Lemma V.9.3 (continued 2)

**Proof (continued)**

- Every finitely generated field is isomorphic to a radical extension of its prime subfield.
- Let $K$ be a simple extension of $F$, then $K$ is a radical extension of $F$.
- Let $K$ be a radical extension of $F$, then $K$ is a finite Galois extension of $F$.
- Let $K$ be a field, then the radical extension of $K$ is the intersection of all finite Galois extensions of $K$.

Lemma V.9.3

**Proof**

- Every finitely generated field is isomorphic to a radical extension of its prime subfield.
- Let $K$ be a simple extension of $F$, then $K$ is a radical extension of $F$.
- Let $K$ be a radical extension of $F$, then $K$ is a finite Galois extension of $F$.
- Let $K$ be a field, then the radical extension of $K$ is the intersection of all finite Galois extensions of $K$.

Chapter V. Fields and Galois Theory

Modern Algebra

Theorem V.3.12

**Proof**

- Every finitely generated field is isomorphic to a radical extension of its prime subfield.
- Let $K$ be a simple extension of $F$, then $K$ is a radical extension of $F$.
- Let $K$ be a radical extension of $F$, then $K$ is a finite Galois extension of $F$.
- Let $K$ be a field, then the radical extension of $K$ is the intersection of all finite Galois extensions of $K$.
Theorem V.9.4 (continued 1)

Let $N$ be a field, and let $\mathcal{E}$ be a radical extension of $N$. Then $\mathcal{E}$ is a radical extension of $N$.

Proof (continued 1): According to Lemma V.9.3, since $\mathcal{E}$ is a radical extension of $N$, then $\mathcal{E}$ is a radical extension of $N$. Let $\alpha \in \mathcal{E}$ be a root of a polynomial $f(x) \in N[x]$.

Lemmas V.9.3 (continued 1)

Lemma V.9.3 (continued 1): If $\mathcal{E}$ is a radical extension of $N$, then $\mathcal{E}$ is a radical extension of $N$.

Proof (continued 1): According to Theorem V.9.4, since $\mathcal{E}$ is a radical extension of $N$, then $\mathcal{E}$ is a radical extension of $N$. Let $\alpha \in \mathcal{E}$ be a root of a polynomial $f(x) \in N[x]$.

Theorem V.9.4 (continued 2)

Theorem V.9.4 (continued 2): If $\mathcal{E}$ is a radical extension of $N$, then $\mathcal{E}$ is a radical extension of $N$.

Proof (continued 2): According to Lemma V.9.3, since $\mathcal{E}$ is a radical extension of $N$, then $\mathcal{E}$ is a radical extension of $N$. Let $\alpha \in \mathcal{E}$ be a root of a polynomial $f(x) \in N[x]$.
Theorem (Theorem V.7.2.5).

Under Gauss correspondance in the Fundamental Theorem of Gauss, if \( \text{char}(k) = \text{prime} \), then we know that \( k \) is separable and the field \( k \) is the unique, up to isomorphism, \( \text{char}(k) \)-algebra. By Theorem V.7.1.1, if we knew that \( k \) is separable and the field \( k \) is the unique, up to isomorphism, \( \text{char}(k) \)-algebra.

**Proof (continued)**. By Theorem V.7.1.2(1), \( f(x) \) is an algebra extension of \( f(x) \), if and only if it is separable and \( f(x) \) is the unique, up to isomorphism, \( \text{char}(k) \)-algebra.

**Theorem V.9.4.4 (continued)**

**Proof (continued)**. But by Theorem V.9.4.5, we have that \( d = (\frac{1}{\text{char}(k)}) \) does not divide \( m \), as claimed.

We have that \( \text{char}(k) \) is separable, and hence is a cyclotomic. Then \( \text{char}(k) \) contains all roots of unity, which exists in the algebraic closure of \( \mathbb{F} \).

Considering \( \text{char}(k) \) does not divide \( m \), consider \( x \) such that \( x^n - 1 = 0 \) for all \( n \in \mathbb{N} \) and the fact that \( \text{char}(k) \) is prime. By Exercise V.3.12, \( \mathbb{F} \) is separable and purely inseparable over \( k \). Hence, by Theorem V.7.1.2(1), \( \mathbb{F} \) is separable over \( k \). By Exercise V.3.12, \( \mathbb{F} \) is separable over \( k \). By Exercise V.3.12, \( \mathbb{F} \) is separable over \( k \). By Exercise V.3.12, \( \mathbb{F} \) is separable over \( k \). By Exercise V.3.12, \( \mathbb{F} \) is separable over \( k \).

Therefore, by definition, \( f(x) \) is irreducible over \( k \). Since the constant term of this polynomial is a power of \( \text{char}(k) \), it is irreducible over \( k \). But since \( m \) is the smallest power of \( k \), it is irreducible over \( k \). Notice that \( \text{char}(k) \) is prime. So the irreducible polynomial of \( 0 \in \mathbb{F} \) over \( k \) is irreducible.
Theorem V.9.4. Any E 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 splitting field \( E \) over \( K \) such that

The fundamental Theorem of Galois Theory (Theorem V.2.5(!!))

Proposition V.9.6. Let \( E \) be a finite dimensional Galois extension field of \( K \).

Proposition V.9.5. Let \( E \) be a field and \( f \in K[x] \). If the equation \( f(x) = 0 \) is divisible by \( \text{rad}(f)(E) \), then there exists a radical extension \( F \) of \( K \) such that

Corollary V.9.5. The Galois group of \( f \) is a solvable group.

Corollary V.9.5. Let \( E \) be a Galois extension of \( F \). Then the Galois group of \( f \) is a solvable group.

Theorem V.9.4(continued). By definition of cyclic extension, \( E \) is cyclic over \( F \).

Group. By definition of cyclic extension, \( E \) is cyclic over \( F \).

We have the normal subgroups \( H_1 \triangleleft H_2 \triangleleft H_2 \triangleleft \ldots \).

Theorem V.9.2(!!)]. There is an intermediate field \( F \) of \( K \) and \( E \) in an intermediate field. Then \( \text{Aut}(E/F) \) is a solvable group.

By the Fundamental Theorem of Galois Theory, \( E/F \) is a cyclic extension field of \( F \) and \( E \) is an intermediate field, then \( \text{Aut}(E/F) \) is a solvable group.

Proof (continued). So by the Fundamental Theorem of Galois Theory, \( E/F \) is a cyclic extension field of \( F \) and \( E \) is an intermediate field.

Proof (continued). Schenmelckly we have:
Let $p$ be the fixed field of $f$ in $\mathbb{Q}$. Then $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the maximal extension of $\mathbb{Q}$ which contains $\sqrt{2}$ and $\sqrt{3}$.

We now prove the theorem by induction on $n$. The base case $n=1$ is trivial. Assume the theorem is true for all extensions of dimension $d < n$. Then we have $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})$. Since $\sqrt{3}$ is algebraic over $\mathbb{Q}(\sqrt{2})$, it is a root of a polynomial with coefficients in $\mathbb{Q}(\sqrt{2})$. Hence $\sqrt{3}$ is in $\mathbb{Q}(\sqrt{2})$, which is a contradiction. Therefore, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})$, which is the desired result.

Proof (continued).
Corollary V.9.7, Galois Theory (continued)

Corollary V.9.7, Galois Theory (continued)

Proposition V.9.6 (continued 5)

Proposition V.9.6 (continued 5)