Section V.9. Radical Extensions

Note. In this section (and the associated appendix) we resolve the most famous problem from classical algebra using the techniques of modern algebra (in fact, this is why the techniques of modern algebra were originally developed!). The idea is to find an algebraic formula for the solution of a polynomial equation (an extension of the concept of the quadratic equation for the solutions of a second degree polynomial equation to general nth degree polynomial equations). By an "algebraic formula" we mean a formula based on addition/subtraction, multiplication/division, and extraction of roots.

Note. The extraction of an nth root of an element c in a field E is equivalent to constructing an extension field $E(u)$ where $u^n = c \in E$. So solving the polynomial equation $f(x) = 0$ algebraically implies the existence of a finite tower of fields $K = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_n$ such that E_n contains a splitting field of f over K and for $i \geq 1$, $E_i = E_{i-1}(u_i)$ where some $n_i \in \mathbb{N}$ yields $u_i^{n_i} \in E_{i-1}$. Conversely, if there is a tower of fields $K = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_n$ where E_n contains a splitting field of f then $E_n = K(u_1, u_2, \ldots, u_n)$ where the u_i are as above and so each solution of the polynomial equation is of the form $f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$ for $f, g \in K[x_1, x_2, \ldots, x_n]$ by Theorem V.1.3(v). That is, each solution is expressible in terms of a finite number of elements in K, a finite number of field operations, and $u_1, u_2, \ldots, u_n$ (which are obtained by extracting roots of order $n_1, n_2, \ldots, n_n$ of $u_1, u_2, \ldots, u_n$ respectively). Thus we have the following definition.

Definition V.9.1. An extension field F of a field K is a *radical extension* of K if $F = K(u_1, u_2, \ldots, u_n)$ where some power of u_1 lies in K and for each $i \geq 2$, some power $n_i \in \mathbb{N}$ of u_i lies in $K(u_1, u_2, \ldots, u_{i-1})$.

Note. With $u_i^{n_i} \in K(u_1, u_2, \ldots, u_{i-1})$ we have that u_i is a root of $x^{n_i} - u_i^{n_i} \in K(u_1, u_2, \ldots, u_{i-1})[x]$. By Theorem V.1.12 (with $X = \{u_i\}$) we have that $K(u_1, u_2, \ldots, u_i)$ is algebraic and finite dimensional over $K(u_1, u_2, \ldots, u_{i-1})$. By Theorem V.1.2, $K(u_1, u_2, \ldots, u_n)$ is finite dimensional over K and so by Theorem V.1.11, $K(u_1, u_2, \ldots, u_n)$ is algebraic over K.

Definition V.9.2. Let K be a field and $f \in K[x]$. The equation $f(x) = 0$ is *solvable by radicals* if there exists a radical extension F of K and a splitting field E of f over K such that $F \supset E \supset K$.

Note. Since F is a radical extension of K, then every element of F can be expressed "in terms of extraction of roots" and the field operations applied to the elements of K. Since E is a splitting field of f over K, then *all* roots of $f(x) = 0$ are in F. Notice that the splitting field itself is not required to be a radical extension.

Note. The following three results set the stage for demonstrating the unsolvability of the quintic. Before stating these results, recall that the *normal closure* of field E over field K is the field E with the properties given in Theorem V.3.16:

Theorem V.3.16. If E is an algebraic extension field of K, then there exists an extension field F of E such that:

(i) F is normal over K;

(ii) No proper subfield of F containing E is normal over K;

(iii) If E is separable over K, then F is Galois over K;

(iv) $[F : K]$ is finite if and only if $[E : K]$ is finite.

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

Recall. For group G, the subgroup of G generated by the set $\{aba^{-1}b^{-1} \mid a, b \in G\}$ is called the *commutator subgroup* of G and denoted $G' = G^{(1)}$. For $i \geq 2$ define $G^{(i)} = (G^{(i-1)})'$ (that is, $G^{(i)}$ is the commutator subgroup of $G^{(i-1)}$). $G^{(i)}$ is the i^{th} *derived subgroup of* G. Group G is *solvable* if $G^{(n)} = \langle e \rangle$ for some n. That is, G is solvable if the sequence of derived subgroups of G is of the form $G > G^{(1)} > G^{(2)} > \cdots > G^{(n)} = \langle e \rangle$. These definitions are from Section II.7. The next result, concerning solvable groups, is a giant step towards both Galois' and Abel's results concerning the algebraic solvability of polynomial equations.

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

Note. The following corollary ties together solvable polynomial equations and solvable groups.

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

Note/Example. We can use the contrapositive of Corollary V.9.5 to show the nonsolvability of certain polynomial equations. Hungerford considers $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ which has Galois group S_5 (see page 276). Since S_5 is not solvable by Corollary II.7.12, then the equation $x^5 - 4x + 2 = 0$ is not solvable by radicals over $\mathbb{Q}$. In the appendix to this section, we will explore other examples of unsolvable quintics over $\mathbb{Q}$.

Note. We must be clear about the field of coefficients for a polynomial when addressing the solvable by radicals question. For any $f \in \mathbb{R}[x]$, we have that $\mathbb{C}$ is a radical extension of $\mathbb{R}$ since $\mathbb{C} = \mathbb{R}(i)$ and so the splitting field of f is either $\mathbb{R}$ or $\mathbb{C}$ by Corollary V.3.20. We know that $\mathrm{Aut}_{\mathbb{R}}(\mathbb{R}) = \{\iota\}$ and $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \cong \mathbb{Z}_2$ and so the Galois polynomial of f is solvable in both cases. To connect this to equations involving radicals, notice that all roots of $f(x) = 0$ are of the form $a + b\sqrt{-1}$ where $a, b \in \mathbb{R}$ (by the Fundamental Theorem of Algebra, Theorem V.3.19).

Note. The next proposition is a partial converse to Theorem V.9.4 (some restrictions are imposed when char(K) is finite). The corollary to this proposition is the major result of Évariste Galois on the "algebraic" solvability of polynomial equations.

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

Note. The following result is Galois' big theorem on solvability of polynomial equations. We discuss the historical setting of this result after the proof.

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

Note. The Note/Example following Corollary V.9.5 is sufficient to establish the classical version of the "unsolvability of the quintic" problem (that is, the problem in the setting of finding a formula for the solution of the general 5th degree polynomial equation with real coefficients and expressing the roots in terms of addition, multiplication, and extraction of roots). For more information on the history of algebraic solutions of 2nd, 3rd, and 4th degree polynomial equations, see the introductory online class notes for Introduction to Modern Algebra at: `http://faculty.etsu.edu/gardnerr/4127/notes/Why-am-I-here.pdf`.

Note. Between around 1550 and 1800, there were a number of mathematicians working on solving polynomial equations of degree 5. Prominent names are Rafael Bombelli (Italian), François Viéte (French), James Gregory (Scottish), Ehrenfried Walther von Tschirnhaus (German), Étienne Bézout (French), Leonhard Euler (Switzerland), Erland Samuel Bring (Sweden), and Joseph-Louis Lagrange (French) [John Derbyshire, *Unknown Quantity: A Real and Imaginary History of Algebra*, Joseph Henry Press: 2006, pages 79–83].

In 1799 Italian Paola Ruffini published a two volume work titled *General Theory of Equations* in which he included a "proof" that the quintic could not be algebraically solved. The proof ran 516 pages [Derbyshire, pages 87 and 88]. However, Ruffini's proof has been judged incomplete. The problem was that Ruffini lacked sufficient knowledge of field theory, a topic initially developed in the early 19th century [Israel Kleiner, *A History of Abstract Algebra*, Birkhäuser: 2007, page 63].

A correct proof that the quintic cannot be algebraically solved was given by the Norwegian Niels Henrik Abel in 1821 (Abel was not aware of Ruffini's alleged proof). Abel was plagued by poverty and in order to save money, he published his result in French in a six page pamphlet which was not widely circulated. Abel died in poverty in 1829 [Derbyshire, pages 96–99]. His work has been expanded and he is now viewed as one of the founders of modern algebra. As we have seen in Corollary V.9.5, if a polynomial equation $f(x) = 0$ is solvable by radicals then the Galois group of f is a solvable group. That is, the Galois group of f has a solvable series (Theorem II.8.5) and so (by definition of "solvable series," Definition II.8.3) the factor groups of a subnormal series of the Galois group of f has associated factor groups which are *abelian.* Historically, this is why commutative groups are called "abelian."

Abel (1802–1829) and Galois (1811–1832)
(From MacTutor History of Mathematics)

Note. Abel died at the age of 26. The other prominent figure in the history of algebra from the early 1800s also died very young. The Frenchman Évariste Galois was born in 1811 and died in a dual in 1832 at the age of 20. He published five papers in 1829–30 (two appearing after his death). Galois gave the conditions under which a polynomial equation $f(x) = 0$ can be solved by radicals (regardless of the degree of the polynomial). His result, in modern terminology, is our Corollary V.9.7.

The mathematical community was slow to accept Galois' result. In 1846, Joseph Liouville published the result, but it only became widely known in the 1870s, following Camille Jordan's publication of Galois' result (expanded and updated) in *Traité* *des substitutions et des équations algebraique.* Today, Galois Theory is a large area of modern mathematics (the American Mathematical Society even includes Galois Theory as a distinct area of mathematics, which they encode as "11R32"). For more historical details on Galois and his life, see `http://faculty.etsu.edu/gardnerr/Galois/Galois200.htm` (this is a website and presentation I prepared for the bicentennial of Galois' birth). In a real sense, Galois, along with Abel, are the ones who gave birth to the modern algebra we study as undergraduates and graduates. Their work on polynomial equations from classical algebra lead to the study of the areas of groups, rings, fields, and extension fields.

Note. We should comment that, just because an equation is not solvable by radicals, that does not mean that the equation is not solvable by other techniques.

The general (monic) quintic equation $x^5 + a_1x^4 + a_2x^3 + a_4x + a_5 = 0$ can be "transformed" into the *Bring-Jerrard quintic equation* of the form $y^5 - A_4y + A_5 = 0$ by using the *Tschirnhaus transformation*, named after Ehrenfried von Tschirnhaus (1651-1708) (for details on the transformation process, see pages 51–54 of R. Bruce King's *Beyond the Quartic Equation*, Boston: Birkhäuser, 1996). However, as shown by the Note/Example above, this type of equation is not in general solvable by radicals. In 1858, Charles Hermite (1822-1901) proved that the Bring-Jerrard equations can be solved in terms of elliptic functions (in his "Sur la résolution de l'équation du cinquième degré," *Comptes Rendus de l'Académie des Sciences* **XLVI**(I): 508-515). For details on the technique, see Alvin Hausner's "The Bring-Jerrard Equation and Weierstrass Elliptic Functions, *The American Mathematical Monthly*, **69**(3), 1962, 193–196 (though this reference requires some previous knowledge of elliptic functions). This is the historical approach, but there are alternate approaches to the problem (all using elliptic functions); see Chapter 6 of *Beyond the Quartic Equation.* In fact, the Wolfram software company (the developers of *Mathematica*) have a poster which explains the history and mathematics of this *analytic* approach (as opposed to a purely *algebraic* approach) to solving a quintic (Google "wolfram quintic poster" for details).

Revised: 5/1/2018