again of the same type by Proposition 21. Let G_i be the subgroups corresponding to the subfields K_i, $i = 0, 1, \ldots, s-1$. Since

$$\mathrm{Gal}(K_{i+1}/K_i) = G_i/G_{i+1} \qquad i = 0, 1, \ldots, s-1$$

it follows that the Galois group $G = \mathrm{Gal}(L/F)$ is a solvable group. The field L contains the splitting field of $f(x)$ so the Galois group of $f(x)$ is a quotient group of the solvable group G, hence is solvable.

Suppose now that the Galois group G of $f(x)$ is a solvable group and let K be the splitting field for $f(x)$. Taking the fixed fields of the subgroups in a chain (22) for G gives a chain

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

where K_{i+1}/K_i, $i = 0, 1, \ldots, s-1$ is a cyclic extension of degree n_i. Let F' be the cyclotomic field over F of all roots of unity of order n_i, $i = 0, 1, \ldots, s-1$ and form the composite fields $K_i' = F'K_i$. We obtain a sequence of extensions

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

The extension $F'K_{i+1}/F'K_i$ is cyclic of degree dividing n_i, $i = 0, 1, \ldots, s-1$ (by Proposition 19). Since we now have the appropriate roots of unity in the base fields, each of these cyclic extensions is a simple radical extension by Proposition 37. Each of the roots of $f(x)$ is therefore contained in the root extension $F'K$ so that $f(x)$ can be solved by radicals.

Corollary 40. The general equation of degree n cannot be solved by radicals for $n \geq 5$.

Proof: For $n \geq 5$ the group S_n is not solvable as we showed in Chapter 4. The corollary follows immediately from Theorems 32 and 39.

This corollary shows that there is no formula involving radicals analogous to the quadratic formula for polynomials of degree 2 for the roots of a polynomial of degree 5. To give an example of a *specific* polynomial over $\mathbb{Q}$ of degree 5 whose roots cannot be expressed in terms of radicals we must demonstrate a polynomial of degree 5 with rational coefficients having S_5 (or A_5, which is also not solvable) as Galois group (cf. also Exercise 21, which gives a criterion for the solvability of a quintic).

Example

Consider the polynomial $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. This polynomial is irreducible since it is Eisenstein at 3. The splitting field K for this polynomial therefore has degree divisible by 5, since adjoining one root of $f(x)$ to $\mathbb{Q}$ generates an extension of degree 5. The Galois group G is therefore a subgroup of S_5 of order divisible by 5 so contains an element of order 5. The only elements in S_5 of order 5 are 5-cycles, so G contains a 5-cycle.

Since $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$, and $f(2) = 23$ we see that $f(x)$ has a real root in each of the intervals $(-2, 0)$, $(0, 1)$ and $(1, 2)$. By the Mean Value Theorem, if there were 4 real roots then the derivative $f'(x) = 5x^4 - 6$ would have at least 3 real zeros, which it does not. Hence these are the only real roots. (This also follows easily by Descartes' rule of signs.) By the Fundamental Theorem of Algebra $f(x)$ has 5 roots in $\mathbb{C}$. Hence $f(x)$ has two complex roots which are not real. Let τ denote the automorphism of

complex conjugation in $\mathbb{C}$. Since the coefficients of $f(x)$ are real, the two complex roots must be interchanged by τ (since they are not fixed, not being real). Hence the restriction of complex conjugation to K fixes three of the roots of $f(x)$ and interchanges the other two. As an element of G, $\tau|_K$ is therefore a transposition.

It is now a simple exercise to show that any 5-cycle together with any transposition generate all of S_5. It follows that $G = S_5$, so the roots of $x^5 - 6x + 3$ cannot be expressed by radicals.

As indicated in this example, a great deal of information regarding the Galois group can be obtained by understanding the *cycle types* of the automorphisms in G considered as a subgroup of S_n. In practice this is the most efficient way of determining the Galois groups of polynomials of degrees ≥ 5 (becoming more difficult the larger the degree, of course, if only because the possible subgroups of S_n are vastly more numerous). We describe this procedure in the next section.

By Theorem 39, any polynomial of degree $n \leq 4$ can be solved by radicals, since S_n is a solvable group for these n. For $n = 2$ this is just the familiar quadratic formula. For $n = 3$ the formula is known as *Cardano's Formula* (named for Geronimo Cardano (1501–1576)) and the formula for $n = 4$ can be reduced to this one. The formulas are valid over any field F of characteristic $\neq 2, 3$, which are the characteristics dividing the orders of the radicals necessary and the orders of the possible Galois groups (which are subgroups of S_3 and S_4). For simplicity we shall derive the formulas over $\mathbb{Q}$.

Solution of Cubic Equations by Radicals: Cardano's Formulas

From the proof of Theorem 39 and the fact that a composition series for S_3 as in equation (22) is given by $1 \leq A_3 \leq S_3$ we should expect that the solution of the cubic

$$f(x) = x^3 + ax^2 + bx + c$$

(or equivalently, under the substitution $x = y - a/3$,

$$g(y) = y^3 + py + q,$$

where

$$p = \frac{1}{3}(3b - a^2) \qquad q = \frac{1}{27}(2a^3 - 9ab + 27c)\ )$$

to involve adjoining the 3rd roots of unity and the formation of Lagrange resolvents involving these roots of unity.

Let ρ denote a primitive 3rd root of unity, so that $\rho^2 + \rho + 1 = 0$. Let the roots of $g(y)$ be α, β, and γ, so that

$$\alpha + \beta + \gamma = 0$$

(one of the reasons for changing from $f(x)$ to $g(x)$). Over the field $\mathbb{Q}(\sqrt{D}\,)$ where D is the discriminant (computed in the last section) the Galois group of $g(y)$ is A_3, i.e., a cyclic group of order 3. If we adjoin ρ then this extension is a radical extension of

degree 3, with generator given by a Lagrange Resolvent, as in the proof of Proposition 37. Consider therefore the elements

$$(\alpha, 1) = \alpha + \beta + \gamma = 0$$
$$\theta_1 = (\alpha, \rho) = \alpha + \rho\beta + \rho^2\gamma$$
$$\theta_2 = (\alpha, \rho^2) = \alpha + \rho^2\beta + \rho\gamma.$$

Note that the sum of these resolvents is

$$\theta_1 + \theta_2 = 3\alpha \tag{14.23}$$

since $1 + \rho + \rho^2 = 0$. Similarly

$$\rho^2\theta_1 + \rho\theta_2 = 3\beta$$
$$\rho\theta_1 + \rho^2\theta_2 = 3\gamma. \tag{14.23'}$$

We also showed in general before Proposition 37 that the cube of these resolvents must lie in $\mathbb{Q}(\sqrt{D}, \rho)$. Expanding θ_1^3 we obtain

$$\alpha^3 + \beta^3 + \gamma^3 + 3\rho(\alpha^2\beta + \beta^2\gamma + \alpha\gamma^2) + 3\rho^2(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma) + 6\alpha\beta\gamma. \tag{14.24}$$

We have

$$\sqrt{D} = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$$
$$= (\alpha^2\beta + \beta^2\gamma + \alpha\gamma^2) - (\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma).$$

Using this equation we see that (24) can be written

$$\alpha^3 + \beta^3 + \gamma^3 + 3\rho[\frac{1}{2}(S + \sqrt{D})] + 3\rho^2[\frac{1}{2}(S - \sqrt{D})] + 6\alpha\beta\gamma \tag{14.24'}$$

where for simplicity we have denoted by S the expression

$$(\alpha^2\beta + \beta^2\gamma + \alpha\gamma^2) + (\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma).$$

Since S is symmetric in the roots, each of the expressions in (24') is a symmetric polynomial in α, β and γ, hence is a polynomial in the elementary symmetric functions $s_1 = 0$, $s_2 = p$, and $s_3 = -q$. After a short calculation one finds

$$\alpha^3 + \beta^3 + \gamma^3 = -3q \qquad S = 3q$$

so that from (24') we find ($\rho + \rho^2 = -1$ and $\rho - \rho^2 = \sqrt{-3}$)

$$\theta_1^3 = -3q + \frac{3}{2}\rho(3q + \sqrt{D}) + \frac{3}{2}\rho^2(3q - \sqrt{D}) - 6q$$
$$= \frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}. \tag{14.25}$$

Similarly, we find

$$\theta_2^3 = \frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}. \tag{14.25'}$$

Equations (25) and (23) essentially give the solutions of our cubic. One small point remains, however, namely the issue of extracting the cube roots of the expressions in (25) to obtain θ_1 and θ_2. There are 3 possible cube roots, which might suggest a total of 9 expressions in (23). This is not the case since θ_1 and θ_2 are not independent (adjoining one of them already gives the Galois extension containing all of the roots). A computation like the one above (but easier) shows that

$$\theta_1\theta_2 = -3p \tag{14.26}$$

showing that the choice of cube root for θ_1 determines θ_2. Using $D = -4p^3 - 27q^2$, we obtain Cardano's explicit formulas, as follows.

Let

$$A = \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}$$

$$B = \sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}}$$

where the cube roots are chosen so that $AB = -3p$. Then the roots of the equation

$$y^3 + py + q = 0$$

are

$$\alpha = \frac{A+B}{3} \quad \beta = \frac{\rho^2 A + \rho B}{3} \quad \gamma = \frac{\rho A + \rho^2 B}{3} \tag{14.27}$$

where $\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Examples

(1) Consider the cubic equation $x^3 - x + 1 = 0$. The discriminant of this cubic is

$$D = -4(-1)^3 - 27(1)^2 = -23$$

which is not the square of a rational number, so the Galois group for this polynomial is S_3. Substituting into the formulas above we have

$$A = \sqrt[3]{\frac{-27}{2} + \frac{3}{2}\sqrt{69}}$$

$$B = \sqrt[3]{\frac{-27}{2} - \frac{3}{2}\sqrt{69}}$$

where we choose A to be the real cube root and then from $AB = 3$ we see that B is also real. The roots of the cubic are given by (27) and we see that there is one real root and two (conjugate) complex roots (which we could have determined without solving for the roots, of course).

(2) Consider the equation $x^3 + x^2 - 2x - 1 = 0$. Letting $x = s - 1/3$ the equation becomes $s^3 - \frac{7}{3}s - \frac{7}{27} = 0$. Multiplying through by 27 to clear denominators and letting $y = 3s$ we see that y satisfies the cubic equation

$$y^3 - 21y - 7 = 0.$$