The Insolvability of the Quintic

A Complete Treatment

December 2025

1 Preliminaries: Groups and Permutations

Definition 1.1 (Symmetric Group). For a positive integer n, the symmetric group S_n is the group of all bijections from $\{1, 2, \ldots, n\}$ to itself, with composition as the group operation. The order of S_n is $n!$.

Convention 1.2 (Composition Order). Throughout this document, composition of permutations is performed right-to-left: for $\sigma, \tau \in S_n$, the product $\sigma\tau$ means "first apply τ, then apply σ". That is, $(\sigma\tau)(x) = \sigma(\tau(x))$.

Definition 1.3 (Transposition and Cycle). A transposition is a permutation that exchanges exactly two elements and fixes all others. A k-cycle $(a_1\, a_2\, \cdots\, a_k)$ is the permutation sending $a_1 \to a_2 \to \cdots \to a_k \to a_1$ and fixing all other elements.

Definition 1.4 (Even and Odd Permutations). A permutation $\sigma \in S_n$ is even if it can be expressed as a product of an even number of transpositions, and odd otherwise. The parity is well-defined.

Definition 1.5 (Alternating Group). The alternating group A_n is the subgroup of S_n consisting of all even permutations. The order of A_n is $n!/2$ for $n \geq 2$.

Definition 1.6 (Support). The support of a permutation σ is $\operatorname{supp}(\sigma) = \{x : \sigma(x) \neq x\}$.

Lemma 1.7 (Generation by 3-Cycles). For $n \geq 3$, the alternating group A_n is generated by 3-cycles.

Proof. Every even permutation is a product of an even number of transpositions. It suffices to show that any product of two transpositions is a product of 3-cycles.

Case 1: $(a\,b)(a\,b) = e$, the identity.

Case 2: $(a\,b)(b\,c)$ with a, b, c distinct. Verification that $(a\,b)(b\,c) = (a\,b\,c)$: - $a \to (b\,c)$ fixes $a \to (a\,b)$ sends $a \to b$. Result: $a \to b$. ✓ - $b \to (b\,c)$ sends $b \to c \to (a\,b)$ fixes c. Result: $b \to c$. ✓ - $c \to (b\,c)$ sends $c \to b \to (a\,b)$ sends $b \to a$. Result: $c \to a$. ✓

Case 3: $(a\,b)(c\,d)$ with a, b, c, d distinct. We claim $(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d)$. Verification: - $a \to (a\,c\,d)$ sends $a \to c \to (a\,c\,b)$ sends $c \to b$. Result: $a \to b$. ✓ - $b \to (a\,c\,d)$ fixes $b \to (a\,c\,b)$ sends $b \to a$. Result: $b \to a$. ✓ - $c \to (a\,c\,d)$ sends $c \to d \to (a\,c\,b)$ fixes d. Result: $c \to d$. ✓ - $d \to (a\,c\,d)$ sends $d \to a \to (a\,c\,b)$ sends $a \to c$. Result: $d \to c$. ✓ ∎

---

2 Normal Subgroups and Quotients

Definition 2.1 (Normal Subgroup). A subgroup N of G is normal, written $N \trianglelefteq G$, if $gNg^{-1} = N$ for all $g \in G$.

Definition 2.2 (Quotient Group). For $N \trianglelefteq G$, the quotient G/N is the set of cosets $\{gN : g \in G\}$ with multiplication $(gN)(hN) := (gh)N$.

Definition 2.3 (Simple Group). A group G is simple if $|G| > 1$ and the only normal subgroups are $\{e\}$ and G.

Lemma 2.4 (Conjugacy of 3-Cycles). In S_n for $n \geq 3$, any two 3-cycles are conjugate.

Proof. Given 3-cycles $(a\,b\,c)$ and $(d\,e\,f)$, choose $\sigma \in S_n$ with $\sigma(a) = d$, $\sigma(b) = e$, $\sigma(c) = f$. Then $\sigma(a\,b\,c)\sigma^{-1} = (d\,e\,f)$ by direct verification on each element. ■

Lemma 2.5 (Commutator in Normal Subgroups). If $N \trianglelefteq G$ and $\sigma \in N$, then $[\sigma, \tau] := \sigma\tau\sigma^{-1}\tau^{-1} \in N$ for all $\tau \in G$.

Proof. We have $[\sigma, \tau] = \sigma(\tau\sigma^{-1}\tau^{-1})$. Since N is normal, $\tau\sigma^{-1}\tau^{-1} \in N$, so $[\sigma, \tau] \in N$. ■

---

3 Simplicity of the Alternating Group

Lemma 3.1 (Conjugation of Cycles). For any permutation σ and cycle $(x\,y\,z)$, we have $\sigma(x\,y\,z)\sigma^{-1} = (\sigma(x)\,\sigma(y)\,\sigma(z))$.

Proof. For any element w: if $w = \sigma(x)$, then $\sigma(x\,y\,z)\sigma^{-1}(w) = \sigma(x\,y\,z)(x) = \sigma(y)$. Similarly for $\sigma(y)$ and $\sigma(z)$. If $w \notin \{\sigma(x), \sigma(y), \sigma(z)\}$, then $\sigma^{-1}(w) \notin \{x, y, z\}$, so $(x\,y\,z)$ fixes $\sigma^{-1}(w)$, and $\sigma(x\,y\,z)\sigma^{-1}(w) = w$. ■

Lemma 3.2 (Reduction from Long Cycles). Let $\sigma \in A_n$ contain a cycle of length $r \geq 4$, with $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\sigma(a_3) = a_4$. Let $\tau = (a_1\,a_2\,a_3)$. Then $[\sigma, \tau] = (a_1\,a_4\,a_2)$, a 3-cycle.

Proof. By Lemma 3.1, $\sigma\tau\sigma^{-1} = (\sigma(a_1)\,\sigma(a_2)\,\sigma(a_3)) = (a_2\,a_3\,a_4)$.

Computing $[\sigma, \tau] = (a_2\,a_3\,a_4)(a_1\,a_3\,a_2)$ where $\tau^{-1} = (a_1\,a_3\,a_2)$: - a_1: $(a_1\,a_3\,a_2)$ sends $a_1 \longrightarrow a_3$; $(a_2\,a_3\,a_4)$ sends $a_3 \longrightarrow a_4$. Result: $a_1 \longrightarrow a_4$. - a_2: $(a_1\,a_3\,a_2)$ sends $a_2 \longrightarrow a_1$; $(a_2\,a_3\,a_4)$ fixes a_1. Result: $a_2 \longrightarrow a_1$. - a_3: $(a_1\,a_3\,a_2)$ sends $a_3 \longrightarrow a_2$; $(a_2\,a_3\,a_4)$ sends $a_2 \longrightarrow a_3$. Result: $a_3 \longrightarrow a_3$ (fixed). - a_4: $(a_1\,a_3\,a_2)$ fixes a_4; $(a_2\,a_3\,a_4)$ sends $a_4 \longrightarrow a_2$. Result: $a_4 \longrightarrow a_2$.

Hence $[\sigma, \tau] = (a_1\,a_4\,a_2)$, a 3-cycle with $\mathrm{supp}([\sigma, \tau]) = \{a_1, a_2, a_4\}$. ■

Lemma 3.3 (Reduction from Multiple Transpositions to Double Transposition). Let $\sigma = (a\,b)(c\,d)\sigma'$ where σ' is a product of transpositions disjoint from $\{a, b, c, d\}$. Let $\tau = (a\,b\,c)$. Then $[\sigma, \tau] = (a\,c)(b\,d)$.

Proof. Since σ' is disjoint from $\{a, b, c\}$, it commutes with $\tau = (a\,b\,c)$. Hence

$$[\sigma, \tau] = [(a\,b)(c\,d)\sigma', \tau] = [(a\,b)(c\,d), \tau].$$

(We do **not** cancel $(c\,d)$, since it does not commute with τ.)

We now compute $[(a\,b)(c\,d), (a\,b\,c)]$ directly. For $\sigma_0 = (a\,b)(c\,d)$ and $\tau = (a\,b\,c)$, note that $\sigma_0^{-1} = \sigma_0$ (since σ_0 is a product of disjoint transpositions). We find $\sigma_0\tau\sigma_0^{-1}$ by tracking each element: - a: $\sigma_0(a) = b$, $\tau(b) = c$, $\sigma_0^{-1}(c) = d$. So $\sigma_0\tau\sigma_0^{-1}(a) = d$. - b: $\sigma_0(b) = a$, $\tau(a) = b$,

$\sigma_0^{-1}(b) = a$. So $\sigma_0\tau\sigma_0^{-1}(b) = a$. - c: $\sigma_0(c) = d$, $\tau(d) = d$, $\sigma_0^{-1}(d) = c$. So $\sigma_0\tau\sigma_0^{-1}(c) = c$. - d: $\sigma_0(d) = c$, $\tau(c) = a$, $\sigma_0^{-1}(a) = b$. So $\sigma_0\tau\sigma_0^{-1}(d) = b$.

So $\sigma_0\tau\sigma_0^{-1}$: $a \longrightarrow d, b \longrightarrow a, c \longrightarrow c, d \longrightarrow b$. This is $(a\,d\,b)$.

Now $[\sigma_0, \tau] = (a\,d\,b)(a\,c\,b)$ where $\tau^{-1} = (a\,c\,b)$: - a: $(a\,c\,b)(a) = c$, $(a\,d\,b)(c) = c$. Result: $a \longrightarrow c$. - b: $(a\,c\,b)(b) = a$, $(a\,d\,b)(a) = d$. Result: $b \longrightarrow d$. - c: $(a\,c\,b)(c) = b$, $(a\,d\,b)(b) = a$. Result: $c \longrightarrow a$. - d: $(a\,c\,b)(d) = d$, $(a\,d\,b)(d) = b$. Result: $d \longrightarrow b$.

Hence $[\sigma, \tau] = (a\,c)(b\,d)$, a double transposition. ■

Lemma 3.4 (From Double Transposition to 3-Cycle). Let $n \geq 5$ and let $\delta = (a\,c)(b\,d)$. Choose $e \in \{1, \ldots, n\} \setminus \{a, b, c, d\}$ and let $\rho = (a\,c\,e)$. Then $[\delta, \rho] = (a\,c\,e)$, a 3-cycle.

Proof. We compute $\delta\rho\delta^{-1}$ directly. Since $\delta = \delta^{-1}$, we compute $\delta\rho\delta$ by tracking each element: - a: $\delta(a) = c$, $\rho(c) = e$, $\delta(e) = e$. So $\delta\rho\delta(a) = e$. - c: $\delta(c) = a$, $\rho(a) = c$, $\delta(c) = a$. So $\delta\rho\delta(c) = a$. - e: $\delta(e) = e$, $\rho(e) = a$, $\delta(a) = c$. So $\delta\rho\delta(e) = c$. - b: $\delta(b) = d$, $\rho(d) = d$, $\delta(d) = b$. So $\delta\rho\delta(b) = b$. - d: $\delta(d) = b$, $\rho(b) = b$, $\delta(b) = d$. So $\delta\rho\delta(d) = d$.

Hence $\delta\rho\delta^{-1} = (a\,e\,c)$.

Now we compute $[\delta, \rho] = (\delta\rho\delta^{-1})\rho^{-1} = (a\,e\,c)(a\,e\,c)$, since $\rho^{-1} = (a\,e\,c)$: - a: $(a\,e\,c)(a) = e$, $(a\,e\,c)(e) = c$. Result: $a \longrightarrow c$. - c: $(a\,e\,c)(c) = a$, $(a\,e\,c)(a) = e$. Result: $c \longrightarrow e$. - e: $(a\,e\,c)(e) = c$, $(a\,e\,c)(c) = a$. Result: $e \longrightarrow a$.

Hence $[\delta, \rho] = (a\,e\,c)^2 = (a\,c\,e)$, a 3-cycle. ■

Lemma 3.5 (Two Disjoint 3-Cycles to 5-Cycle). Let $\sigma = (a\,b\,c)(d\,e\,f)\sigma'$ where σ' is disjoint from $\{a, b, c, d, e, f\}$. Let $\tau = (a\,b\,d)$. Then $[\sigma, \tau] = (a\,d\,c\,e\,b)$, a 5-cycle.

Proof. Since σ' is disjoint from $\{a, b, d\}$, it commutes with τ and cancels in the commutator.

By Lemma 3.1, $\sigma\tau\sigma^{-1} = (\sigma(a)\,\sigma(b)\,\sigma(d)) = (b\,c\,e)$.

Computing $[\sigma, \tau] = (b\,c\,e)(a\,d\,b)$ where $\tau^{-1} = (a\,d\,b)$: - a: $(a\,d\,b)(a) = d$, $(b\,c\,e)(d) = d$. Result: $a \longrightarrow d$. - b: $(a\,d\,b)(b) = a$, $(b\,c\,e)(a) = a$. Result: $b \longrightarrow a$. - c: $(a\,d\,b)(c) = c$, $(b\,c\,e)(c) = e$. Result: $c \longrightarrow e$. - d: $(a\,d\,b)(d) = b$, $(b\,c\,e)(b) = c$. Result: $d \longrightarrow c$. - e: $(a\,d\,b)(e) = e$, $(b\,c\,e)(e) = b$. Result: $e \longrightarrow b$.

Hence $[\sigma, \tau] = (a\,d\,c\,e\,b)$, a 5-cycle. ■

Theorem 3.6 (Simplicity of A_n). For $n \geq 5$, the alternating group A_n is simple.

Proof. Let $N \trianglelefteq A_n$ with $N \neq \{e\}$. We show $N = A_n$.

Step 1: N contains a 3-cycle.

Choose $\sigma \in N \setminus \{e\}$ with $|\operatorname{supp}(\sigma)|$ minimal. We show $|\operatorname{supp}(\sigma)| = 3$ by contradiction.

Suppose $|\operatorname{supp}(\sigma)| > 3$. We derive a contradiction by producing a non-identity element in N with strictly smaller support.

Case A: σ contains a cycle of length ≥ 4.

By Lemma 3.2, $[\sigma, \tau]$ is a 3-cycle in N. Since a 3-cycle is non-identity with $|\operatorname{supp}| = 3 < |\operatorname{supp}(\sigma)|$, this contradicts minimality.

Case B: σ is a product of disjoint 3-cycles, with at least two.

Then $|\operatorname{supp}(\sigma)| \geq 6$. By Lemma 3.5, $[\sigma, \tau]$ is a 5-cycle in N. Since a 5-cycle has length ≥ 4, Lemma 3.2 applies and yields a 3-cycle in N with $|\operatorname{supp}| = 3 < 6 \leq |\operatorname{supp}(\sigma)|$, contradicting minimality.

Case C: σ is a product of disjoint transpositions.

Since $\sigma \in A_n$, σ has at least 2 transpositions, so $|\operatorname{supp}(\sigma)| \geq 4$.

Subcase C1: $|\operatorname{supp}(\sigma)| > 4$ (at least 3 transpositions).

By Lemma 3.3, $[\sigma, \tau] = (a\ c)(b\ d) \in N$. Since $(a\ c)(b\ d) \neq e$ (it moves four elements), this is a non-identity element of N with $|\operatorname{supp}| = 4 < |\operatorname{supp}(\sigma)|$, contradicting minimality.

Subcase C2: $|\operatorname{supp}(\sigma)| = 4$ (exactly a double transposition).

Write $\sigma = (a\ c)(b\ d)$. By Lemma 3.4, $[\sigma, \rho] = (a\ c\ e) \in N$. Since $(a\ c\ e) \neq e$ (it is a 3-cycle), this is a non-identity element of N with $|\operatorname{supp}| = 3 < 4$, contradicting minimality.

Exhaustiveness: In the disjoint cycle decomposition of σ, if any cycle has length ≥ 4, we are in Case A. Otherwise all nontrivial cycles have length 2 or 3. If there are at least two 3-cycles, we are in Case B. If there are no 3-cycles, we are in Case C.

Since all cases yield contradictions, $|\operatorname{supp}(\sigma)| \leq 3$. Since $\sigma \neq e$ and $\sigma \in A_n$, we have $|\operatorname{supp}(\sigma)| \geq 2$. A non-identity even permutation with $|\operatorname{supp}(\sigma)| = 2$ would be a single transposition, which is odd—contradiction. Thus $|\operatorname{supp}(\sigma)| = 3$.

An even permutation with support exactly 3 must be a 3-cycle. Therefore σ is a 3-cycle, and N contains a 3-cycle.

Step 2: N contains all 3-cycles.

Let $(a\ b\ c) \in N$. For any 3-cycle $(d\ e\ f)$, by Lemma 2.4 there exists $\sigma \in S_n$ with $\sigma(a\ b\ c)\sigma^{-1} = (d\ e\ f)$.

If $\sigma \in A_n$, then $(d\ e\ f) \in N$ by normality.

If $\sigma \notin A_n$, choose distinct $p, q \in \{1, \ldots, n\} \setminus \{a, b, c\}$. Such p, q exist since $n \geq 5$. Let $\rho = (p\ q)$. Then $\sigma\rho \in A_n$ (product of two odd permutations). Since ρ is disjoint from $(a\ b\ c)$, we have $\rho(a\ b\ c)\rho^{-1} = (a\ b\ c)$. Thus:

$$(\sigma\rho)(a\ b\ c)(\sigma\rho)^{-1} = \sigma\rho(a\ b\ c)\rho^{-1}\sigma^{-1} = \sigma(a\ b\ c)\sigma^{-1} = (d\ e\ f) \in N.$$

By Lemma 1.7, $N = A_n$. ■

4 Solvable Groups

Definition 4.1 (Solvable Group). A group G is solvable if there exists a chain $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G$ with each G_{i+1}/G_i abelian.

Lemma 4.2 (Non-Abelian Simple $\Rightarrow$ Not Solvable). A non-abelian simple group is not solvable.

Proof. Let G be simple and non-abelian. In any solvable series $\{e\} = G_0 \trianglelefteq \cdots \trianglelefteq G_k = G$, simplicity forces $G_{k-1} \in \{\{e\}, G\}$. If $G_{k-1} = G$, the term is redundant. Removing redundancies, we reach $\{e\} \trianglelefteq G$, requiring $G/\{e\} \cong G$ to be abelian, contradicting non-abelianity. ■

Lemma 4.3 (Subgroups of Solvable Groups). If G is solvable and $H \leq G$, then H is solvable.

Proof. Given a solvable series $\{e\} = G_0 \trianglelefteq \cdots \trianglelefteq G_k = G$, define $H_i = G_i \cap H$. Then $H_i \trianglelefteq H_{i+1}$, and the map $H_{i+1} \to G_{i+1}/G_i$ given by $h \mapsto hG_i$ has kernel H_i. By the first isomorphism theorem, H_{i+1}/H_i embeds into the abelian group G_{i+1}/G_i, hence is abelian. ■

Theorem 4.4 (S_n Not Solvable for $n \geq 5$). For $n \geq 5$, S_n is not solvable.

Proof. By Theorem 3.6, A_n is simple. It is non-abelian: $(1\,2\,3)(1\,2\,4) = (1\,3)(2\,4) \neq (1\,4)(2\,3) = (1\,2\,4)(1\,2\,3)$. By Lemma 4.2, A_n is not solvable. Since $A_n \leq S_n$, Lemma 4.3 implies S_n is not solvable. ■

---

5 Field Extensions

Definition 5.1 (Field Extension). A field extension L/K is an inclusion $K \subseteq L$. The degree $[L : K]$ is $\dim_K(L)$.

Definition 5.2 (Algebraic Element). $\alpha \in L$ is algebraic over K if it satisfies some non-zero $f(x) \in K[x]$. The minimal polynomial is the unique monic irreducible polynomial in $K[x]$ with α as a root.

Definition 5.3 (Splitting Field). A splitting field of $f(x) \in K[x]$ over K is an extension L where f factors completely as $f(x) = c\prod(x - \alpha_i)$ and $L = K(\alpha_1, \ldots, \alpha_n)$.

Lemma 5.4 (Tower Law). For $K \subseteq M \subseteq L$ with finite degrees, $[L : K] = [L : M][M : K]$.

Proof. If $\{u_1, \ldots, u_m\}$ is a K-basis for M and $\{v_1, \ldots, v_n\}$ is an M-basis for L, then $\{u_i v_j\}$ is a K-basis for L. ■

---

6 Galois Theory

Definition 6.1 (Galois Group). For L/K, the Galois group $\mathrm{Gal}(L/K)$ is the group of K-automorphisms of L.

Lemma 6.2 (Automorphisms Permute Roots). Let $f(x) \in K[x]$ have roots $\alpha_1, \ldots, \alpha_n$ in L. Every $\sigma \in \mathrm{Gal}(L/K)$ permutes $\{\alpha_1, \ldots, \alpha_n\}$.

Proof. For $f(x) = \sum a_i x^i$ with $a_i \in K$: $f(\sigma(\alpha)) = \sum a_i \sigma(\alpha)^i = \sum \sigma(a_i)\sigma(\alpha)^i = \sigma(\sum a_i \alpha^i) = \sigma(0) = 0$. ∎

Definition 6.3 (Separable Polynomial). A polynomial $f \in K[x]$ is separable if it has no repeated roots in any extension of K. In characteristic 0, every irreducible polynomial is separable.

Theorem 6.4 (Characterisation of Galois Extensions). A finite extension L/K is Galois (meaning $|\mathrm{Gal}(L/K)| = [L : K]$) if and only if L is the splitting field of a separable polynomial over K.

Theorem 6.5 (Galois Correspondence). For a finite Galois extension L/K with $G = \mathrm{Gal}(L/K)$, there is an inclusion-reversing bijection between intermediate fields $K \subseteq M \subseteq L$ and subgroups $H \leq G$. Moreover, M/K is Galois iff $\mathrm{Gal}(L/M) \trianglelefteq G$, in which case $\mathrm{Gal}(M/K) \cong G/\mathrm{Gal}(L/M)$.

---

7 Symmetric Functions and the Generic Polynomial

Definition 7.1 (Elementary Symmetric Polynomials). For indeterminates $x_1, \ldots, x_n$, define $e_1 = \sum x_i$, $e_2 = \sum_{i<j} x_i x_j$, …, $e_n = x_1 \cdots x_n$, so that $\prod(t - x_i) = t^n - e_1 t^{n-1} + \cdots + (-1)^n e_n$.

Theorem 7.2 (Fundamental Theorem of Symmetric Functions). Let $F = k(x_1, \ldots, x_n)$ with S_n acting by permuting variables. Then $F^{S_n} = k(e_1, \ldots, e_n)$.

Proof. Let $E = k(e_1, \ldots, e_n)$. Clearly $E \subseteq F^{S_n}$.

For the reverse: let $g \in k[x_1, \ldots, x_n]$ be symmetric. Among all monomials of g, choose one with maximal exponent sequence $(a_1, \ldots, a_n)$ in lexicographic order. Since g is symmetric and this monomial is maximal, we have $a_1 \geq a_2 \geq \cdots \geq a_n$ (otherwise permuting would yield a larger monomial).

The polynomial $e_1^{a_1 - a_2} e_2^{a_2 - a_3} \cdots e_n^{a_n}$ has leading monomial $x_1^{a_1} \cdots x_n^{a_n}$. Subtracting an appropriate scalar multiple from g reduces the maximal monomial. By induction on the well-ordered set of monomial sequences, $g \in k[e_1, \ldots, e_n]$.

For $f/g \in F^{S_n}$ with $f, g \in k[x_1, \ldots, x_n]$ and $g \neq 0$: the product $\prod_{\sigma \in S_n}(\sigma \cdot g)$ is symmetric (applying any $\tau \in S_n$ permutes the factors), hence lies in $k[e_1, \ldots, e_n]$. The numerator $f \cdot \prod_{\sigma \neq e}(\sigma \cdot g)$ equals $(f/g) \cdot \prod_{\sigma \in S_n}(\sigma \cdot g)$, which is the product of the S_n-invariant element f/g with a symmetric polynomial, hence symmetric, hence in $k[e_1, \ldots, e_n]$. Thus $f/g \in k(e_1, \ldots, e_n)$. ∎

Theorem 7.3 (Galois Group of the Generic Polynomial). Let k have characteristic 0, $E = k(e_1, \ldots, e_n)$, $F = k(x_1, \ldots, x_n)$. Then:

(i) F is the splitting field of $P(t) = t^n - e_1 t^{n-1} + \cdots + (-1)^n e_n$ over E.
(ii) F/E is Galois with $\mathrm{Gal}(F/E) \cong S_n$.
(iii) $[F : E] = n!$.

Proof.

(i) By definition, $P(t) = \prod(t - x_i)$, so the roots are $x_1, \ldots, x_n \in F$, and $F = E(x_1, \ldots, x_n)$.
(ii) The roots $x_1, \ldots, x_n$ are distinct elements of F (they are independent indeterminates). Over characteristic 0, $P(t) = \prod(t - x_i)$ is therefore separable. Thus F/E is Galois by Theorem 6.4.

Each $\sigma \in S_n$ induces an E-automorphism φ_σ of F by $\varphi_\sigma(f(x_1, \ldots, x_n)) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. This defines a homomorphism $\varphi : S_n \longrightarrow \mathrm{Gal}(F/E)$.

Injectivity: If $\sigma \neq \tau$, then $\sigma(i) \neq \tau(i)$ for some i, so $\varphi_\sigma(x_i) \neq \varphi_\tau(x_i)$.

Surjectivity: Any $\psi \in \mathrm{Gal}(F/E)$ permutes $\{x_1, \ldots, x_n\}$ by Lemma 6.2. If $\psi(x_i) = x_{\sigma(i)}$, then $\psi = \varphi_\sigma$ since $F = E(x_1, \ldots, x_n)$.

(iii) Since F/E is Galois, $[F : E] = |\mathrm{Gal}(F/E)| = |S_n| = n!$. ■

---

8 Radical Extensions

Definition 8.1 (Radical Extension). L/K is a radical extension if there exists $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L$ with $K_{i+1} = K_i(\alpha_i)$ and $\alpha_i^{n_i} \in K_i$.

Definition 8.2 (Solvable by Radicals). $f(x) \in K[x]$ is solvable by radicals if some radical extension of K contains all roots of f.

Lemma 8.3 (Radical Expressions Lie in Radical Extensions). Any expression built from elements of K using $+, -, \times, \div$ and extraction of n-th roots lies in some radical extension of K.

Proof. Such an expression is constructed in finitely many steps. Each arithmetic operation stays within the current field. Each n-th root extraction $K_i(\alpha)$ with $\alpha^n \in K_i$ is a simple radical extension. The composition of finitely many simple radical extensions is a radical extension. ■

Lemma 8.4 (Cyclic Galois Groups from n-th Roots). Let K contain a primitive n-th root of unity ζ, let $a \in K$, and let $L = K(\alpha)$ where $\alpha^n = a$. Then L/K is Galois with cyclic Galois group of order dividing n.

Proof. The roots of $x^n - a$ are $\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha$. Since $\zeta \in K \subseteq L$, all roots lie in L, so L is the splitting field of $x^n - a$ over K. In characteristic 0, $x^n - a$ is separable. By Theorem 6.4, L/K is Galois.

For $\sigma \in \mathrm{Gal}(L/K)$, we have $\sigma(\alpha)^n = a$, so $\sigma(\alpha) = \zeta^{k_\sigma}\alpha$ for some k_σ. The map $\sigma \mapsto k_\sigma \pmod{n}$ is an injective homomorphism $\mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z}$. Thus $\mathrm{Gal}(L/K)$ is cyclic of order dividing n. ■

Lemma 8.5 (Roots of Unity). For K of characteristic 0, the splitting field of $x^n - 1$ over K has abelian Galois group.

Proof. Let $L = K(\zeta)$ for a primitive n-th root of unity. Each $\sigma \in \mathrm{Gal}(L/K)$ satisfies $\sigma(\zeta) = \zeta^{a_\sigma}$ for some $a_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$. The map $\sigma \mapsto a_\sigma$ embeds $\mathrm{Gal}(L/K)$ into the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$. ■

Lemma 8.6 (Compositum of Abelian Extensions). Let $L_1/K, \ldots, L_m/K$ be finite Galois extensions with abelian Galois groups, all contained in some field Ω. The compositum $L = L_1 \cdots L_m$ satisfies: L/K is Galois, and $\mathrm{Gal}(L/K)$ is abelian.

Proof. Each L_i is the splitting field of a separable polynomial f_i over K. Then L is the splitting field of $f_1 \cdots f_m$ over K, hence Galois.

Define $\varphi : \mathrm{Gal}(L/K) \to \prod \mathrm{Gal}(L_i/K)$ by $\varphi(\sigma) = (\sigma|_{L_1}, \ldots, \sigma|_{L_m})$. This is injective: if $\sigma|_{L_i} = \mathrm{id}$ for all i, then σ fixes L. Thus $\mathrm{Gal}(L/K)$ embeds into an abelian group, hence is abelian. ■

Theorem 8.7 (Solvable by Radicals $\Rightarrow$ Solvable Galois Group). Let K have characteristic 0. If $f(x) \in K[x]$ is solvable by radicals, then $\mathrm{Gal}(f/K)$ is solvable.

Proof. Let L be the splitting field of f, and let $M \supseteq L$ be a radical extension of K with tower $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = M$, where $K_{i+1} = K_i(\alpha_i)$ with $\alpha_i^{n_i} \in K_i$.

Step 1: Adjoin roots of unity. Let $N = \mathrm{lcm}(n_0, \ldots, n_{r-1})$ and let ζ be a primitive N-th root of unity. Define $K' = K(\zeta)$ and $K_i' = K_i(\zeta)$. The tower $K' \subseteq K_1' \subseteq \cdots \subseteq M' = M(\zeta)$ still has $K_{i+1}' = K_i'(\alpha_i)$ with $\alpha_i^{n_i} \in K_i'$.

Step 2: Each step is Galois with cyclic group. Since K_i' contains a primitive n_i-th root of unity, Lemma 8.4 implies K_{i+1}'/K_i' is Galois with cyclic Galois group.

Step 3: Pass to normal closures. Let M'' be the normal closure of M' over K. For each i, let L_i be the normal closure of K_i' over K within M''.

Step 4: Build solvable series. The extension L_{i+1}/L_i is generated by conjugates of α_i over K. Each conjugate β satisfies $\beta^{n_i} \in L_i$, and since L_i contains all n_i-th roots of unity, $L_i(\beta)/L_i$ is Galois with cyclic Galois group by Lemma 8.4.

The extension L_{i+1}/L_i is the compositum of these cyclic extensions. By Lemma 8.6, $\mathrm{Gal}(L_{i+1}/L_i)$ is abelian.

Step 5: Conclude solvability. The chain $K \subseteq K(\zeta) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = M''$ has $\mathrm{Gal}(L_0/K)$ abelian by Lemma 8.5 and each $\mathrm{Gal}(L_{i+1}/L_i)$ abelian by Step 4. Thus $G = \mathrm{Gal}(M''/K)$ has a subnormal series with abelian quotients, so G is solvable.

Step 6: Conclude for f. We have $K \subseteq L \subseteq M''$. By the Galois correspondence, $\mathrm{Gal}(L/K) \cong G/\mathrm{Gal}(M''/L)$. A quotient of a solvable group is solvable. Thus $\mathrm{Gal}(L/K)$ is solvable. ■

9 The Main Theorem

Theorem 9.1 (Abel–Ruffini). For $n \geq 5$, the generic polynomial of degree n is not solvable by radicals.

Proof. Let k have characteristic 0, let $E = k(e_1, \ldots, e_n)$, and let $P(t) = t^n - e_1 t^{n-1} + \cdots + (-1)^n e_n$.

By Theorem 7.3, $\mathrm{Gal}(P/E) \cong S_n$.

By Theorem 4.4, S_n is not solvable for $n \geq 5$.

If P were solvable by radicals, Theorem 8.7 would imply S_n is solvable, a contradiction.

Therefore P is not solvable by radicals. ■

Corollary 9.2 (No General Algebraic Formula). There is no algebraic formula expressing the roots of a general polynomial of degree $n \geq 5$ in terms of its coefficients using only $+, -, \times, \div$ and extraction of radicals.

Proof. Such a formula, applied to $P(t)$ with indeterminate coefficients $e_1, \ldots, e_n$, would express the roots $x_1, \ldots, x_n \in k(x_1, \ldots, x_n)$ in terms of $e_1, \ldots, e_n$ using radicals. By Lemma 8.3, the roots would then lie in a radical extension of $E = k(e_1, \ldots, e_n)$, meaning P is solvable by radicals. This contradicts Theorem 9.1. ■