Niels Hendrik Abel and Equations of the Fifth Degree

Michael I. Rosen

This paper is dedicated to the memory of my close friend and colleague Kenneth Ireland.

In most textbooks it is stated that Abel was the first to prove that the general equation of the fifth degree cannot be solved in radicals. However, Abel's proof is almost never presented. Instead, the theorem is proved by means of Galois theory.

Abel published his first proof of this theorem (at his own expense) in 1824 [**1**, Vol 1], and a longer more elaborate version appeared in Crelle in 1826 [**1**, Vol. 1]. E. Galois was thirteen years old in 1824. His spectacular paper on the theory of equations was submitted to, and rejected by, the French Academy of Science in 1830. It wasn't published until 1846, fourteen years after his death. For details of this sad story the reader can consult the very interesting book of Harold Edwards [**5**]. From all this it is clear that Abel's proof could not have used Galois theory. How then did he do it? The purpose of this article is to provide an answer to this question which will be easily accessible to a modern reader familiar with the elements of the theory of fields. The proof we will give is not identical with that of Abel, but is in the spirit of his proof and uses nothing that was unavailable to him. Both before and after the proof we try to put things in historical context, and indicate how matters developed after 1826. In particular we will discuss the earlier work of P. Ruffini and the later work of Galois, as well as a pretty contribution of L. Kronecker.

Of course, other authors have discussed this material. What's new here is mainly the mode of presentation and the arrangement of the proofs. R. Ayoub's article on Ruffini [**2**] gives an excellent historical and mathematical overview of the theorem. J. P. Tignol's recent book on the theory of equations [**7**] gives among other things a history of the subject from ancient times up to the era of Galois. Both these sources discuss Abel's contributions. Nevertheless, we feel that a relatively brief and accessible exposition of these matters from a somewhat different point of view may be of interest to readers who are unfamiliar with this fascinating piece of mathematical history.

SECTION 1. The solution of the quadratic equation $x^2 + ax + b = 0$ goes back to antiquity. The roots are

$$x_1, x_2 = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

The solution of the cubic equation $x^3 + ax^2 + bx + c = 0$ was not discovered until the 16th century. Around 1515, S. del Ferro found a solution, but did not

publish it. The solution was rediscovered in 1535 by N. Fontana, nicknamed Tartaglia, who also kept it a secret until it was coaxed out of him by G. Cardano and published in Cardano's famous work "Ars Magna". The first step is to reduce the cubic $x^3 + ax^2 + bx + c$ to the form $x^3 + px + q$ by means of the substitution $x \to x - \frac{a}{3}$. The solutions of $x^3 + px + q = 0$ are given by

$$x_1, x_2, x_3 = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}.$$

This formula must be supplemented by a rule telling how to choose the cube roots properly.

Soon after Tartaglia found his solution to the cubic equation, a solution was found to the quartic equation by L. Ferrari, the brilliant assistant to Cardano. We shall not write it down, but simply note that it involves nothing more than the rational operations of addition, subtraction, multiplication, and division, as well as extractions of square and cube roots. At this point it seemed reasonable to believe that the quintic equation could be solved by similar means, i.e. starting with the coefficients of the equations one should employ the rational operations together with the extraction of square, cube, and possibly fifth roots. However, in spite of much effort on the part of some of the best mathematicians in the world, no solution was found for over two and one half centuries.

The first mathematician to state definitively that no solution existed was Ruffini. In 1799, Ruffini published a two volume treatise entitled, "Teoria Generale delle Equazioni" in which he claims to show that the general equation of the fifth degree cannot be solved in radicals. For various reasons his results were received with skepticism, even though as eminant a mathematician as A. Cauchy found his arguments convincing. It turns out that although Ruffini did prove quite a lot, and did make important contributions, there was a significant gap in his proof. For all this the reader should consult [2]. We will discuss the gap in Ruffini's proof in Section 4.

While Ruffini's proof did not find universal acceptance, his work did help turn the direction of research away from the problem of finding a solution to an equation of the fifth degree to the problem of showing that in general no such solution exists. It is in this atmosphere that the young Abel entered the picture.

SECTION 2. In this section we set up notation, give a precise statement of the problem, review the solution via Galois theory, and begin our discussion of how Abel was able to find a proof which doesn't use Galois theory; a necessity for him since Galois theory had not yet been invented when he discovered his proof.

Throughout this paper we will use freely the notion of field, field extension, etc. Abel and his predecessors expressed themselves in different, but equivalent language. All fields will be assumed to be of characteristic zero.

Let k be a field and $f(x) \in k[x]$ a monic polynomial. If

$$f(x) = (x - \theta_1)(x - \theta_2) \cdots (x - \theta_n)$$

in some extension field of k, we call $F = k(\theta_1, \theta_2, \ldots, \theta_n)$ a splitting field of $f(x)$ over k. In other words, a splitting field F of $f(x)$ over k is the field obtained from k by adjoining all the roots of $f(x) = 0$ to k.

A finite algebraic extension E/k is called a radical tower over k if there is a series of intermediate fields

$$k = E_0 \subset E_1 \subset \cdots \subset E_{m-1} \subset E_m = E$$

such that for each $0 \leq i \leq m$, $E_{i+1} = E_i\left(\sqrt[p_i]{\alpha_i}\right)$ where p_i is a prime and $\alpha_i \in E_i^*$.

We can now give the precise definition of what it means for an equation to be solvable in radicals. Let $f(x) \in k[x]$ be a polynomial, and F a splitting field for $f(x)$ over k. We say that the equation $f(x) = 0$ is solvable in radicals if there is a radical tower E/k such that $F \subset E$. This definition is just a way of saying, in the language of fields, that the roots of $f(x) = 0$ can be obtained from the coefficients by the successive use of the rational operations and the extraction of roots. It is not clear, *a priori*, when $f(x) = 0$ is solvable in radicals, that F/k is itself a radical tower. In fact, this is not true in general as can be seen by considering the extension $\mathbf{Q}(\alpha)/\mathbf{Q}$ where $\alpha = 2\cos(2\pi/7)$. This extension is not a radical extension. On the other hand, α is a root of the irreducible cubic $x^3 + x^2 - 2x - 1$ which splits into linear factors in $\mathbf{Q}(\alpha)$.

One of the principal accomplishments of Galois was to give a beautiful criterion for when an equation $f(x) = 0$ was solvable in radicals. It is no real loss of generality to assume that $f(x)$ is irreducible, and we do so. In this circumstance, Galois shows how to assign a group G_f to $f(x)$. It is a certain transitive subgroup of the group of permutations of the roots of $f(x)$.

Theorem (Galois). *$f(x) = 0$ is solvable in radicals if and only if G_f is a solvable group.*

We recall that a finite group G is solvable if there is a sequence of subgroups

$$(e) = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$$

such that for each i, $0 \leq i < m$, G_i is normal in G_{i+1} and $p_{i+1} = [G_{i+1}: G_i]$ is prime.

To use Galois' theorem to show equations of the fifth degree and higher are not in general solvable in radicals, one computes the Galois group of the general equation of the nth degree and shows it is equal to S_n, the full symmetric group on n letters. One then shows that S_n is not a solvable group when $n \geq 5$. This is the approach used in all modern texts in algebra.

Let's explain the notion of the "general equation of degree n". Let k be a field of characteristic zero, and let $s_1, s_2, \ldots, s_n$ be quantities which are algebraically independent over k. Set $K = k(s_1, s_2, \ldots, s_n)$ and define

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n \in K[x]$$

to be the general equation of degree n over k.

Suppose $f(x) = (x - x_1)(x - x_2)\cdots(x - x_n)$ in some extension field of K. Set $L = K(x_1, x_2, \ldots, x_n)$. Clearly, L is a splitting field for $f(x)$ over K. It is not hard to show that $x_1, x_2, \ldots, x_n$ are algebraically independent over k (for details, see [6]). Moreover, the s_i are elementary symmetric functions of the x_i.

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2 \cdots x_n. \end{aligned}$$

Each permutation of the x_i induces an automorphism of L which leaves K fixed. Moreover, the only elements of L which are left fixed by all such automorphisms are the elements of K. Although this is stated in modern language, the content is all quite old. The last part is easily seen from the theorem that a symmetric polynomial is a polynomial in the elementary symmetric functions of the variables. This fact goes back, in essence, to Newton (see [5]), and was used freely by the predecessors of Abel and Galois. Reverting to modern language, we see that L/K is a Galois extension with Galois group isomorphic to S_n, or, put another way, S_n is the Galois group of the general equation of degree n over k. So, with this setup a certain amount of Galois theory was available to people like Vandermonde, Lagrange, Ruffini, and Abel. What was missing was the notion of normal subgroup. This fundamental notion is not visible in the work of these earlier authors. Thus they could not even formulate the notion of a solvable group, never mind prove Galois' criterion for when an equation was solvable in radicals. The rudiments of group theory will play a big role in our treatment of Abel's work on this problem, but nowhere will the notion of normal subgroup make an appearance.

SECTION 3. We will now devote our attention to properties of the group S_n. Very little will be needed. The elements of S_n will be considered to be permutations of the set $\{1, 2, \ldots, n\}$. For a polynomial in n variables $f(x_1, x_2, \ldots, x_n)$ and an element $\sigma \in S_n$ we define

$$(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

This action extends in a natural way to an action on rational functions. Now define

$$\delta = \prod_{i<j} (x_i - x_j) \quad \text{and} \quad \Delta = \delta^2.$$

For any $\sigma \in S_n$, $\sigma\delta = \pm\delta$. If τ is a transposition, $\tau\delta = -\delta$. Then, $A_n \subset S_n$ is defined to be the subset of S_n consisting of all $\sigma \in S_n$ such that $\sigma\delta = \delta$. Clearly, A_n is a subgroup. Note that $[S_n: A_n] = 2$ since for any $\sigma \in S$ and any transposition τ, either σ or $\tau\sigma$ is in A_n.

Facts:

1. S_n is generated by transpositions.
2. A_n is generated by 3-cycles.
3. A_n is generated by m-cycles, where m is any odd number between 3 and n.

The first two facts are standard. To prove the third, note that an m-cycle is a product of $m - 1$ transpositions, so if m is odd an m-cycle is in A_n. On the other hand, the identity

$$(a_1a_2a_3) = (a_2a_1a_3a_4 \ldots a_m)(a_ma_{m-1} \ldots a_4a_3a_2a_1)$$

shows that every 3-cycle is in the group generated by the m-cycles, so Fact 3 follows from Fact 2.

These facts are all we will need, but we add one more, due to Cauchy, since Abel made use of it in his original proof.

4. Let S_n act on $L = K(x_1, x_2, \ldots, x_n)$ as explained above. Let p be the largest prime less than or equal to n. Then, for $f \in L$, the number of distinct values taken on by f under the action of S_n (i.e. the number of distinct rational functions obtained from f by permuting the variables) either exceeds p or is at most 2.

Proof: Let $\sigma \in S_n$ be a p-cycle, and $\langle \sigma \rangle$ be the subgroup generated by σ. Define $H = \{\tau \in \langle \sigma \rangle | \tau f = f\}$. Since p is a prime, either $H = \langle \sigma \rangle$ or $H = \langle e \rangle$. Thus, either $f, \sigma f, \ldots, \sigma^{p-1} f$ are all distinct, or $\sigma f = f$. If f takes on fewer than p values, we must have $\sigma f = f$ for all p-cycles. By Fact 3 this implies that f is fixed by A_n. Since A_n has index 2 in S_n the result follows.

It is, of course, true that this result is really about S_n acting on an arbitrary set (same proof), but we have given the original formulation.

SECTION 4. We have now assembled everything we shall need. We use the notation of Section 2, except that we now add the assumption, as Abel did, that sufficiently many roots of unity are in the ground field k. Readers who are bothered by this can take $k = \mathbf{C}$, the complex numbers. Nothing essential is lost by this.

Theorem (Abel). *Let* $f(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$ *be the general equation of degree n over* k. *If* $n \geq 5$ *then this equation is not solvable in radicals.*

Recall that $f(x) = (x - x_1)(x - x_2)\ldots(x - x_n)$ in $L = K(x_1, x_2, \ldots, x_n)$. S_n acts on L by permuting the x_i and $K = k(s_1, s_2, \ldots, s_n)$ is the fixed field. If $f(x) = 0$ were solvable in radicals, we would have a radical tower E/K such that $L \subseteq E$. Abel proceeds in two steps.

Step 1. If L is contained in a radical tower over K, then L/K is itself a radical tower.

Step 2. If $n \geq 5$ then L/K is not a radical tower (in fact, Abel restricts himself to the case $n = 5$).

When he discovered his proof, Abel was unaware that the proof of Step 2 had been achieved years earlier by Ruffini. Ruffini did not give a proof of Step 1. It is not clear that he realized it was necessary. That was the gap in his proof! So, the proof of Step 1 was Abel's essential contribution.

In the next section we will give a proof of Step 2 by a method different from that of either Abel or Ruffini, although it is close in spirit to some of Ruffini's later proofs (he gave many). I have adapted it from the classic text of Burnside and Panton [**3**]. The proof is short and elegant and uses nothing that was unavailable to either Abel or Ruffini. In Section 6 a proof of Step 1 will be given which is in essence that of Abel except for the use of the language of field theory and the inclusion of more details than are given in the original paper. At the end of that section we will also sketch a portion of Abel's own proof of Step 1.

SECTION 5. With the previous notation still in effect, we will show that L/K cannot be a radical tower if $n \geq 5$.

We re-emphasize that we are assuming that the base field k contains as many roots of unity as needed.

Suppose

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n = L$$

is a radical tower. Then there is a prime p and an element $a \in K^*$ such that $K_1 = K\left(\sqrt[p]{a}\right)$. We will show that $p = 2$ and that $a = b^2 \Delta$ where $b \in K^*$ and Δ is

the symmetric function defined at the beginning of Section 3. In other words, K_1 is uniquely determined and is the field $K(\sqrt{\Delta})$.

To prove this, set $\alpha = \sqrt[p]{a}$ and let $\tau \in S_n$ be a transposition. Applying τ to $\alpha^p = a$ we find $\tau(\alpha)^p = a$ and consequently, $(\tau(\alpha)/\alpha)^p = 1$ so that $\tau(\alpha) = \zeta\alpha$ where $\zeta^p = 1$. Now apply τ to both sides of the equation $\tau(\alpha) = \zeta\alpha$ and one finds $\alpha = \tau(\zeta\alpha) = \zeta\tau(\alpha) = \zeta^2\alpha$. It follows that either $\tau(\alpha) \neq \alpha$ for some transposition τ and $p = 2$, or α is fixed by all transpositions. In the latter case, α is fixed by all S_n (use Fact 1 of Section 3) and is an element of K, contrary to assumption. The proof shows that $\tau(\alpha) = \pm\alpha$ for all transpositions τ. It follows that $\sigma(\alpha) = \pm\alpha$ for all $\sigma \in S_n$. Now, every three-cycle is a square; in fact, $(abc) = (acb)^2$. Thus, α is fixed by three-cycles and so by all of A_n by Fact 2 of Section 3. Since $\tau(\alpha) = -\alpha$ for at least one transposition we now see this must be true for every transposition. This property also holds for the polynomial δ. Consequently, α/δ is fixed by all transpositions and so also by all elements in S_n. Thus, $\alpha/\delta = b \in K$ and so $a = \alpha^2 = b^2\delta^2 = b^2\Delta$ which shows $K_1 = K(\sqrt{\Delta})$ as asserted.

We will show that when $n \geq 5$, K_1 has no radical extension in L. This will complete the proof that L/K is not a radical tower when $n \geq 5$.

Suppose $c \in K_1^*$ and $K_2 = K_1(\sqrt[q]{c})$. Set $\gamma = \sqrt[q]{c}$. By the first part of the proof, A_n leaves K_1 fixed. Let ρ be a three-cycle, and apply ρ to both sides of the equation $\gamma^q = c$. One deduces that $\rho(\gamma) = \zeta\gamma$ where $\zeta^q = 1$. Applying ρ twice to the equation $\rho(\gamma) = \zeta\gamma$ yields $\gamma = \rho^3(\gamma) = \zeta^3\gamma$. Thus, either $\rho(\gamma) = \gamma$ for all three-cycles ρ or $\rho(\gamma) \neq \gamma$ for some three-cycle and $q = 3$. In the former case, γ is fixed by A_n and is in K_1, contrary to assumption. As we point out below, one need not invoke Galois theory to establish this point. The conclusion is that $q = 3$. If $n \geq 5$, A_n is also generated by five-cycles (use Fact 3 of Section 3). Repeating the same arguments shows that $q = 5$. This contradiction establishes the result.

Remark 1. The fact that $K_1 = K(\sqrt{\Delta})$ is the fixed field of A_n can be proven as follows. Let $\gamma \in L$ be fixed by A_n and let τ be a transposition. It is not hard to see that $a = \gamma + \tau(\gamma)$ and $b = \gamma \cdot \tau(\gamma)$ are both fixed by S_n and so are in K. But, γ is a root of the equation $x^2 - ax + b = 0$ and so must generate a quadratic extension of K in L. We have seen that $K_1 = K(\sqrt{\Delta})$ is the unique quadratic extension of K in L, and so $\gamma \in K_1$.

Remark 2. The group theory behind the proof is very simple and general. Let G be a group generated by elements of order r and of order s. Suppose that $\gcd(r, s) = 1$. Then, G has no abelian quotients. For, if G/N is an abelian quotient, it must be generated by elements of order r and elements of order s. Since it is an abelian group it is annihilated by r and s, and so also by 1 which is the gcd of r and s. Thus, $G = N$. In the above proof we took $G = A_n$ for $n \geq 5$, and $r = 3$, $s = 5$.

SECTION 6. We now come to Abel's proof of Step 1; if L/K is contained in a radical tower it is a radical tower. We continue to assume that $K = k(s_1, s_2, \ldots, s_n)$ and that L is the splitting field of the generic polynomial $x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$. However, the arguments are quite general and apply whenever L/K is the splitting field of a separable polynomial over K, and K contains sufficiently many roots of unity.

All the results we will need are in Abel's original article [1, pp. 66–87] with perhaps different formulations. The first Lemma is now a standard result.

Lemma 1. *Let F be a field containing a primitive q'th root of unity. If $a \in F^*$ is not a q'th power, the $x^q - a$ is irreducible.*

If α is a root of $x^q - a = 0$ then every $\gamma \in F(\alpha)$ can be written in the form

$$\gamma = a_0 + a_1\alpha + \cdots + a_{q-1}\alpha^{q-1} \tag{1}$$

where the a_i are in F.

Lemma 2. *Assume that $x^q - a \in F[x]$ is irreducible and that α is a root. Let γ be an element of $F(\alpha)$ with $\gamma \notin F$. Then there is a $\beta \in F(\alpha)$ such that $\beta^q \in F$ and*

$$\gamma = b_0 + \beta + b_2\beta^2 + \cdots + b_{q-1}\beta^{q-1}$$

where $b_0, b_2, \ldots, b_{q-1} \in F$.

Proof: Write γ as in equation (1) above. Let $1 \le k < q$ be the smallest integer such that $a_k \neq 0$. Set $\beta = a_k\alpha^k$. Clearly, $\beta^q \in F$. For $1 \le m < q$ we can find integers r and s such that $0 \le s < q$ and $rq + sk = m$. Then

$$\alpha^m = (\alpha^q)^r(\alpha^k)^s = c_s\beta^s \quad \text{with } c_s \in F.$$

The desired expression for γ now follows by substitution into equation (1).

Lemma 3. *Let q be a prime, and ζ a primitive q'th root of unity. Then, for each integer i,*

$$1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(q-1)i} = \begin{cases} 0 & \text{if } q \text{ does not divide } i, \\ q & \text{if } q \text{ divides } i. \end{cases}$$

Proof: Again, this is standard. If q divides i the result is clear. If q doesn't divide i one uses the formula for the sum of a geometric series.

Lemma 4. *Consider the extension L/K. Let $y \in L$. Then the irreducible polynomial for y over K splits into linear factors in $L[x]$.*

Proof: Let $y_1, y_2, \ldots, y_m$ be the distinct values (conjugates) of y under the action of the symmetric group. Then, $g(x) = (x - y_1)(x - y_2)\ldots(x - y_m)$ has coefficients which are invariant under S_n and so are elements of K. The irreducible polynomial for y over K must divide $g(x)$ and the result follows. (Of course, it is easy to see that the irreducible polynomial for y over K is $g(x)$).

We now come to the main lemma which contains the crux of the argument. Roughly speaking, it asserts that if a radical extension containing K is intersected with L, the resulting pair of fields is again a radical extension. It might be worthwhile at this point to remind the reader once more that we are assuming all the roots of unity that arise are in the base field. If this assumption is not made, the result may well be false.

Lemma 5. *Let E/K be an extension field, q a prime, and $a \in E$ an element such that $x^q - a \in E[x]$ is irreducible. Let α be a root of $x^q - a = 0$. Set $M = E(\alpha) \cap L$ and $M_0 = E \cap L$. If $M \neq M_0$ then M/M_0 is a radical extension. More precisely, there is a $\beta \in M$ such that $\beta^q \in M_0$ and β generates M over M_0.*

Proof: Let $y \in M$, $y \notin M_0$. By Lemma 2, we can find a $\beta \in E(\alpha)$ such that $\beta^q = b \in E$ and

$$y = b_0 + \beta + b_2\beta^2 + \cdots + b_{q-1}\beta^{q-1}$$

where the $b_i \in E$. Let $g(x) \in K[x]$ be the irreducible polynomial for y over K, and set

$$G(x) = g\left(b_0 + x + b_2x^2 + \cdots + b_{q-1}x^{q-1}\right).$$

$G(x)$ is in $E[x]$ and has β for a root. By Lemma 1, $x^q - b \in E[x]$ is irreducible. Thus $x^q - b$ divides $G(x)$. It follows that $G(\zeta^i\beta) = 0$ where ζ is a primitive q'th root of unity, and i is any integer, and so the numbers

$$\begin{aligned} y &= y_1 = b_0 + \beta + b_2\beta^2 + \cdots + b_{q-1}\beta^{q-1} \\ y_2 &= b_0 + \zeta\beta + b_2\zeta^2\beta^2 + \cdots + b_{q-1}\zeta^{q-1}\beta^{q-1} \\ &\vdots \\ y_q &= b_0 + \zeta^{q-1}\beta + b_2\zeta^{2(q-1)}\beta^2 + \cdots + b_{q-1}\zeta^{(q-1)(q-1)}\beta^{q-1} \end{aligned} \tag{2}$$

are all roots of $g(x)$. By Lemma 4, we see that the numbers $y_1, y_2, \ldots, y_q$ are all in L (we implicitly assume that L and $E(\alpha)$ are contained in some common extension field). Multiply the i'th equation in (2) by ζ^{1-i} and add all the resulting equations. Using Lemma 3, we find

$$\beta = \frac{1}{q}\sum_{i=1}^{q} \zeta^{1-i}y_i \in L.$$

Thus $\beta \in L \cap E(\alpha) = M$ and $\beta^q = b \in L \cap E = M_0$.

It remains to show that β generates M over M_0. Let $\gamma \in M$. We can write

$$\gamma = c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{q-1}\beta^{q-1} \quad c_i \in E.$$

It will suffice to show that the coefficients $c_i \in E \cap L = M_0$. To do this one repeats the above argument to show that

$$\gamma_i = c_0 + c_1\zeta^{i-1}\beta + \cdots + \zeta^{(i-1)(q-1)}\beta^{q-1}$$

is in $L \cap E(\alpha) = M$ for $i = 1, 2, \ldots, q$. Multiply γ_i by $\zeta^{k(1-i)}$ and add up over i ranging from 1 to q. Using Lemma 3 once more we find

$$c_k\beta^k = \sum_{i=1}^{q} \zeta^{k(1-i)}\gamma_i \in M.$$

Since $\beta \in M$, it follows that $c_k \in M \cap E = M_0$ which completes the proof.

This argument is so pretty and ingenious, one is lost in admiration! We are now ready to state and prove the main result.

Theorem. *If L/K is contained in a radical tower, then L/K is itself a radical tower.*

Proof: Suppose that E/K is a radical tower and that $L \subseteq E$. We have

$$K = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_m = E$$

where $E_{i+1} = E_i\left(\sqrt[q_i]{a_i}\right)$, q_i being a prime, and $a_i \in E_i$.

Now, consider the tower

$$K = E_0 \cap L \subseteq E_1 \cap L \subseteq \cdots \subseteq E_{m-1} \cap L \subseteq L. \tag{3}$$

If $E_{i+1} \cap L = E_i \cap L$ there is nothing that need be said. If $E_{i+1} \cap L \neq E_i \cap L$ then Lemma 5 shows that $E_{i+1} \cap L/E_i \cap L$ is a radical extension (of degree q_i). Thus, after eliminating equalities, equation (3) demonstrates L as a radical tower over K.

This completes the proof of Step 1 of Section 4. Since we proved Step 2 in the last section, the proof that the general equation of degree 5 or greater cannot be solved in radicals is now complete.

Abel's original proof of Step 2 is different from the one we have given, and we want to give an idea of how he did it. To do this we sketch Abel's proof that any radical extension of K inside L has degree 2. We will assume, as Abel did, that we are dealing with the general equation of degree 5.

Let $K \subset K_1 \subset L$ and suppose $K_1 = K(\alpha)$ where $\alpha^q = a \in K$ and q is a prime. Let m be the number of distinct values that α takes on under the action of S_5 (i.e. the number of distinct conjugates of α). As we have seen, m is the degree of the irreducible equation for α over K. Since $x^q - a$ is irreducible it follows that $m = q$. Since $|S_5| = 120$, q must divide 120, i.e. $q = 2$, 3, or 5. By Cauchy's result, Fact 4 of Section 3, q cannot equal 3. Thus $q = 2$ or $q = 5$, and we must show $q = 5$ is impossible. Abel does this by first showing that the only fields between K and L of degree 5 over K are the fields $K(x_i)$, where $i = 1, 2, 3, 4, 5$. If $q = 5$ we can then assume that $K(\alpha) = K(x_1)$. By modifying α, if necessary, as in the proof of Lemma 2, we can write

$$x_1 = a_0 + \alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 \qquad a_i \in K.$$

Applying the same technique as in Lemma 5 one shows

$$\alpha = \tfrac{1}{5}\left(x_1 + \zeta^{-1}x_2 + \zeta^{-2}x_3 + \zeta^{-3}x_4 + \zeta^{-4}x_5\right) \tag{4}$$

where ζ is a primitive fifth root of unity. The contradiction arises from the fact that under the action of S_5, α has five values, but the right hand side of (4) has 120 values.

Abel goes on to show that $K_1 = K\left(\sqrt{\Delta}\right)$ and that $K\left(\sqrt{\Delta}\right)$ has no radical extensions in L. The proof of the latter assertion is similar to the one we have just given. If I am not mistaken there is a minor flaw in Abel's proof that $K_1 = K\left(\sqrt{\Delta}\right)$, but this is very minor and is easily corrected.

SECTION 7. We conclude by indicating some further developments. In this section we continue to assume that we are in characteristic zero, but will no longer demand that roots of unity be in the base field.

Abel was fascinated with the theory of equations. He published three articles on the subject, and a fourth appears among his posthumous work (see item XVIII of Volume II of his collected works [**1**]). He was at work on a major new memoir on this theory when he died, tragically, at the early age of 27.

Having proved that the general equation of degree 5 or greater cannot be solved in radicals, the thrust of his later work was to find conditions on special equations which insure that they can be solved in radicals. His best known result in this direction is the following proposition.

Proposition 1 (Abel). *Let $f(x) \in k[x]$ and suppose that $\theta_1, \theta_2, \ldots, \theta_n$ are its roots in some extension field of k. Suppose each θ_i is a rational function of θ_1, i.e. each $\theta_i = R_i(\theta_1)$ where $R_i(x) \in k(x)$. Suppose further that for each pair i and j we have*

$$R_i\left(R_j(\theta_1)\right) = R_j\left(R_i(\theta_1)\right).$$

Then $f(x) = 0$ is solvable in radicals.

The reader can see that the hypotheses can be translated as follows. The splitting field of $f(x)$ is generated by θ_1, and the Galois group of $f(x)$ is abelian. Thus the proposition is a consequence of Galois theory, though this is not, of

course, how Abel proved it. It is probably because of this result that Abel's name is attached to groups in which the elements commute with one another.

Abel never published a general criterion for when an equation is solvable in radicals, but in a letter to Crelle dated October 18, 1828 (see [1], Vol. 2), he writes

> "Si trois racines d'une équation quelconque irréductible dont le degré est un nombre premier, sont liées entre elles de sorte que l'une de ces racines puisse être exprimée rationellement par le deux autres, l'équation en question sera toujours résoluble à l'aide de radicaux."

Roughly translated, this reads "If every three roots of an irreducible equation of prime degree are related to one another in such a way that one of them may be expressed rationally in terms of the other two, then the equation is solvable in radicals". Abel gives no indication of how he came to this result, or how he proved it. It is remarkable in part because the statement is almost identical to one of the principal results of Galois' fundamental memoir of 1830, which as we have already pointed out was not published until 1846. Here is Galois' statement of the result as translated into English by Harold Edwards in [5].

Proposition 2 (Galois). *In order for an irreducible equation of prime degree to be solvable in radicals it is necessary and sufficient that once any two of the roots are known, that the others can be deduced from them rationally.*

One can rephrase this result in more modern language. Let $f(x) \in k[x]$ be irreducible of prime degree, and $\theta_1, \theta_2, \ldots, \theta_p$ be its roots. Given any three roots $\theta_i, \theta_j, \theta_m$ there exists a rational function $R(x, y) \in k[x, y]$ such that $\theta_m = R(\theta_i, \theta_j)$. Or, more simply, the splitting field of $f(x)$ is generated by any two of its roots.

Considering the simplicity and beauty of this result, it is somewhat surprising that it is not better known. A proof is outlined in the exercises to Section 8, chapter 4 of [6]. A complete proof can be found in Section 5 of Chapter 14 of [7]. Edwards [5] also gives a complete proof, but since he uses Galois' original language it is somewhat hard to read.

It might be objected that this criterion is not useful because the hypothesis is very difficult to check. As it turns out, it can be quite useful. In 1856, L. Kronecker proved the following interesting result (see [4]).

Proposition 3 (Kronecker). *Let* $\mathbf{Q}$ *be the rational numbers, and suppose* $f(x) \in \mathbf{Q}[x]$ *is an irreducible polynomial of prime degree. If* $f(x) = 0$ *is solvable in radicals, then either* $f(x)$ *has exactly one real root, or all its roots are real.*

Kronecker's proof uses the methods of Abel. He was clearly unaware of Galois' work, since this proposition is an immediate corollary of Proposition 2. If θ_1 and θ_2 are any pair of real roots, and $R(x, y) \in \mathbf{Q}[x]$, Then clearly $R(\theta_1, \theta_2)$ is also real, and so all the roots must be real.

It is easy to use Proposition 2 to produce polynomials in $\mathbf{Q}[x]$ which are not solvable in radicals. For example, let $q \geq 5$ and p be primes, and $a \geq 2$ be an integer. Let $f(x) = x^q - apx - p$. By Eisenstein's criterion, $f(x)$ is irreducible. We claim it has exactly three real roots. For x large and negative, $f(x)$ is negative. At $x = -1$, $f(-1) = -1 + p(a - 1) > 0$. At $x = 0$, $f(0) = -p < 0$. Finally, when x is large and positive, $f(x)$ is positive. By the intermediate value theorem, $f(x)$ has at least three real roots. However, $f'(x) = qx^{q-1} - ap$ has exactly two real roots, so $f(x)$ must have exactly three real roots. By Kronecker's result it

follows that $f(x) = 0$ cannot be solved in radicals. The simplest special case is $x^5 - 4x - 2$.

It is of some interest to point out that a l-adic version of Proposition 3 is valid.

Proposition 3*l*. *Suppose $f(x) \in \mathbf{Q}[x]$ is of prime degree. Let $\mathbf{Q}_l$ denote the field of l-adic numbers. If $f(x) = 0$ is solvable in radicals, then either exactly one root of $f(x)$ is in $\mathbf{Q}_l$ or all its roots are in $\mathbf{Q}_l$.*

As before, the proof is an immediate consequence of Proposition 2.

Here is an example of how to use this. Consider the polynomial

$$f(x) = x^5 + 3x^4 + 3x^3 + 6x^2 + 3x + 6.$$

$f(x)$ is an Eisenstein polynomial at 3 and so it is irreducible over $\mathbf{Q}$. Considering $f(x)$ modulo 2 we find

$$f(x) \equiv x^5 + x^4 + x^3 + x \equiv x(x + 1)(x^3 + x + 1) \pmod 2.$$

Since $f(x)$ has exactly two roots modulo 2, both of which are simple roots, one can invoke Hensel's lemma to conclude that $f(x)$ has exactly two roots in $\mathbf{Q}_2$. It follows from Proposition 3*l* that $f(x) = 0$ cannot be solved in radicals.

We conclude by using these ideas to answer the question; do there exist polynomials in $\mathbf{Q}[x]$ of prime degree, all of whose roots are real, but which are not solvable in radicals? Here is an amusing way to show that the answer is yes. Let p and l be primes. Let $f_1(x)$, $f_2(x)$, and $f_3(x) \in \mathbf{Q}[x]$ be polynomials of the same prime degree $q \geq 5$ such that $f_1(x)$ is an Eisenstein polynomial at p, $f_2(x)$ has exactly two distinct roots modulo l, and $f_3(x)$ has q distinct real roots. Use the weak approximation theorem to find a polynomial $f(x) \in \mathbf{Q}[x]$ which is p-adically close to $f_1(x)$, l-adically close to $f_2(x)$, and close in archimedean absolute value to $f_3(x)$. Then, since $f(x)$ is p-adically close to $f_1(x)$ it is irreducible. Since it is close to $f_3(x)$ in the archimedean absolute value, it has all its roots real. Finally, since it is l-adically close to $f_2(x)$, it has exactly two distinct roots in $\mathbf{Q}_l$ and by Proposition 3*l* it is not solvable in radicals.

All of this provides a nice, if simple, example of the fruitful way old and new mathematics can be combined to good effect.

REFERENCES

1. N. H. Abel, *Oeuvres Complètes*, Two Volumes, (L. Sylow and S. Lie, ed.), Grondahl and Son, Christiana, 1881.
2. R. Ayoub, Paolo Ruffini's Contributions to the Quintic, *Arch. Hist. Exact Sci.*, Vol. 23, pp. 253–277, 1980.
3. W. S. Burnside and A. W. Panton, *The Theory of Equations*, Vol. 2, Longmans, Green, and Co., London-New York-Toronto, 1928.
4. H. Dörrie, *One Hundred Great Problems of Elementary Mathematics*, Dover Publ., New York, 1965.
5. H. Edwards, *Galois Theory*, Springer Verlag, New York-Berlin-Heidelberg-Tokyo, 1984.
6. N. Jacobson, *Basic Algebra 1*, W. H. Freeman and Co., San Francisco, 1974.
7. J.-P. Tignol, *Galois' theory of algebraic equations*, Longman Scientific Technical co-published with John Wiley and Sons, New York, 1987.

Mathematics Department
Brown University
Providence, RI 02912
MA408000@brownvm.bitnet