Galois Lite
or
How Euler Could Have Proved
the Quintic is Unsolvable

Ian Stewart
Mathematics Institute
University of Warwick
Coventry CV4 7AL
United Kingdom

June 14, 2010

Abstract

How complicated must a proof of the unsolvability of the quintic be?

Not very.

We prove that a specific quintic $x^5 - 80x + 30 = 0$ cannot be solved by radicals, without using the Galois correspondence, the degree of a field extension, or the concept of a solvable group. Instead, we mix-and-match simple facts known in the 18th and 19th Centuries, ideas from Abel and Galois, and elementary pieces of modern algebra. The proof, suitably expanded to fill in 'obvious' statements, is accessible to any student familiar with basic concepts in finite groups and polynomials. It could be used to provide motivation for a standard 'groups, rings, fields' course.

1 Introduction

We know, thanks to Abel, Galois, and others, that the quintic is unsolvable by radicals. The classical proofs are obscure to modern eyes, and it takes many weeks to develop Galois Theory to this point. So it seems worth finding a simple proof ('As simple as possible, but not more so,' Albert Einstein) that goes straight for the jugular. We present one such proof here. Different tactics could be used for several key steps depending on background or what seems appropriate. Very little in it was not known to Euler, and he could have invented the rest, if necessary by brute force. All he would really need to know is that $\mathbb{S}_5$ has an element of order 5 and $\mathbb{A}_5$ has no cyclic quotient.

The material could be taught in about six lectures as part of a standard groups-rings-fields course in abstract algebra, and nearly everything involved is of general interest in such a context. Aiming at a Big Theorem of historical interest, which can be stated very easily, can add motivation to what might otherwise be a lengthy exercise in 'general nonsense'.

2 Potted History

Somewhere between 2000 BC and 1600 BC, a Babylonian scribe, priest, or mathematician worked out how to solve quadratic equations. We know this from cuneiform tablets that record all of the computational steps required, using 'generic' examples. The procedure is equivalent to the technique of 'completing the square', which in turn is equivalent to the usual formula.

Cubic equations were less tractable, but eventually cracked when the mathematicians of Renaissance Italy unleashed the power of algebra, though not in today's notation. The story of Tartaglia, Scipio del Ferro, Antonio Fior, and Girolamo Cardano is too well known to relate again here [3, 7, 8]. It culminated in a formula for the roots of a general cubic. With the cubic in standard form

$$x^3 + ax + b = 0$$

this is of course *Cardano's formula*:

$$x = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}}$$

Observe that this expression involves nothing worse than square roots and cube roots, together with the basic operations of algebra. The formula requires cube roots of complex numbers in some cases — curiously, when all three roots are real (and the cubic is irreducible).

Shortly afterwards, Cardano's student Ludovico Ferrari obtained a more complicated formula to solve the quartic equation, again involving nothing worse than square roots (iterated to get a fourth root) and cube roots. Cardano published this procedure, along with that for the cubic, in his *Ars Magna* of 1545, unleashing a controversy with Tartaglia over priority.

The obvious next step was the general quintic equation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

and the obvious guess was that there would be an even more complicated formula for the solutions involving nothing worse than square roots, cube roots, and fifth roots. Algebraists would have been happy to allow 29th roots or whatever if necessary, but that seemed unlikely. A formula that expresses a root in terms of the coefficients, using the usual algebraic operations, together with nth roots for various n, is called a *radical*. So mathematicians were seeking a solution of the quintic by radicals. However, all attempts to derive such a formula failed, and it slowly began to dawn on the mathematical community that perhaps no such formula existed. Around 1770, Joseph-Louis Lagrange laid the foundations for the eventual proof that this was correct, by putting all of the known methods for the quadratic, cubic, and quartic into the same overall framework—and proving that this general method failed for the quintic [9]. However, that did not prove that no formula involving radicals existed; just that a specific method failed to find one.

A few hardy souls turned their attention to an impossibility proof. In 1799 Paolo Ruffini published a two-volume book totalling 516 pages, claiming to prove that the quintic cannot be solved by radicals. The mathematical community was skeptical, probably because of the length and the unfamiliar methods; however, no one found any errors, probably because no one was willing to spend enough time to find out. A distressed Ruffini published two further versions, intended to clarify his arguments, but these were also ignored [9]. In 1824 Niels Henrik Abel published an impossibility proof that was accepted [1]. It contained a key result, the 'Theorem on Natural Irrationalities', which later mathematicians realised filled the main gap in Ruffini's attempt, but at the time this was not noticed. Abel's proof used different methods from Ruffini's, and it contained a relatively minor error. However, this could easily be be patched up. A simpler and complete proof was given by Leopold Kronecker in 1879, and a general conceptual framework was established by Galois, with his famous correspondence between subfields of a splitting field and subgroups of the Galois group [2, 4, 5, 7].

The machinery of Galois theory makes the impossibility transparent, but the resulting proof requires a complicated analysis with many technicalities and — in modern form — a sophisticated level of abstraction. It is therefore an interesting exercise to find a proof that is as straightforward, and as elementary, as possible. Here we present one route to the impossibility theorem, in which most ingredients are developed in a relatively concrete form and the rest are easy to understand. The material could be a useful adjunct to, and motivation for, a standard 'groups, rings, fields' course. It also brings several branches of mathematics together with a common, comprehensible, objective.

The proof can be seen as an exercise in reverse engineering — a rediscovery of things known to Abel, Galois, Kronecker, and their predecessors. It could be made even closer to their way of thinking by removing the remaining traces of abstraction, such as the quotient of a polynomial ring by a principal ideal. Nothing presented here is new, apart perhaps from the overall package — though I doubt it would have surprised Abel, Galois, or Kronecker. Or Euler, for that matter, given a few minutes to take the ideas on board.

Unlike the classical authors, we prove that a *specific* quintic over $\mathbb{Q}$ cannot be solved by radicals, rather than the 'general' quintic whose roots are independent transcendentals. This is a stronger result because it does not assume there is a universal 'formula'. Specifically, we will prove:

Theorem 2.1 *The zeros of the quintic polynomial* $F(x) = x^5 - 80x + 30$ *cannot be expressed by radicals.*

The same proof applies to any irreducible quintic over $\mathbb{Q}$ with three real and two complex zeros. The one chosen makes it easy to establish these properties.

3 Background

We will assume, without explicit reference, a number of basic mathematical concepts and results. Among them are:

- *Groups.* Basic finite group theory up to quotients. The symmetric group $\mathbb{S}_5$. The alternating group $\mathbb{A}_5$ is a normal subgroup of $\mathbb{S}_5$ with quotient $\mathbb{Z}_2$, and comprises the even permutations. Commutators.

- *Fields.* The only fields required are subfields of $\mathbb{C}$, definable as subsets closed under the operations of algebra. In particular, if all $\alpha_i \in \mathbb{C}$, then the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_s)$ is defined as the smallest subfield of $\mathbb{C}$ containing the generators α_i. We also require the notion of isomorphism.

- *Polynomials.* Fundamental theorem of algebra. Polynomial ring $K[x]$ over a subfield K of $\mathbb{C}$. Symmetric polynomials in the zeros are functions of the coefficients. Irreducibility, Gauss's Lemma. Any isomorphism $\phi : K_1 \to K_2$ extends to an isomorphism $\phi : K_1[x] \to K_2[x]$ (we use the same notation for both) by applying ϕ to the coefficients.

- *Field Adjunction.* If K is a subfield of $\mathbb{C}$ and $\alpha \in \mathbb{C}$ is algebraic over K, then its minimal polynomial $m(x)$ is irreducible over K. The extension $K(\alpha)$ is isomorphic to $K[x]/\langle m(x)\rangle$.

- *Automorphisms.* Define $\mathrm{Aut}(K)$ to be the set of all field automorphisms of K. This is a group.

4 Solution by Radicals

Informally, a *radical* is constructed by a series of field operations and extractions of nth roots. Formally, define a subfield $L \subseteq \mathbb{C}$ to be *radical* if there is a *radical tower* of subfields $K_j \subseteq \mathbb{C}$

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots K_r = L \tag{4.1}$$

By definition, such a tower satsifies three conditions: for $i = 1, \ldots, r$

- $K_i = K_{i-1}(\alpha_i)$

- $\alpha_i \notin K_{i-1}$

- $\alpha_i^{p_i} \in K_{i-1}$ for some prime $p_i \geq 2$. (We may refine any such tower to make all p_i prime, and it is simpler to make this property part of the definition.)

Define $\theta \in \mathbb{C}$ to be *radical* if θ is an element of some radical subfield L of $\mathbb{C}$.

5 Permutations of the Zeros of F

We now introduce the central character in the drama. Let

$$F(x) = x^5 - 80x + 30 \in \mathbb{Q}[x]$$

We will study the symmetries of the zeros of F, in a sense to be made precise. This is the classical tactic. To do so, we first prove that F has exactly three simple real zeros, so the other two form a complex conjugate pair in $\mathbb{C}$.

The derivative $F'[x] = 5x^4 - 80$. This is prime to F, so all zeros are simple. The turning points of F are given by $F'(x) = 0$, so $x = \pm 2$. Since real zeros of F are separated by those of F' (Rolle's Theorem) there are at most three real zeros. Now $F(-4) = -674, F(0) = 30, F(1) = -49, F(3) = 33$, so F has three changes of sign, hence there exist exactly 3 real zeros. Since the coefficients of F are real, the other two zeros form a complex conjugate pair. As a check, Figure 1 shows the graph of F.

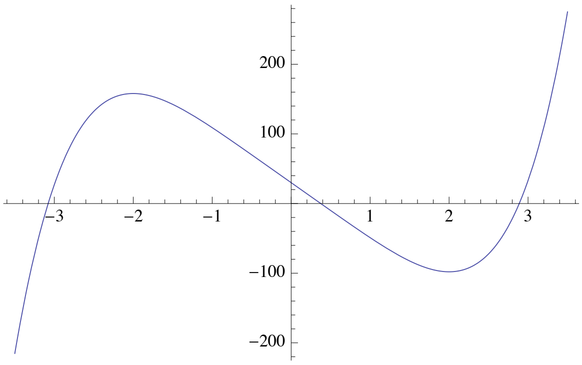

Figure 1: Graph of F.

We claim that F is irreducible over $\mathbb{Q}$. This follows from Eisenstein's Criterion for irreducibility, which we now prove for monic polynomials. Here $|$ means 'divides' and $\not|$ means 'does not divide'.

Theorem 5.1 (Eisenstein's Criterion) *Let $a(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a monic polynomial over $\mathbb{Z}$. Suppose there exists a prime p such that $p \not| a_n$, $p | a_j$ $(0 \leq j \leq n-1)$, and $p^2 \not| a_0$. Then a is irreducible over $\mathbb{Q}$.*

Proof Suppose $a(x) = b(x)c(x)$ where b, c have smaller degree than a and without loss of generality are monic. By Gauss's Lemma we can assume b, c have coefficients in $\mathbb{Z}$. Use hats to denote images modulo p. Then

$$\hat{b}(x)\hat{c}(x) = \hat{a}(x) = x^n$$

By unique factorization in $\mathbb{Z}_p[t]$, $b(x) = x^r, c(x) = x^{n-r}$ for $1 \leq s \leq n-1$. Therefore the constant terms b_0 and c_0 are both divisible by p, so $a_0 = b_0 c_0$ is divisible by p^2, a contradiction. □

Eisenstein's Criterion with $p = 5$ implies that F is irreducible over $\mathbb{Q}$, as claimed.

Let the zeros be $\theta_1, \theta_2, \theta_3, \theta_4, \theta_5$, so that

$$F(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4)(x - \theta_5) \tag{5.1}$$

Let

$$\Sigma = \mathbb{Q}(\theta_1, \theta_2, \theta_3, \theta_4, \theta_5) \subseteq \mathbb{C}$$

be the field generated by the five zeros. (This is usually called the 'splitting field' of F, but the general concept is not required.)

Proposition 5.2 *The group* $\mathrm{Aut}(\Sigma)$ *permutes the* θ_j*.*

Proof Let $\alpha \in \mathrm{Aut}(\Sigma)$. Then $\hat{\alpha}(F) = F$ since $F \in \mathbb{Q}[t]$ and α is the identity on $\mathbb{Q}$. Therefore

$$F = \hat{\alpha}(F) = (x - \alpha(\theta_1))(x - \alpha(\theta_2))(x - \alpha(\theta_3))(x - \alpha(\theta_4))(x - \alpha(\theta_5))$$

Comparing with (5.1), α must permute the five zeros. □

We may identify $\mathrm{Aut}(\Sigma)$ with a subgroup of $\mathbb{S}_5$ by making it act on the subscripts j of the θ_j.

Proposition 5.3 $\mathrm{Aut}(\Sigma)$ *contains a* 2*-cycle.*

Proof Suppose that the non-real zeros are θ_j, θ_k, with $\theta_k = \overline{\theta_j}$. Complex conjugation is an automorphism of Σ, and acts as the transposition (jk) because the other three zeros are real. □

Proposition 5.4 $\mathrm{Aut}(\Sigma)$ *acts transitively on* $\{1, 2, 3, 4, 5\}$.

Proof Let $j \in \{2, 3, 4, 5\}$. We prove that there exists an automorphism sending θ_1 to θ_j. Since F is irreducible over $\mathbb{Q}$, θ_1 and θ_j have the same minimal polynomial over $\mathbb{Q}$, namely F. Therefore there is an isomorphism

$$\psi : \mathbb{Q}(\theta_1) \to \mathbb{Q}(\theta_j)$$

We claim that ψ extends to an automorphism of Σ.

Let $m(x)$ be the minimal polynomial of θ_2 over $\mathbb{Q}(\theta_1)$. Then $m(x)$ divides $F(x)$ since $F(\theta_2) = 0$ and F is a polynomial over $\mathbb{Q}$, hence over $\mathbb{Q}(\theta_1)$. Also $(x - \theta_2)$ divides $m(x)$. From (5.1)

$$m(x) = (x - \theta_{j_1}) \cdots (x - \theta_{j_s})$$

where the j_t are distinct numbers in $\{1, 2, 3, 4, 5\}$ and $j_1 = 2$.

Clearly $\psi(m(x))$ is the minimal polynomial of $\psi(\theta_2)$ over $\psi(\mathbb{Q}(\theta_1)) = \mathbb{Q}(\theta_2)$. Since

$$F(\psi(\theta_2)) = \psi(F)(\theta_2) = F(\theta_2) = 0$$

we must have

$$\psi(m(x)) = (x - \phi_{j_1}) \cdots (x - \phi_{j_r sr})$$

where the ϕ's are some subset of the θ's. Now $\mathbb{Q}(\theta_1, \theta_2) = \mathbb{Q}(\theta_1)(\theta_2)$ is isomorphic to $\mathbb{Q}(\theta_2)(\phi_1) = \mathbb{Q}(\theta_2, \phi_1)$ by an isomorphism extending ψ. Continue inductively, adjoining $\theta_3, \theta_4, \theta_5$ in turn, and the result follows. □

Corollary 5.5 $|\mathrm{Aut}(\Sigma)|$ *is divisible by* 5.

Proof This is the orbit-stabilizer theorem. Bare hands:

Let $\Gamma = \mathrm{Aut}(\Sigma) \subseteq \mathbb{S}_5$, and define

$$\Gamma_j = \{g \in \Gamma : g(1) = j\} \qquad 1 \leq j \leq 5$$

Then Γ is the disjoint union of the Γ_j. We claim that for each j there exists a bijection $\phi_j : \Gamma_1 \to \Gamma_j$. By transitivity there exists $g_j \in \Gamma$ such that $g_j(1) = j$. Define

$$\phi_j(h) = g_j h \qquad h \in \Gamma_1$$

Then $h(1) = 1$ so $g_j h(1) = g_j(1) = j$. Therefore

$$\phi_j : \Gamma_1 \to \Gamma_j$$

Clearly ϕ_j is one-to-one. It is onto since if $k \in \Gamma_j$ then $\phi_j(g_j^{-1}k) = k$ and $g_j^{-1}k(1) = g_j^{-1}(j) = 1$. Therefore

$$|\Gamma| = \sum_{j=1}^{5} |\Gamma_j| = 5|\Gamma_1|$$

□

We next observe that any subgroup of $\mathbb{S}_5$ of order divisible by 5 has an element of order 5. This is a special case of Cauchy's Theorem [6]. The simplest direct proof I can find (other than using heavy machinery such as Sylow) follows.

Lemma 5.6 *If A is a finite abelian group and a prime p divides $|A|$, then A has an element of order p.*

Proof Induction on $|A|$. Let $1 \neq a \in A$ and consider the subgroup B generated by a. If p divides $|B|$ we are done, unless $B = A$ in which case A is cyclic of order sp for some s, and a^s has order p. If p does not divide $|B|$ then A/B has an element Bg (using multiplicative notation) of order p. Now g generates a cyclic subgroup of order divisible by p and we argue as before. □

The next proposition is very artificial, but does exactly what we need. It refers to the commutator subgroup $\Gamma' \subseteq \Gamma$.

Proposition 5.7 *If Γ is a quotient of a subgroup of $\mathbb{S}_5$ and $|\Gamma|$ is divisible by 5, then either $\Gamma' = \Gamma$ or Γ contains an element of order 5.*

Proof If $\Gamma' = \Gamma$ we are done, so we may assume $\Gamma' \subsetneq \Gamma$. If $|\Gamma'|$ is divisible by 5 then the result holds by induction on $|\Gamma|$. Otherwise $|\Gamma/\Gamma'|$ is divisible by 5. If $\Gamma' = \{1\}$ then Γ is abelian and Lemma 5.7 applies. If not, then by induction $|\Gamma/\Gamma'|$ has an element of order 5. Let this be the coset $\Gamma' g$ for $g \in \Gamma$. Then the order of g is divisible by 5, say equal to $5s$, so g^s has order 5. □

Proposition 5.8 $\mathrm{Aut}(\Sigma) = \mathbb{S}_5$.

Proof By Proposition 5.3, $\mathrm{Aut}(\Sigma)$ contains a 2-cycle. By Proposition 5.4, it is transitive, so its order is divisible by 5. By Proposition 5.7 either $\Gamma' = \Gamma$ or Γ contains an element of order 5. Now $\Gamma \ni (12)$ which is an odd permutation, but $\Gamma' \subseteq \mathbb{A}_5$ which consist of the even permutations, so $\Gamma' \neq \Gamma$. Thus Γ contains an element of order 5, which must be a 5-cycle. Conjugating the 2-cycle by suitable powers of the 5-cycle, $\mathrm{Aut}(\Sigma)$ contains every 2-cycle. But these generate $\mathbb{S}_5$. □

Proposition 5.9 *If $\alpha \in \Sigma$ and $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathbb{S}_5$, then $\alpha \in \mathbb{Q}$.*

Proof By assumption α is a symmetric polynomial in the θ_j, hence a polynomial in the coefficients of F, which are in $\mathbb{Q}$. □

6 Nice Radicals

A *nice* radical tower is one such that $L = \Sigma$ in (4.1). That is, all the radicals α_i belong to Σ. A *nice radical* is an element of a nice radical tower. We next prove a weak impossibility theorem, essentially what Ruffini proved:

Theorem 6.1 *The zeros of F are not nice radicals.*

First, we need:

Lemma 6.2 (1) *The group $\mathbb{S}_n$ has a cyclic quotient of prime order p if and only if $p = 2$ and the kernel is the alternating group $\mathbb{A}_5$.*
(2) *The group $\mathbb{A}_5$ has no nontrivial cyclic quotient.*

Of course $\mathbb{A}_5$ is simple, but this will not be needed.

Proof

(1) Suppose that N is a normal subgroup of $\mathbb{S}_5$ and $\mathbb{S}_5/N \cong \mathbb{Z}_p$. Then $\mathbb{S}_5/N$ is abelian, so N contains every commutator $ghg^{-1}h^{-1}$ for $g, h \in \mathbb{S}_5$. Let $g = (12), h = (13)$. Then

$$ghg^{-1}h^{-1} = (123)$$

is a 3-cycle. Since N is a normal subgroup, it is closed under conjugation by elements of $\mathbb{S}_5$, so it contains all 3-cycles. But the 3-cycles generate $\mathbb{A}_5$. Since $|\mathbb{S}_5/\mathbb{A}_5| = 2$ the rest follows.

(2) Suppose that N is a normal subgroup of $\mathbb{A}_5$ and $\mathbb{A}_5/N \cong \mathbb{Z}_p$. Again, N contains every commutator. Let $g = (123), h = (124)$. Then

$$N \ni ghg^{-1}h^{-1} = (12)(34)$$

By conjugation, N contains all permutations $(ab)(cd)$. Now

$$(12)(34) \cdot (12)(35) = (354)$$

so N contains a 3-cycle, hence all 3-cycles. But the 3-cycles generate $\mathbb{A}_5$. □

Next, consider the expression

$$\delta = \prod_{j<k}^{5} (\theta_j - \theta_k)$$

Then δ is not a symmetric polynomial in the θ_j, but its square $\Delta = \delta^2$ is, because

$$\Delta = \prod_{j \neq k}^{5} (\theta_j - \theta_k)$$

The expression Δ is the *discriminant* of F. If $\sigma \in \mathbb{S}_5$, then the action of σ sends δ to $\pm\delta$. The even permutations (those in $\mathbb{A}_5$) fix δ, and the odd ones map δ to $-\delta$. Indeed, this is a standard way to define odd and even permutations.

Proof of Theorem 6.1 Assume that $F(x) = 0$ is solvable by nice radicals, with a tower (4.1) of subfields K_j. Consider the first step in the tower

$$\mathbb{Q} \subseteq K_1 \subseteq \Sigma$$

where $K_1 = \mathbb{Q}(\alpha_1), \alpha_1^p \in \mathbb{Q}, \alpha_1 \notin \mathbb{Q}$, and $p = p_1$ is prime.

Since $\alpha_1 \in \Sigma$ we can act on it by $\mathbb{S}_5$, and since every σ fixes $\mathbb{Q}$ we have

$$(\sigma(\alpha_1))^p = \alpha_1^p$$

Therefore $\sigma(\alpha_1) = \zeta^{j(\sigma)}\alpha_1$, for ζ a primitive pth root of unity and $j(\sigma)$ an integer between 0 and $p-1$.

The set of all pth roots of unity in $\mathbb{C}$ is a cyclic group under multiplication, isomorphic to $\mathbb{Z}_p$. Indeed $\zeta^a\zeta^b = \zeta^{a+b}$ where $a+b$ is taken modulo p. The map $j : \mathbb{S}_5 \to \mathbb{Z}_p$ taking σ to $j(\sigma)$ is clearly a group homomorphism. Since $\alpha_1 \notin \mathbb{Q}$, the map j is nontrivial. Since $\mathbb{Z}_p$ has prime order, hence no nontrivial proper subgroups, j must be onto. Therefore $\mathbb{S}_5$ has a homomorphic image that is cyclic of order p. By Lemma 6.2, $p = 2$ and the kernel is $\mathbb{A}_5$. Therefore α_1 is fixed by $\mathbb{A}_5$.

We claim that this implies that $\alpha_1 \in \mathbb{Q}(\delta)$. Suppose that $h \in \Sigma$ is fixed by $\mathbb{A}_5$, and let $\sigma = (12)$, which lies in $\mathbb{S}_5 \setminus \mathbb{A}_5$. Write $h = h_e + h_o$ where

$$h_e = \tfrac{1}{2}(h + \sigma(h)) \qquad h_o = \tfrac{1}{2}(h - \sigma(h))$$

Then h_e is fixed by $\mathbb{A}_5$ and σ, which generate $\mathbb{S}_5$, so $h_e \in \mathbb{Q}$. Clearly h_o is mapped to $-h_o$ by σ and fixed by $\mathbb{A}_5$. Therefore δh_o is fixed by σ and $\mathbb{A}_5$, so is fixed by $\mathbb{S}_5$, so $\delta h_o \in \mathbb{Q}$. Therefore $h_o \in \mathbb{Q}(\delta)$. Finally, $h = h_e + h_o \in \mathbb{Q} + \mathbb{Q}(\delta) = \mathbb{Q}(\delta)$. Now apply this result with $h = \alpha_1$.

If $r = 2$ in (4.1) we are finished. Otherwise consider the second step in the tower

$$\mathbb{Q}(\delta) \subseteq K_2 = \mathbb{Q}(\delta)(\alpha_2)$$

By a similar argument, α_2 defines a group homomorphism $j : \mathbb{A}_5 \to \mathbb{Z}_p$, which again must be onto. But this is a contradiction. □

7 Natural Irrationalities

In order to prove the main theorem, we follow the traditional route (Ruffini's omission, proved by Abel without realising it filled the only serious gap).

Theorem 7.1 *If $F(x) = 0$ can be solved by radicals, then it can be solved by nice radicals.*

Corollary 7.2 *The equation $F(x) = 0$ is unsolvable by radicals.*

These follow from Theorem 6.1 once we establish:

Theorem 7.3 (Natural Irrationalities) *If $u \in \Sigma$ and u lies in a radical field R, then there exists a radical field R' with $u \in R' \subseteq \Sigma$.*

Once we have proved Theorem 7.3, any solution of $F(x) = 0$ by radicals can be converted into one by nice radicals. Theorem 7.1 and Corollary 7.2 are then immediate.

It remains to prove Theorem 7.3. We follow Abel's strategic insights. We need several lemmas, and a technical definition.

Definition 7.4 Let L be radical. The *height* of L is the smallest r in a radical tower (4.1).

We prove Theorem 7.3 by induction on the height of a radical field R that contains u. The key step is height 1.

Lemma 7.5 *Let M be a subfield of Σ and let $a \in M$, where a is not a pth power in M. Then*

1. *a^k is not a pth power in M for $k = 1, 2, \ldots, p-1$.*
2. *The polynomial $m(x) = x^p - a$ is irreducible over M.*

Proof
(1) Since k is prime to p there exist integers q, l such that $kl + pq = 1$. If $a^k = b^p$ with $b \in M$, then

$$(a^q b^l)^p = a^{qp} b^{lp} = a^{qp} a^{kl} = a$$

contrary to a not being a pth power in M.
(2)

Let ζ be a primitive pth root of unity in $\mathbb{C}$. Let b satisfy $b^p = a$. Over Σ,

$$x^p - a = x^p - b^p = \prod_{i=0}^{p-1} (x - \zeta^i b)$$

If $x^p - a$ is reducible, it must have a factor

$$P(x) = \prod_{i \in X} (x - \zeta^i b) \in M[x]$$

where $X \subseteq \{0, 1, \ldots, p-1\}$ and $1 \leq |X| \leq p-1$. Let $x = 0$ to deduce that

$$\zeta^s b^c \in M$$

for some s, where $c = |X|$ so $1 \leq c \leq p-1$.

There exist $h, k \in \mathbb{Z}$ such that $hc + kp = 1$. Now M contains $(\zeta^s b^c)^h = \zeta^{hs} b^{hc} = \zeta^{hs} b^{1-kp}$. But $b^p = a \in M$ so $\zeta^{hs} b \in M$. However, $(\zeta^{hs} b)^p = b^p = a$ so a is a pth power in M, a contradiction. □

Now suppose that $R = M(\alpha)$ where $\alpha^p \in M$, $\alpha \notin M$. Then $u \in R \setminus M$ is uniquely expressible as

$$u = u_0 + u_1\alpha + u_2\alpha^2 + \cdots u_{p-1}\alpha^{p-1} \tag{7.1}$$

where the $u_j \in M$.This follows by irreducibility of m. We want to put u into a more convenient form, by changing α to some other element β of $M(\alpha)$ and therefore changing a to $b = \beta^p$. In this new form, $u_1 = 1$. The precise statement is:

Lemma 7.6 *For given $u \in R$, there exist $\beta \in M(\alpha)$ and $b \in M$ with $b = \beta^p$, such that b is not the pth power of an element of M, and*

$$u = y_0 + \beta + y_2\beta^2 + \cdots y_{p-1}\beta^{p-1}$$

where the $y_j \in M$.

Proof We know that $u \notin M$, so in (7.1) some $u_s \neq 0$ for $1 \leq s \leq p-1$. Let $\beta = u_s\alpha^s$, and let $b = \beta^p$. Then $b = u_s^p\alpha^{sp} = u_s^p a^s$, and if b is a pth power of an element of M then a^s is a pth power of an element of M, contrary to Lemma 7.5(1). Therefore b is not the pth power of an element of M.

Now s is prime to p, and the additive group $\mathbb{Z}_p$ is cyclic of prime order p, so s generates $\mathbb{Z}_p$. Therefore the powers β^j of β run through the powers of α precisely once as j runs from 0 to $p-1$. Since $\beta^0 = 1, \beta^1 = \alpha^s$, we have

$$u = y_0 + \beta + y_2\beta^2 + \cdots + y_{p-1}\beta^{p-1}$$

for suitable $y_j \in M$, where in fact $y_0 = u_0$. □

Lemma 7.7 *Let $q \in \Sigma$. Then the minimal polynomial of q over $\mathbb{Q}$ splits into linear factors over L.*

Proof The polynomial

$$f_q(x) = \prod_{\sigma \in \mathbb{S}_5} (x - \sigma(q))$$

has q as a zero. Symmetry under $\mathbb{S}_5$ implies that $f_q \in \mathbb{Q}[x]$. The minimal polynomial m_q of q over $\mathbb{Q}$ divides f_q, and f_q is a product of linear factors; therefore m_q is the product of some subset of those linear factors. □

We are now ready for the climax of Galois Lite:

Proof of Theorem 2.1 We prove the theorem by induction on the height h of R.

If $h = 0$ then the theorem is obvious.

Suppose that $h \geq 1$. Then $R = R_1(\alpha)$ where R_1 is radical of height $h - 1$, and $\alpha^p \in R_1$, $\alpha \notin R_1$, with p prime. Let $\alpha^p = a \in R_1$.

By Lemma 7.6 we may assume without loss of generality that

$$u = u_0 + \alpha + u_2\alpha^2 + \cdots + u_{p-1}\alpha^{p-1}$$

where the $u_j \in R_1$. (Replace α by β as in the lemma, and then change notation back to α.) The mimimum polynomial m of x over $\mathbb{Q}$ splits into linear factors in Σ by Lemma 7.7. In particular, u is a zero of m, while all zeros of m lie in Σ. Therefore $\alpha, u_0, u_2, \ldots u_{p-1} \in \Sigma$.

Also, $\alpha, u_0, u_2, \ldots u_{p-1} \in R_1$. The height of R_1 is $h - 1$, so by induction, each of these elements lies in some radical extension of $\mathbb{Q}$ that is contained in Σ. The subfield J generated by all of these elements is clearly radical, and contains $\alpha^p, u_0, u_2, \ldots u_{p-1}$. Then $u \in J(\alpha) \subseteq \Sigma$, and $J(\alpha)$ is radical. This completes the induction step, and with it, the proof. □

References

[1] N.H. Abel *Oeuvres Complètes* (2 vols.) (eds. Sylow, L. and Lie, S.), Grøndahl, Christiana, Norway 1881.

[2] R. Bourgne and J.-P. Azra, *Écrits et Mémoires Mathématiques d'Évariste Galois*, Gauthier-Villars, Parisi 1962.

[3] C.B. Boyer, *A History of Mathematics*, Wiley, New York 1968.

[4] E. Galois, *Oeuvres Mathématiques d'Évariste Galois*, Gauthier-Villars, Paris 1897.

[5] D.J.H. Garling, *A Course in Galois Theory*, Cambridge University Press, Cambridge 1960.

[6] P.M. Neumann, G.A. Stoy, and E.C. Thompson, *Groups and Geometry*, Oxford University Press, Oxford 1994.

[7] I. Stewart, *Galois Theory* (3rd edition), Chapman and Hall /CRC Press, Boca Raton 2004.

[8] I. Stewart, *Why Beauty is Truth*, Basic Books, New York 2007.

[9] J.-P. Tignol, *Galois' Theory of Algebraic Equations*, Longman, London 1988.