That is, every $K$-automorphism in $\mathrm{Aut}_K N$ maps $E$ into itself. Consequently, for any $\sigma \in \mathrm{Aut}_K N$ we can restrict $\sigma$ to $E$ (i.e., $\sigma|_E$) to produce an element of $\mathrm{Aut}_K E$. Now since $K \subset M = K(\zeta)$ then $\mathrm{Aut}_M N < \mathrm{Aut}_K E$.

# Proposition V.9.6 (continued 2)

**Proof (continued).** First, observe that $E$ is a stable intermediate field between $N$ and $K$ by Lemma V.2.13 (since $E$ is Galois over $K$ and algebraic over $K$ by Theorem V.1.11). That is, every $K$-automorphism in $\mathrm{Aut}_K N$ maps $E$ into itself. Consequently, for any $\sigma \in \mathrm{Aut}_K N$ we can restrict $\sigma$ to $E$ (i.e., $\sigma|_E$) to produce an element of $\mathrm{Aut}_K E$. Now since $K \subset M = K(\zeta)$ then $\mathrm{Aut}_M N < \mathrm{Aut}_K E$. Let $\theta : \mathrm{Aut}_M N \to \mathrm{Aut}_K E$ be defined as $\theta(\sigma) = \sigma|_E$. Then $\theta$ is a homomorphism because $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|E = \sigma_1|E\sigma_2|E = \theta(\sigma_1)\theta(\sigma_2)$.

# Proposition V.9.6 (continued 2)

**Proof (continued).** First, observe that $E$ is a stable intermediate field between $N$ and $K$ by Lemma V.2.13 (since $E$ is Galois over $K$ and algebraic over $K$ by Theorem V.1.11). That is, every $K$-automorphism in $\mathrm{Aut}_K N$ maps $E$ into itself. Consequently, for any $\sigma \in \mathrm{Aut}_K N$ we can restrict $\sigma$ to $E$ (i.e., $\sigma|_E$) to produce an element of $\mathrm{Aut}_K E$. Now since $K \subset M = K(\zeta)$ then $\mathrm{Aut}_M N < \mathrm{Aut}_K E$. Let $\theta : \mathrm{Aut}_M N \to \mathrm{Aut}_K E$ be defined as $\theta(\sigma) = \sigma|_E$. Then $\theta$ is a homomorphism because $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|E = \sigma_1|E\sigma_2|E = \theta(\sigma_1)\theta(\sigma_2)$. If $\sigma \in \mathrm{Aut}_M N$ then $\sigma(\zeta) = \zeta$ (since $M = K(\zeta)$). If $\sigma \in \mathrm{Ker}(\theta)$ then $\sigma|E$ must be the identity and since $N = E(\zeta)$ then $\sigma$ must be the identity on $N$. So by Theorem I.2.3(i), $\theta$ is one to one and so is a monomorphism.

# Proposition V.9.6 (continued 2)

**Proof (continued).** First, observe that $E$ is a stable intermediate field between $N$ and $K$ by Lemma V.2.13 (since $E$ is Galois over $K$ and algebraic over $K$ by Theorem V.1.11). That is, every $K$-automorphism in $\mathrm{Aut}_K N$ maps $E$ into itself. Consequently, for any $\sigma \in \mathrm{Aut}_K N$ we can restrict $\sigma$ to $E$ (i.e., $\sigma|_E$) to produce an element of $\mathrm{Aut}_K E$. Now since $K \subset M = K(\zeta)$ then $\mathrm{Aut}_M N < \mathrm{Aut}_K E$. Let $\theta : \mathrm{Aut}_M N \to \mathrm{Aut}_K E$ be defined as $\theta(\sigma) = \sigma|_E$. Then $\theta$ is a homomorphism because $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|E = \sigma_1|E\sigma_2|E = \theta(\sigma_1)\theta(\sigma_2)$. If $\sigma \in \mathrm{Aut}_M N$ then $\sigma(\zeta) = \zeta$ (since $M = K(\zeta)$). If $\sigma \in \mathrm{Ker}(\theta)$ then $\sigma|E$ must be the identity and since $N = E(\zeta)$ then $\sigma$ must be the identity on $N$. So by Theorem I.2.3(i), $\theta$ is one to one and so is a monomorphism.

We now prove the theorem by induction on $n = [E : K]$. In the case $[E : K] = 1$ we have $E = K$ and $M = K(\zeta)$ is the desired radical extension $F$. Assume the theorem is true for all extensions of dimension $k < n$ and consider the two possibilities:

# Proposition V.9.6 (continued 2)

**Proof (continued).** First, observe that $E$ is a stable intermediate field between $N$ and $K$ by Lemma V.2.13 (since $E$ is Galois over $K$ and algebraic over $K$ by Theorem V.1.11). That is, every $K$-automorphism in $\mathrm{Aut}_K N$ maps $E$ into itself. Consequently, for any $\sigma \in \mathrm{Aut}_K N$ we can restrict $\sigma$ to $E$ (i.e., $\sigma|_E$) to produce an element of $\mathrm{Aut}_K E$. Now since $K \subset M = K(\zeta)$ then $\mathrm{Aut}_M N < \mathrm{Aut}_K E$. Let $\theta : \mathrm{Aut}_M N \to \mathrm{Aut}_K E$ be defined as $\theta(\sigma) = \sigma|_E$. Then $\theta$ is a homomorphism because $\theta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|E = \sigma_1|E\sigma_2|E = \theta(\sigma_1)\theta(\sigma_2)$. If $\sigma \in \mathrm{Aut}_M N$ then $\sigma(\zeta) = \zeta$ (since $M = K(\zeta)$). If $\sigma \in \mathrm{Ker}(\theta)$ then $\sigma|E$ must be the identity and since $N = E(\zeta)$ then $\sigma$ must be the identity on $N$. So by Theorem I.2.3(i), $\theta$ is one to one and so is a monomorphism.

We now prove the theorem by induction on $n = [E : K]$. In the case $[E : K] = 1$ we have $E = K$ and $M = K(\zeta)$ is the desired radical extension $F$. Assume the theorem is true for all extensions of dimension $k < n$ and consider the two possibilities:

# Proposition V.9.6 (continued 3)

**Proof (continued).**

(i) $\text{Aut}_M N$ is isomorphic under $\theta$ to a proper subgroup of $\text{Aut}_K E$;

(ii) $\text{Aut}_M N \cong \text{Aut}_K E$ and $\theta$ is an isomorphism.

Since $\text{Aut}_K E$ is solvable, then by Theorem II.7.11(i) we have that $\text{Aut}_M N$ is solvable in either case. Since $E$ is a finite dimensional extension of $K$ by hypothesis an d$N = E(\zeta)$ is a finite dimensional extension of $E$ (by Theorem V.1.6(iii)) then $N$ is a finite dimensional extension of $K$ by Theorem V.1.2.

# Proposition V.9.6 (continued 3)

**Proof (continued).**

(i) $\text{Aut}_M N$ is isomorphic under $\theta$ to a proper subgroup of $\text{Aut}_K E$;

(ii) $\text{Aut}_M N \cong \text{Aut}_K E$ and $\theta$ is an isomorphism.

Since $\text{Aut}_K E$ is solvable, then by Theorem II.7.11(i) we have that $\text{Aut}_M N$ is solvable in either case. Since $E$ is a finite dimensional extension of $K$ by hypothesis an d$N = E(\zeta)$ is a finite dimensional extension of $E$ (by Theorem V.1.6(iii)) then $N$ is a finite dimensional extension of $K$ by Theorem V.1.2. As shown above (after the diagram) $N$ is Galois over $K$ and so by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) $N$ is Galois over the intermediate field $M = K(\zeta)$. In case (i) we have $[N : M] = |\text{Aut}MN|$ and $[E : K] = |\text{Aut}_K E| = n$ by Theorem V.2.15(i) and so $[N : M] < [E : K] = n$.

# Proposition V.9.6 (continued 3)

**Proof (continued).**

(i) $\text{Aut}_M N$ is isomorphic under $\theta$ to a proper subgroup of $\text{Aut}_K E$;

(ii) $\text{Aut}_M N \cong \text{Aut}_K E$ and $\theta$ is an isomorphism.

Since $\text{Aut}_K E$ is solvable, then by Theorem II.7.11(i) we have that $\text{Aut}_M N$ is solvable in either case. Since $E$ is a finite dimensional extension of $K$ by hypothesis an d$N = E(\zeta)$ is a finite dimensional extension of $E$ (by Theorem V.1.6(iii)) then $N$ is a finite dimensional extension of $K$ by Theorem V.1.2. As shown above (after the diagram) $N$ is Galois over $K$ and so by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) $N$ is Galois over the intermediate field $M = K(\zeta)$. In case (i) we have $[N : M] = |\text{Aut}MN|$ and $[E : K] = |\text{Aut}_K E| = n$ by Theorem V.2.15(i) and so $[N : M] < [E : K] = n$. Whence by the induction hypothesis there is a radical extension of $M$ that contains $N$. As remarked in the first paragraph, this proves the theorem in case (i).

# Proposition V.9.6 (continued 3)

**Proof (continued).**

(i) $\text{Aut}_M N$ is isomorphic under $\theta$ to a proper subgroup of $\text{Aut}_K E$;

(ii) $\text{Aut}_M N \cong \text{Aut}_K E$ and $\theta$ is an isomorphism.

Since $\text{Aut}_K E$ is solvable, then by Theorem II.7.11(i) we have that $\text{Aut}_M N$ is solvable in either case. Since $E$ is a finite dimensional extension of $K$ by hypothesis an d$N = E(\zeta)$ is a finite dimensional extension of $E$ (by Theorem V.1.6(iii)) then $N$ is a finite dimensional extension of $K$ by Theorem V.1.2. As shown above (after the diagram) $N$ is Galois over $K$ and so by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) $N$ is Galois over the intermediate field $M = K(\zeta)$. In case (i) we have $[N : M] = |\text{Aut}MN|$ and $[E : K] = |\text{Aut}_K E| = n$ by Theorem V.2.15(i) and so $[N : M] < [E : K] = n$. Whence by the induction hypothesis there is a radical extension of $M$ that contains $N$. As remarked in the first paragraph, this proves the theorem in case (i).

# Proposition V.9.6 (continued 4)

**Proof.** In case (ii), let $J = \theta^{-1}(H)$. Notice that $\theta : \text{Aut}_M N \to \text{Aut}_K E$ is an isomorphism in this case, so $\theta^{-1} : \text{Aut}_K E \to \text{Aut}_M N$ is an isomorphism and since $H$ is a normal subgroup of index $p$ in $\text{Aut}_K E$, then $J$ is a normal subgroup of index $p$ in $\text{Aut}_M N$. Since $\text{Aut}_K E$ is solvable and $\text{Aut}_M N \cong \text{Aut}_K E$, then $\text{Aut}_M N$ is solvable and by Theorem II.7.11(i), $J < \text{Aut}_M N$ is solvable. Let $P$ be the fixed field of $J$ relative to $\text{Aut}_M N$.

# Proposition V.9.6 (continued 4)

**Proof.** In case (ii), let $J = \theta^{-1}(H)$. Notice that $\theta : \text{Aut}_M N \to \text{Aut}_K E$ is an isomorphism in this case, so $\theta^{-1} : \text{Aut}_K E \to \text{Aut}_M N$ is an isomorphism and since $H$ is a normal subgroup of index $p$ in $\text{Aut}_K E$, then $J$ is a normal subgroup of index $p$ in $\text{Aut}_M N$. Since $\text{Aut}_K E$ is solvable and $\text{Aut}_M N \cong \text{Aut}_K E$, then $\text{Aut}_M N$ is solvable and by Theorem II.7.11(i), $J < \text{Aut}_M N$ is solvable. Let $P$ be the fixed field of $J$ relative to $\text{Aut}_M N$. Then we have

$$\begin{array}{ccccc} \{\iota\} & \lhd & J = \text{Aut}_P N & \lhd & \text{Aut}_M N \\ \updownarrow & & \updownarrow & & \updownarrow \\ N & \supset & P & \supset & M \end{array}$$

# Proposition V.9.6 (continued 4)

**Proof.** In case (ii), let $J = \theta^{-1}(H)$. Notice that $\theta : \mathrm{Aut}_M N \to \mathrm{Aut}_K E$ is an isomorphism in this case, so $\theta^{-1} : \mathrm{Aut}_K E \to \mathrm{Aut}_M N$ is an isomorphism and since $H$ is a normal subgroup of index $p$ in $\mathrm{Aut}_K E$, then $J$ is a normal subgroup of index $p$ in $\mathrm{Aut}_M N$. Since $\mathrm{Aut}_K E$ is solvable and $\mathrm{Aut}_M N \cong \mathrm{Aut}_K E$, then $\mathrm{Aut}_M N$ is solvable and by Theorem II.7.11(i), $J < \mathrm{Aut}_M N$ is solvable. Let $P$ be the fixed field of $J$ relative to $\mathrm{Aut}_M N$. Then we have

$$\begin{array}{ccccc} \{\iota\} & \lhd & J = \mathrm{Aut}_P N & \lhd & \mathrm{Aut}_M N \\ \updownarrow & & \updownarrow & & \updownarrow \\ N & \supset & P & \supset & M \end{array}$$

Notice that since $P$ is the fixed field of $J$ and $P$ is Galois over $M$ by Theorem V.2.15(ii), so $J = \mathrm{Aut}_P N$. Also be Theorem V.2.5(ii) (with $F = n$, $E = P$, and $K = M$) we have $\mathrm{Aut}_M P \cong (\mathrm{Aut}_M N)/(\mathrm{Aut}_P N) = (\mathrm{Aut}_M N)/J$.

# Proposition V.9.6 (continued 4)

**Proof.** In case (ii), let $J = \theta^{-1}(H)$. Notice that $\theta : \mathrm{Aut}_M N \to \mathrm{Aut}_K E$ is an isomorphism in this case, so $\theta^{-1} : \mathrm{Aut}_K E \to \mathrm{Aut}_M N$ is an isomorphism and since $H$ is a normal subgroup of index $p$ in $\mathrm{Aut}_K E$, then $J$ is a normal subgroup of index $p$ in $\mathrm{Aut}_M N$. Since $\mathrm{Aut}_K E$ is solvable and $\mathrm{Aut}_M N \cong \mathrm{Aut}_K E$, then $\mathrm{Aut}_M N$ is solvable and by Theorem II.7.11(i), $J < \mathrm{Aut}_M N$ is solvable. Let $P$ be the fixed field of $J$ relative to $\mathrm{Aut}_M N$. Then we have

$$\begin{array}{ccccc} \{\iota\} & \lhd & J = \mathrm{Aut}_P N & \lhd & \mathrm{Aut}_M N \\ \updownarrow & & \updownarrow & & \updownarrow \\ N & \supset & P & \supset & M \end{array}$$

Notice that since $P$ is the fixed field of $J$ and $P$ is Galois over $M$ by Theorem V.2.15(ii), so $J = \mathrm{Aut}_P N$. Also be Theorem V.2.5(ii) (with $F = n$, $E = P$, and $K = M$) we have $\mathrm{Aut}_M P \cong (\mathrm{Aut}_M N)/(\mathrm{Aut}_P N) = (\mathrm{Aut}_M N)/J$. But $[\mathrm{Aut}_M N : J] = p$ be construction, whence $\mathrm{Aut}_M P \cong \mathbb{Z}_p$ by Exercise I.4.3. Therefore $P$ is a cyclic extension of $M = K(\zeta)$.

# Proposition V.9.6 (continued 4)

**Proof.** In case (ii), let $J = \theta^{-1}(H)$. Notice that $\theta : \text{Aut}_M N \to \text{Aut}_K E$ is an isomorphism in this case, so $\theta^{-1} : \text{Aut}_K E \to \text{Aut}_M N$ is an isomorphism and since $H$ is a normal subgroup of index $p$ in $\text{Aut}_K E$, then $J$ is a normal subgroup of index $p$ in $\text{Aut}_M N$. Since $\text{Aut}_K E$ is solvable and $\text{Aut}_M N \cong \text{Aut}_K E$, then $\text{Aut}_M N$ is solvable and by Theorem II.7.11(i), $J < \text{Aut}_M N$ is solvable. Let $P$ be the fixed field of $J$ relative to $\text{Aut}_M N$. Then we have

$$\begin{array}{ccccc} \{\iota\} & \lhd & J = \text{Aut}_P N & \lhd & \text{Aut}_M N \\ \updownarrow & & \updownarrow & & \updownarrow \\ N & \supset & P & \supset & M \end{array}$$

Notice that since $P$ is the fixed field of $J$ and $P$ is Galois over $M$ by Theorem V.2.15(ii), so $J = \text{Aut}_P N$. Also be Theorem V.2.5(ii) (with $F = n$, $E = P$, and $K = M$) we have $\text{Aut}_M P \cong (\text{Aut}_M N)/(\text{Aut}_P N) = (\text{Aut}_M N)/J$. But $[\text{Aut}_M N : J] = p$ be construction, whence $\text{Aut}_M P \cong \mathbb{Z}_p$ by Exercise I.4.3. Therefore $P$ is a cyclic extension of $M = K(\zeta)$.

# Proposition V.9.6 (continued 5)

**Proposition V.9.6.** Let $E$ be a finite dimensional Galois extension field of $K$ with solvable Galois group $\text{Aut}_K(F)$. Assume that char$(K)$ does not divide $[E : K]$. Then there exists a radical extension $F$ of $K$ such that $F \supset E \supset K$.

**Proof (continued).** By Theorem V.7.11(ii), $P = M(u)$ where $u$ is a root of some irreducible $x^p - a \in M[x]$. Thus $P$ is a radical extension of $M$ where $[P : M] > 1$ and, since $[N : M] = [N : P][P : M]$ by Theorem V.1.2, then $[N : P] < [N : M] = [F : K] = n$ (since $\text{Aut}_M N \cong \text{Aut}_K E$ in case (ii)). Since $\text{Aut}_P N = J$ is solvable and $N$ is Galois over $P$ by Theorem V.2.5(ii), the induction hypothesis implies that there is a radical extension $F$ of $P$ that contains $N$.

# Proposition V.9.6 (continued 5)

**Proposition V.9.6.** Let $E$ be a finite dimensional Galois extension field of $K$ with solvable Galois group $\mathrm{Aut}_K(F)$. Assume that char$(K)$ does not divide $[E : K]$. Then there exists a radical extension $F$ of $K$ such that $F \supset E \supset K$.

**Proof (continued).** By Theorem V.7.11(ii), $P = M(u)$ where $u$ is a root of some irreducible $x^p - a \in M[x]$. Thus $P$ is a radical extension of $M$ where $[P : M] > 1$ and, since $[N : M] = [N : P][P : M]$ by Theorem V.1.2, then $[N : P] < [N : M] = [F : K] = n$ (since $\mathrm{Aut}_M N \cong \mathrm{Aut}_K E$ in case (ii)). Since $\mathrm{Aut}_P N = J$ is solvable and $N$ is Galois over $P$ by Theorem V.2.5(ii), the induction hypothesis implies that there is a radical extension $F$ of $P$ that contains $N$. Since $F$ is a radical extension of $P$ and $P$ is a radical extension of $M = K(\zeta)$ (and so $K(\zeta)$ is a radical extension of $K$), then $F$ is a radical extension of $K$ which contains $N = E(\zeta)$ and hence contains $K$. So the result holds in case (iii). □

# Proposition V.9.6 (continued 5)

**Proposition V.9.6.** Let $E$ be a finite dimensional Galois extension field of $K$ with solvable Galois group $\text{Aut}_K(F)$. Assume that $\text{char}(K)$ does not divide $[E : K]$. Then there exists a radical extension $F$ of $K$ such that $F \supset E \supset K$.

**Proof (continued).** By Theorem V.7.11(ii), $P = M(u)$ where $u$ is a root of some irreducible $x^p - a \in M[x]$. Thus $P$ is a radical extension of $M$ where $[P : M] > 1$ and, since $[N : M] = [N : P][P : M]$ by Theorem V.1.2, then $[N : P] < [N : M] = [F : K] = n$ (since $\text{Aut}_M N \cong \text{Aut}_K E$ in case (ii)). Since $\text{Aut}_P N = J$ is solvable and $N$ is Galois over $P$ by Theorem V.2.5(ii), the induction hypothesis implies that there is a radical extension $F$ of $P$ that contains $N$. Since $F$ is a radical extension of $P$ and $P$ is a radical extension of $M = K(\zeta)$ (and so $K(\zeta)$ is a radical extension of $K$), then $F$ is a radical extension of $K$ which contains $N = E(\zeta)$ and hence contains $K$. So the result holds in case (iii). □

# Corollary V.9.7. Galois' Theorem

**Corollary V.9.7. Galois' Theorem.** Let $K$ be a field and $f \in K[x]$ a polynomial of degree $n > 0$, where $\text{char}(K)$ does not divide $n!$ (which is always true when $\text{char}(K) = 0$). Then the equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f$ is solvable.

**Proof.** (1) Suppose $f(x) = 0$ is solvable by radicals. Then (by Definition V.9.2) there is a radical extension $E$ of $K$ and a splitting field $E$ of $f$ over $K$ such that $F \supset E \supset K$.

# Corollary V.9.7. Galois' Theorem

**Corollary V.9.7. Galois' Theorem.** Let $K$ be a field and $f \in K[x]$ a polynomial of degree $n > 0$, where char($K$) does not divide $n$! (which is always true when char($K$) = 0). Then the equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f$ is solvable.

**Proof.** (1) Suppose $f(x) = 0$ is solvable by radicals. Then (by Definition V.9.2) there is a radical extension $E$ of $K$ and a splitting field $E$ of $f$ over $K$ such that $F \supset E \supset K$. By Definition V.4.1, the Galois group of $f$ is $\text{Aut}_K E$. By Theorem V.9.4, $\text{Aut}_K F$ is solvable.

# Corollary V.9.7. Galois' Theorem

**Corollary V.9.7. Galois' Theorem.** Let $K$ be a field and $f \in K[x]$ a polynomial of degree $n > 0$, where $\mathrm{char}(K)$ does not divide $n!$ (which is always true when $\mathrm{char}(K) = 0$). Then the equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f$ is solvable.

**Proof.** (1) Suppose $f(x) = 0$ is solvable by radicals. Then (by Definition V.9.2) there is a radical extension $E$ of $K$ and a splitting field $E$ of $f$ over $K$ such that $F \supset E \supset K$. By Definition V.4.1, the Galois group of $f$ is $\mathrm{Aut}_K E$. By Theorem V.9.4, $\mathrm{Aut}_K F$ is solvable.
(2) Suppose the Galois group of $f$ is solvable. So let $E$ be a splitting field of $f$ over $K$ (which exists since the algebraic closure of $K$ exists by Theorem V.3.6). Then this means that $\mathrm{Aut}_K E$ is solvable. Notice that $E$ can be chosen to be a finite dimensional extension by Theorem V.3.2, with $[E : K] \leq n!$.

# Corollary V.9.7. Galois' Theorem

**Corollary V.9.7. Galois' Theorem.** Let $K$ be a field and $f \in K[x]$ a polynomial of degree $n > 0$, where char$(K)$ does not divide $n!$ (which is always true when char$(K) = 0$). Then the equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f$ is solvable.

**Proof.** (1) Suppose $f(x) = 0$ is solvable by radicals. Then (by Definition V.9.2) there is a radical extension $E$ of $K$ and a splitting field $E$ of $f$ over $K$ such that $F \supset E \supset K$. By Definition V.4.1, the Galois group of $f$ is $\mathrm{Aut}_K E$. By Theorem V.9.4, $\mathrm{Aut}_K F$ is solvable.
(2) Suppose the Galois group of $f$ is solvable. So let $E$ be a splitting field of $f$ over $K$ (which exists since the algebraic closure of $K$ exists by Theorem V.3.6). Then this means that $\mathrm{Aut}_K E$ is solvable. Notice that $E$ can be chosen to be a finite dimensional extension by Theorem V.3.2, with $[E : K] \leq n!$.

# Corollary V.9.7. Galois' Theorem (continued 1)

**Proof (continued).** By Proposition V.9.6, it is sufficient to show that $E$ is Galois over $K$ and $\text{char}(K) \nmid [E : K]$ (since Proposition V.9.6 then implies the existence of radical extension $F$ of $K$ where $F \supset E \supset K$, and then by Definition V.9.2, $f(x) = 0$ is solvable by radicals). We have hypothesized that $\text{char}(K) \nmid n!$ where $n$ is the degree of polynomial $f$. By Theorem III.6.10, an irreducible factor $g$ of $f$ has no multiple roots in $E$ if and only if $g' \neq 0$. Since $g$ is a factor of $f$ then the degree of $g$ is between 1 and $n$.

# Corollary V.9.7. Galois' Theorem (continued 1)

**Proof (continued).** By Proposition V.9.6, it is sufficient to show that $E$ is Galois over $K$ and $\mathrm{char}(K) \nmid [E:K]$ (since Proposition V.9.6 then implies the existence of radical extension $F$ of $K$ where $F \supset E \supset K$, and then by Definition V.9.2, $f(x) = 0$ is solvable by radicals). We have hypothesized that $\mathrm{char}(K) \nmid n!$ where $n$ is the degree of polynomial $f$. By Theorem III.6.10, an irreducible factor $g$ of $f$ has no multiple roots in $E$ if and only if $g' \neq 0$. Since $g$ is a factor of $f$ then the degree of $g$ is between 1 and $n$. If $\mathrm{char}(k) = 0$ then $g' \neq 0$ by Exercise III.6.3(a). If $\mathrm{char}(K) = p \neq 0$ (since $\mathrm{char}(K) \nmid n!$ then $\mathrm{char}(K) > n$) then by Exercise III.6.3(b), $g' = 0$ if and only if $g$ is a polynomial in $x^p$.

# Corollary V.9.7. Galois' Theorem (continued 1)

**Proof (continued).** By Proposition V.9.6, it is sufficient to show that $E$ is Galois over $K$ and $\text{char}(K) \nmid [E : K]$ (since Proposition V.9.6 then implies the existence of radical extension $F$ of $K$ where $F \supset E \supset K$, and then by Definition V.9.2, $f(x) = 0$ is solvable by radicals). We have hypothesized that $\text{char}(K) \nmid n!$ where $n$ is the degree of polynomial $f$. By Theorem III.6.10, an irreducible factor $g$ of $f$ has no multiple roots in $E$ if and only if $g' \neq 0$. Since $g$ is a factor of $f$ then the degree of $g$ is between 1 and $n$. If $\text{char}(k) = 0$ then $g' \neq 0$ by Exercise III.6.3(a). If $\text{char}(K) = p \neq 0$ (since $\text{char}(K) \nmid n!$ then $\text{char}(K) > n$) then by Exercise III.6.3(b), $g' = 0$ if and only if $g$ is a polynomial in $x^p$. But if $g$ is a polynomial in $x^p$ then the degree of $g$ is greater than $n$, so it must be that $g' \neq 0$ in this case as well. So (by Theorem III.6.10), the irreducible factors of $f$ are separable (see Definition V.3.10).

# Corollary V.9.7. Galois' Theorem (continued 1)

**Proof (continued).** By Proposition V.9.6, it is sufficient to show that $E$ is Galois over $K$ and $\text{char}(K) \nmid [E : K]$ (since Proposition V.9.6 then implies the existence of radical extension $F$ of $K$ where $F \supset E \supset K$, and then by Definition V.9.2, $f(x) = 0$ is solvable by radicals). We have hypothesized that $\text{char}(K) \nmid n!$ where $n$ is the degree of polynomial $f$. By Theorem III.6.10, an irreducible factor $g$ of $f$ has no multiple roots in $E$ if and only if $g' \neq 0$. Since $g$ is a factor of $f$ then the degree of $g$ is between 1 and $n$. If $\text{char}(k) = 0$ then $g' \neq 0$ by Exercise III.6.3(a). If $\text{char}(K) = p \neq 0$ (since $\text{char}(K) \nmid n!$ then $\text{char}(K) > n$) then by Exercise III.6.3(b), $g' = 0$ if and only if $g$ is a polynomial in $x^p$. But if $g$ is a polynomial in $x^p$ then the degree of $g$ is greater than $n$, so it must be that $g' \neq 0$ in this case as well. So (by Theorem III.6.10), the irreducible factors of $f$ are separable (see Definition V.3.10).

# Corollary V.9.7. Galois' Theorem (continued 2)

**Corollary V.9.7. Galois' Theorem.** Let $K$ be a field and $f \in K[x]$ a polynomial of degree $n > 0$, where char$(K)$ does not divide $n!$ (which is always true when char$(K) = 0$). Then the equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f$ is solvable.

**Proof (continued).** By Exercise V.3.13 (the (iii)$\Rightarrow$(ii) part), $E$ is separable over $K$. Then by Theorem V.3.11 (the (ii)$\Rightarrow$(i) part), and the fact that $E$ is a splitting field of $f$) $E$ is Galois over $K$. Since $[E : K] \leq n!$ then every prime that divides $[E : K]$ must also divide $n!$. Since char$(K)$ is either 0 or prime and char$(K) \nmid n!$ then char$(K) \nmid [E : K]$.

# Corollary V.9.7. Galois' Theorem (continued 2)

**Corollary V.9.7. Galois' Theorem.** Let $K$ be a field and $f \in K[x]$ a polynomial of degree $n > 0$, where $\text{char}(K)$ does not divide $n!$ (which is always true when $\text{char}(K) = 0$). Then the equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f$ is solvable.

**Proof (continued).** By Exercise V.3.13 (the (iii)$\Rightarrow$(ii) part), $E$ is separable over $K$. Then by Theorem V.3.11 (the (ii)$\Rightarrow$(i) part), and the fact that $E$ is a splitting field of $f$) $E$ is Galois over $K$. Since $[E : K] \leq n!$ then every prime that divides $[E : K]$ must also divide $n!$. Since $\text{char}(K)$ is either 0 or prime and $\text{char}(K) \nmid n!$ then $\text{char}(K) \nmid [E : K]$. As mentioned above, Proposition V.9.6 now implies that the equation $f(x) = 0$ is solvable by radicals. $\square$

# Corollary V.9.7. Galois' Theorem (continued 2)

**Corollary V.9.7. Galois' Theorem.** Let $K$ be a field and $f \in K[x]$ a polynomial of degree $n > 0$, where $\text{char}(K)$ does not divide $n!$ (which is always true when $\text{char}(K) = 0$). Then the equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f$ is solvable.

**Proof (continued).** By Exercise V.3.13 (the (iii)$\Rightarrow$(ii) part), $E$ is separable over $K$. Then by Theorem V.3.11 (the (ii)$\Rightarrow$(i) part), and the fact that $E$ is a splitting field of $f$) $E$ is Galois over $K$. Since $[E : K] \leq n!$ then every prime that divides $[E : K]$ must also divide $n!$. Since $\text{char}(K)$ is either 0 or prime and $\text{char}(K) \nmid n!$ then $\text{char}(K) \nmid [E : K]$. As mentioned above, Proposition V.9.6 now implies that the equation $f(x) = 0$ is solvable by radicals. □