14.7 SOLVABLE AND RADICAL EXTENSIONS: INSOLVABILITY OF THE QUINTIC

We now investigate the question of solving for the roots of a polynomial by *radicals*, that is, in terms of the algebraic operations of addition, subtraction, multiplication, division and the extraction of n^{th} roots. The quadratic formula for the roots of a polynomial of degree 2 is familiar from elementary algebra and we shall derive below similar formulas for the roots of cubic and quartic polynomials. For polynomials of degree ≥ 5, however, we shall see that such formulas are not possible — this is Abel's Theorem on the insolvability of the general quintic. The reason for this is quite simple: we shall see that a polynomial is solvable by radicals if and only if its Galois group is a solvable group (which explains the terminology) and for $n \geq 5$ the group S_n is not solvable.

We first discuss *simple radical extensions*, namely extensions obtained by adjoining to a field F the n^{th} root of an element a in F. Since all the roots of the polynomial $x^n - a$ for $a \in F$ differ by factors of the n^{th} roots of unity, adjoining one such root will give a Galois extension if and only if this field contains the n^{th} roots of unity. Simple radical extensions are best behaved when the base field F already contains the appropriate roots of unity. The symbol $\sqrt[n]{a}$ for $a \in F$ will be used to denote any root of the polynomial $x^n - a \in F[x]$.

Definition. The extension K/F is said to be *cyclic* if it is Galois with a cyclic Galois group.

Proposition 36. Let F be a field of characteristic not dividing n which contains the n^{th} roots of unity. Then the extension $F(\sqrt[n]{a})$ for $a \in F$ is cyclic over F of degree dividing n.

Proof: The extension $K = F(\sqrt[n]{a})$ is Galois over F if F contains the n^{th} roots of unity since it is the splitting field for $x^n - a$. For any $\sigma \in \text{Gal}(K/F)$, $\sigma(\sqrt[n]{a})$ is another root of this polynomial, hence $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$ for some n^{th} root of unity ζ_σ. This gives a map

$$\begin{aligned} \text{Gal}(K/F) &\to \mu_n \\ \sigma &\mapsto \zeta_\sigma \end{aligned}$$

where μ_n denotes the group of n^{th} roots of unity. Since F contains μ_n, every n^{th} root of unity is fixed by every element of $\text{Gal}(K/F)$. Hence

$$\begin{aligned} \sigma\tau(\sqrt[n]{a}) &= \sigma(\zeta_\tau \sqrt[n]{a}) \\ &= \zeta_\tau \sigma(\sqrt[n]{a}) \\ &= \zeta_\tau \zeta_\sigma \sqrt[n]{a} = \zeta_\sigma \zeta_\tau \sqrt[n]{a} \end{aligned}$$

which shows that $\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau$, so the map above is a homomorphism. The kernel consists precisely of the automorphisms which fix $\sqrt[n]{a}$, namely the identity. This gives an injection of $\text{Gal}(K/F)$ into the cyclic group μ_n of order n, which proves the proposition.

Let now K be any cyclic extension of degree n over a field F of characteristic not dividing n which contains the n^{th} roots of unity. Let σ be a generator for the cyclic group $\text{Gal}(K/F)$.

Definition. For $\alpha \in K$ and any n^{th} root of unity ζ, define the *Lagrange resolvent* $(\alpha, \zeta) \in K$ by

$$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha).$$

If we apply the automorphism σ to (α, ζ) we obtain

$$\sigma(\alpha, \zeta) = \sigma\alpha + \zeta\sigma^2(\alpha) + \zeta^2\sigma^3(\alpha) + \cdots + \zeta^{n-1}\sigma^n(\alpha)$$

since ζ is an element of the base field F so is fixed by σ. We have $\zeta^n = 1$ in μ_n and $\sigma^n = 1$ in $\mathrm{Gal}(K/F)$ so this can be written

$$\begin{aligned}\sigma(\alpha, \zeta) &= \sigma\alpha + \zeta\sigma^2(\alpha) + \zeta^2\sigma^3(\alpha) + \cdots + \zeta^{-1}\alpha \\ &= \zeta^{-1}(\alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)) \\ &= \zeta^{-1}(\alpha, \zeta). \end{aligned} \tag{14.19}$$

It follows that

$$\sigma(\alpha, \zeta)^n = (\zeta^{-1})^n(\alpha, \zeta)^n = (\alpha, \zeta)^n$$

so that $(\alpha, \zeta)^n$ is fixed by $\mathrm{Gal}(K/F)$, hence is an element of F for any $\alpha \in K$.

Let ζ be a primitive n^{th} root of unity. By the linear independence of the automorphisms $1, \sigma, \ldots, \sigma^{n-1}$ (Theorem 7), there is an element $\alpha \in K$ with $(\alpha, \zeta) \neq 0$. Iterating (19) we have

$$\sigma^i(\alpha, \zeta) = \zeta^{-i}(\alpha, \zeta), \qquad i = 0, 1, \ldots,$$

and it follows that σ^i does not fix (α, ζ) for any $i < n$. Hence this element cannot lie in any proper subfield of K, so $K = F((\alpha, \zeta))$. Since we proved $(\alpha, \zeta)^n = a \in F$ above, we have $F(\sqrt[n]{a}) = F((\alpha, \zeta)) = K$. This proves the following converse of Proposition 36.

Proposition 37. Any cyclic extension of degree n over a field F of characteristic not dividing n which contains the n^{th} roots of unity is of the form $F(\sqrt[n]{a})$ for some $a \in F$.

Remark: The two propositions above form a part of what is referred to as *Kummer theory*. A group G is said to have *exponent* n if $g^n = 1$ for every $g \in G$. Let F be a field of characteristic not dividing n which contains the n^{th} roots of unity. If we take elements $a_1, \ldots, a_k \in F^\times$ then as in Proposition 36 we can see that the extension

$$F(\sqrt[n]{a_1}, \sqrt[n]{a_2}, \ldots, \sqrt[n]{a_k}) \tag{14.20}$$

is an abelian extension of F whose Galois group is of exponent n. Conversely, any abelian extension of exponent n is of this form.

Denote by $(F^\times)^n$ the subgroup of the multiplicative group $F^\times$ consisting of the n^{th} powers of nonzero elements of F. The quotient group $F^\times/(F^\times)^n$ is an abelian group of exponent n. The Galois group of the extension in (20) is isomorphic to the group generated in $F^\times/(F^\times)^n$ by the elements $a_1, \ldots, a_k$ and two extensions as in (20) are equal if and only if their associated groups in $F^\times/(F^\times)^n$ are equal.

Hence the (finitely generated) subgroups of $F^\times/(F^\times)^n$ classify the abelian extensions of exponent n over fields containing the n^{th} roots of unity (and characteristic not

dividing n). Such extensions are called *Kummer extensions*.

These results generalize the case $k = 1$ above and can be proved in a similar way.

For simplicity we now consider the situation of a base field F of characteristic 0. As in the previous propositions the results are valid over fields whose characteristics do not divide any of the orders of the roots that will be taken.

Definition.

(1) An element α which is algebraic over F can be *expressed by radicals* or *solved for in terms of radicals* if α is an element of a field K which can be obtained by a succession of simple radical extensions

$$F = K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_s = K \tag{14.21}$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$, $i = 0, 1, \ldots, s-1$. Here $\sqrt[n_i]{a_i}$ denotes some root of the polynomial $x^{n_i} - a_i$. Such a field K will be called a *root extension* of F.

(2) A polynomial $f(x) \in F[x]$ can be *solved by radicals* if all its roots can be solved for in terms of radicals.

This gives a precise meaning to the intuitive notion that α is obtained by successive algebraic operations (addition, subtraction, multiplication and division) and successive root extractions. For example, the element

$$-1 + \sqrt{17} + \sqrt{2(17 - \sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}}$$

encountered at the end of Section 5 (used to construct the regular 17-gon) is expressed by radicals and is contained in the field K_4, where

$$\begin{aligned}
K_0 &= \mathbb{Q} \\
K_1 &= K_0(\sqrt{a_0}) \qquad a_0 = 17 \\
K_2 &= K_1(\sqrt{a_1}) \qquad a_1 = 2(17 - \sqrt{17}) \\
K_3 &= K_2(\sqrt{a_2}) \qquad a_2 = 2(17 + \sqrt{17}) \\
K_4 &= K_3(\sqrt{a_3}) \qquad a_3 = 17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}.
\end{aligned}$$

Each of these extensions is a radical extension. The fact that no roots other than square roots are required reflects the fact that the regular 17-gon is constructible by straightedge and compass.

In considering radical extensions one may always adjoin roots of unity, since by definition the roots of unity are radicals. This is useful because then cyclic extensions become radical extensions and conversely. In particular we have:

Lemma 38. If α is contained in a root extension K as in (21) above, then α is contained in a root extension which is Galois over F and where each extension K_{i+1}/K_i is cyclic.

Proof: Let L be the Galois closure of K over F. For any $\sigma \in \mathrm{Gal}(L/F)$ we have the chain of subfields

$$F = \sigma K_0 \subset \sigma K_1 \subset \cdots \subset \sigma K_i \subset \sigma K_{i+1} \subset \cdots \subset \sigma K_s = \sigma K$$

where $\sigma K_{i+1}/\sigma K_i$ is again a simple radical extension (since it is generated by the element $\sigma(\sqrt[n_i]{a_i})$, which is a root of the equation $x^{n_i} - \sigma(a_i)$ over $\sigma(K_i)$). It is easy to see that the composite of two root extensions is again a root extension (if K' is another root extension with subfields K_i', first take the composite of K_1' with the fields $K_0, K_1, \ldots, K_s$, then the composite of these fields with K_2', etc. so that each individual extension in this process is a simple radical extension). It follows that the composite of all the conjugate fields $\sigma(K)$ for $\sigma \in \mathrm{Gal}(L/F)$ is again a root extension. Since this field is precisely L, we see that α is contained in a Galois root extension.

We now adjoin to F the n_i-th roots of unity for all the roots $\sqrt[n_i]{a_i}$ of the simple radical extensions in the Galois root extension K/F, obtaining the field F', say, and then form the composite of F' with the root extension:

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_i \subseteq F'K_{i+1} \subseteq \cdots \subseteq F'K_s = F'K.$$

The field $F'K$ is a Galois extension of F since it is the composite of two Galois extensions. The extension from F to $F' = F'K_0$ can be given as a chain of subfields with each individual extension cyclic (this is true for any abelian extension). Each extension $F'K_{i+1}/F'K_i$ is a simple radical extension and since we now have the appropriate roots of unity in the base fields, each of these individual extensions from F' to $F'K$ is a cyclic extension by Proposition 36. Hence $F'K/F$ is a root extension which is Galois over F with cyclic intermediate extensions, completing the proof.

Recall from Section 3.4 (cf. also Section 6.1) that a finite group G is *solvable* if there exists a chain of subgroups

$$1 = G_s \leq G_{s-1} \leq \cdots \leq G_{i+1} \leq G_i \leq \cdots \leq G_0 = G \tag{14.22}$$

with G_i/G_{i+1} cyclic, $i = 0, 1, \ldots, s-1$. We have proved that subgroups and quotient groups of solvable groups are solvable and that if $H \leq G$ and G/H are both solvable, then G is solvable.

We now prove Galois' fundamental connection between solving for the roots of polynomials in terms of radicals and the Galois group of the polynomial. We continue to work over a field F of characteristic 0, but it is easy to see that the proof is valid over any field of characteristic not dividing the order of the Galois group or the orders of the radicals involved.

Theorem 39. The polynomial $f(x)$ can be solved by radicals if and only if its Galois group is a solvable group.

Proof: Suppose first that $f(x)$ can be solved by radicals. Then each root of $f(x)$ is contained in an extension as in the lemma. The composite L of such extensions is