10. SOLUBILITY BY RADICALS

§10.1. A Short History of the Solubility of Polynomials

The formula for the solutions of the cubic equation $ax^3 + bx^2 + cx + d = 0$ was discovered in 1515 by Scipio del Ferro. It enables the zeros of the polynomial to be computed in terms of the coefficients, a, b, c, ... , and certain rational numbers such as ½, 27, ... by means of the operations of addition, subtraction, multiplication, division and extraction of roots. A polynomial for which such a formula exists is said to be **soluble by radicals**. As the quadratic and cubic formulae demonstrate, every quadratic and cubic is soluble by radicals.

In 1545 L. Ferrari obtained a formula for the zeros of a quartic equation which showed that quartics, too, are soluble by radicals. It is actually a little simpler than the cubic formula, but we won't present it here.

For about three centuries mathematicians tried unsuccessfully to find a formula for the zeros of a general quintic $ax^5 + bx^4 + cx^3 + dx^2 + ex + f$. It was not until Abel, in 1824, proved that no such formula exists that the search was called off. A few years later, Évariste Galois, then only 19, proved the insolubility of the quintic using quite different methods and established what is now known as Galois Theory. He went far beyond Abel by not

simply showing that there's no *general* formula for the quintic, and higher degree polynomials, but by finding a criterion for determining whether a given polynomial is soluble by radicals. While most quintics are insoluble, some *can* be solved by radicals. Galois was able to distinguish between them.

Example 1: Show that the quintic $x^5 - 2x^3 - 2x^2 + 4$ is soluble by radicals.
Solution: $x^5 - 2x^3 - 2x^2 + 4 = (x^3 - 2)(x^2 - 2)$ and the zeros are $2^{1/3}$, $2^{1/3}\omega$, $2^{1/3}\omega^2$, $2^{1/2}$ and $-2^{1/2}$.

In a sense this is cheating because rather than a quintic it is really a cubic times a quadratic. Clearly every composite quintic is soluble by radicals. But even if the quintic is prime it's still possible for it to be soluble by radicals.

Example 2: Find the solutions to the equation

$$x^5 + 5x^4 + 10x^3 + 5x + 15 = 0.$$

Solution: Clearly this polynomial is prime by Eisenstein. Yet we can solve it if we notice that it can be rewritten as $(x + 1)^5 = -14$. Then we can see that the solutions can be expressed in terms of $\sigma = e^{2\pi i/5}$, a 5'th root of unity and $14^{1/5}$:
The zeros are: $-14^{1/5} - 1$, $-14^{1/5}\sigma - 1$, $14^{1/5}\sigma^2 - 1$,
$-14^{1/5}\sigma^3 - 1$ and $-14^{1/5}\sigma^4 - 1$.

We could leave it at that, but we'll obtain another form.

Suppose $c = \cos(2k\pi/5)$ and $s = \sin(2k\pi/5)$.
Then $(c + is)^5 = 1$.

If we now equate imaginary parts we get:

$$5c^4s - 10c^2s^3 + s^5 = 0.$$

Dividing through by s (clearly $s \neq 0$) we get:

$$5c^4 - 10c^2s^2 + s^4 = 0.$$

Now putting $s^2 = 1 - c^2$ this becomes
$16c^4 - 12c^2 + 1 = 0$. Solving this as a quadratic in c^2 we get $c = \pm\sqrt{\frac{3 \pm \sqrt{5}}{8}}$ and hence $s = \pm\sqrt{\frac{5 \pm \sqrt{5}}{8}}$.

We can decide that, in fact:
$c = \sqrt{\frac{3 - \sqrt{5}}{8}}$ and $s = \sqrt{\frac{5 + \sqrt{5}}{8}}$.

The solutions to $x^5 = 1$ are thus:

$$1,$$

$$\sqrt{\frac{3 - \sqrt{5}}{8}} \pm i\sqrt{\frac{5 + \sqrt{5}}{8}} \text{ and}$$

$$-\sqrt{\frac{3 + \sqrt{5}}{8}} \pm i\sqrt{\frac{5 - \sqrt{5}}{8}}.$$

Hence the zeros of $x^5 + 5x^4 + 10x^3 + 5x + 15$ are thus:

$$-14^{1/5} - 1,$$

$$-14^{1/5}\left(\sqrt{\frac{3-\sqrt{5}}{8}} + i\sqrt{\frac{5+\sqrt{8}}{8}}\right) - 1,$$

$$-14^{1/5}\left(\sqrt{\frac{3-\sqrt{5}}{8}} - i\sqrt{\frac{5+\sqrt{8}}{8}}\right) - 1,$$

$$-14^{1/5}\left(-\sqrt{\frac{3+\sqrt{5}}{8}} + i\sqrt{\frac{5-\sqrt{8}}{8}}\right) - 1 \text{ and}$$

$$-14^{1/5}\left(-\sqrt{\frac{3+\sqrt{5}}{8}} - i\sqrt{\frac{5-\sqrt{8}}{8}}\right) - 1.$$

In this chapter we'll prove that $3x^5 - 5x^3 + 1$ is not soluble by radicals. There's nothing very special about this polynomial – it's just that it's convenient numerically.

§10.2. Solubility By Radicals

The word 'radical' is derived from the Latin word meaning 'root' or 'source'. The $\sqrt{}$ symbol is called the 'radical symbol' and any expression involving it is called a 'surd'. Used on its own it denotes a square root, but more generally $\sqrt[n]{}$ denotes the n'th root. The n'th root of a positive real number y is that positive real number x such that $x^n = y$. The n'th root is thus the root from which the powers grow.

These days we use the word 'radical' politically, to mean the opposite of 'conservative'. A radical is someone

who wants to break down traditional ways of doing things and to get back to fundamentals (roots). Galois was a radical, not only mathematically but politically as well!

A complex number α is expressible by radicals over a field F if it can be expressed in terms of elements of F using the operations of addition, subtraction, multiplication, division and extraction of roots.

Example 3: $\alpha = \sqrt[3]{\sqrt{1+\sqrt[5]{3}} + \frac{\sqrt{5}-\sqrt[4]{7}}{\sqrt[5]{3}}} + e^{2\pi i/5}$ is expressible by radicals over $\mathbb{Q}$.

More precisely α is **expressible by radicals** over F if there exists a sequence of fields $F = F_0 \leq F_1 \leq ... \leq F_n$ such that each F_{i+1} is a radical extension of F_i, and F_n contains α.

Example 4: In the case of the number α of Example 3 we can take:
$F_0 = \mathbb{Q}$
$F_1 = F_0[x^5 = 1]$ (type 1 radical extension)
$F_2 = F_1[x^5 = 3]$ (type 2 radical extension)
$F_3 = F_2[x^2 = 5]$ (type 2 radical extension)
$F_4 = F_3[x^4 = 1]$ (type 1 radical extension)
$F_5 = F_4[x^4 = 7]$ (type 2 radical extension)
$F_6 = F_5[x^2 = 1+\sqrt[5]{3}\,]$ (type 2 radical extension)
$F_7 = F_6[x^3 = 1]$ (type 1 radical extension)

$$F_8 = F_7\left[x^3 = \sqrt{1+\sqrt[5]{3}} + \frac{\sqrt{5}-\sqrt[4]{7}}{\sqrt[5]{3}} \right] \text{ (type 2 radical extension)}$$

Now fields are closed under the four field operations, so combining the elements of a field by these operations keeps us within the field. But extracting an *n*'th root usually takes us outside. However such an *n*'th root will be in some radical extension. So in expressing such a number we build up a sequence of fields, each being a radical extension of the one before. And we can arrange for each such radical extension to be type 1 or type 2.

A polynomial $f(x) \in K[x]$ is **soluble by radicals** over F if all its zeros are expressible by radicals over K. Quadratics, cubics and quartics are soluble by radicals. If we leave out the 'over F' qualification we mean 'over $\mathbb{Q}$'.

Quadratic: $f(x) = ax^2 + bx + c$:
Define $K_0 = \mathbb{Q}$ and $K_1 = K_0[x^2 = b^2 - 4ac]$.

Cubic: $f(x) = ax^3 + bx^2 + cx + d$:
In terms of the notation in Chapter 8.
$K_0 = K$ contains a, b, c, d, S, Q, P, E, F,
$\Delta_1 + \Delta_2$, $\Delta_1\Delta_2$ and $(\Delta_1 - \Delta_2)^2$.
$K_1 = K_0[x^2 = (\Delta_1 - \Delta_2)^2]$ contains $\Delta_1 - \Delta_2$,
Δ_1, Δ_2, E^3 and F^3.

$K_2 = K_1[x^3 = 1]$,

$K_3 = K_2[x^3 = E^3]$ (or $K_2[x^3 = F^3]$ if $E = 0$)
contains E, F, α, β and γ.

§10.3. Soluble Groups

Recall that a group G is **soluble** if there exists a chain of subgroups

$$1 = G_0 \leq G_1 \leq \ldots \leq G_m = G$$

such that each G_i is a normal subgroup of G_{i+1} and the quotient G_{i+1}/G_i is abelian.

The **derived subgroup** of G is G′, the group generated by all the commutators $[g, h] = g^{-1}h^{-1}gh$ where $g, h \in G$. This is a normal subgroup of G and it is the largest normal subgroup of G for which the quotient is abelian.

The ***n*'th derived subgroup $G^{(n)}$** of G is defined inductively by taking the derived subgroup of the derived subgroup ... (*n* times), in other words:

$$G_0 = G,$$
$$G^{(n+1)} = G^{(n)\prime} \text{ for all } n.$$

An alternative definition of a group G being soluble is that $G^{(n)} = 1$ for some *n*.

From this it is easy to prove that any subgroup or quotient group of a soluble group is soluble.

Example 5: $\mathbf{S}_4$ is soluble.
Simply take the sequence $1 \leq \mathbf{V}_4 \leq \mathbf{A}_4 \leq \mathbf{S}_4$.
Here $\mathbf{V}_4 = \{I, (12)(34), (13)(24), (14)(23)\}$ and $\mathbf{A}_4$ is the alternating group consisting of all even permutations.
$|\mathbf{V}_4| = 4$ and so is abelian. $|\mathbf{A}_4/\mathbf{V}_4| = 3$ and so $\mathbf{A}_4/\mathbf{V}_4 \cong \mathbf{C}_3$ which is abelian.
$|\mathbf{S}_4/\mathbf{A}_4| = 2$ and so $\mathbf{S}_4/\mathbf{A}_4 \cong \mathbf{C}_2$ which is abelian.

Example 6: $\mathbf{S}_n$ is not soluble if $n \geq 5$.
If $n \geq 5$ the only proper non-trivial normal subgroup of $\mathbf{S}_n$ is $\mathbf{A}_n$ and $\mathbf{A}_n$ is simple, that is, it has no proper non-trivial normal subgroups. (You can find the full details in my *Group Theory Volume 1* notes.) Yet $\mathbf{A}_n$ is non-abelian. We can't get down from $\mathbf{S}_n$ to $\mathbf{1}$ with abelian quotients.

§10.4. Soluble Polynomials and Soluble Groups

We're going to consider a sequence of radical extensions, but while each field is a radical extension of the previous one the last field may not be a polynomial extension of the first.

Example 7: $\mathbb{Q} \leq \mathbb{Q}[x^3 = 2] \leq \mathbb{Q}[x^3 = 2][x^4 = 1+\sqrt[3]{2}\,]$ is a sequence of radical extensions. However the algebraic conjugates over $\mathbb{Q}$ of the 4^{th} roots of $1+\sqrt[3]{2}$ include the 4^{th} roots of $1+\sqrt[3]{2}\,\omega$ and the 4^{th} roots of $1+\sqrt[3]{2}\,\omega^2$ and so cannot be a polynomial extension of $\mathbb{Q}$. However we can reach a

polynomial extension by making further radical extensions.

Theorem 2: Suppose $F \leq H \leq K$ where H is a polynomial extension of F and K is a radical extension of H. Then there is a sequence of radical extensions:

$$K = K_1 \leq K_2 \leq ... \leq K_m$$

where K_m is a polynomial extension of F.

Proof: Suppose that $H = F[f(x)]$ and $K = H[x^n = \alpha]$ where $\alpha \in H$. Let $\alpha = \alpha_1, \alpha_2, ..., \alpha_m$ be the algebraic conjugates of α over F, with minimum polynomial $p(x)$ over F. Take $K_{i+1} = K_i[x^n = \alpha_i]$. Then $K_m = F[f(x)p(x)]$.

Example 7 continued:

The minimum polynomial of $1+\sqrt[3]{2}$ is:

$$(x - 1)^3 - 2 = x^3 - 3x^2 + 3x - 3$$

so $1+\sqrt[3]{2}$ has 3 conjugates over $\mathbb{Q}$, namely $1+\sqrt[3]{2}$, $1+\sqrt[3]{2}\,\omega$ and $1+\sqrt[3]{2}\,\omega^2$.

Take $K_1 = \mathbb{Q}[x^3 = 2][x^4 = 1+\sqrt[3]{2}\,] = K$

$K_2 = K_1[x^4 = 1+\sqrt[3]{2}\,\omega]$

$K_3 = K_2[x^4 = 1+\sqrt[3]{2}\,\omega^2]$

$= F[x^{12} - 3x^8 + 3x^4 - 3 = 0]$

Theorem 3: If $F = \mathbb{Q}[a_0, a_1, \ldots, a_n]$ and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

is soluble by radicals the $G(F[f(x) = 0]/F)$ is a soluble group.

Proof: Suppose that $f(x)$ is soluble by radicals and that F is the extension of $\mathbb{Q}$ by the coefficients. Then there's a sequence of fields $F = F_0 < F_1 < \ldots < F_m$ such that each F_{i+1} is a radical extension of F_i and $F[f(x) = 0] \leq F_m$.

We may assume, without loss of generality, that the radical extensions are all of type 1 or 2 (for if not we can introduce some intermediate field so that they are). We may also assume that F_m is a polynomial extension of F since, by Theorem 2, after each radical extension we can add extra radical extensions until we reach a polynomial extension.

For each i, define $G_i = G(F_m/F_i)$. These form a chain $1 = G_m \leq G_{m-1} \leq \ldots \leq G_0$. Applying Theorem 3 of §7.2 to the chain $F_i \leq F_{i+1} \leq F_m$ we conclude that G_{i+1} is a normal subgroup of G_i and $G_i/G_{i+1} \cong G(F_{i+1}/F_i)$. By Theorems 7 and 8 of §7.3 these quotients are all abelian. Hence $G_0 = G(F_m/F)$ is soluble.

Now consider the chain $F \leq F[f(x) = 0] \leq F_m$. Then $G(F_m/F)/G(F[f(x) = 0]) \cong G(F[f(x) = 0]/F)$. Hence $G(F_m/F)$ is soluble and every quotient of a soluble group is soluble, so $G(F[f(x) = 0]/F)$ is soluble.

§10.5. Insoluble Quintics

In view of Theorem 3 all we have to do to prove that a given polynomial is insoluble by radicals is to compute its Galois group and show that this group is not soluble.

Now the Galois group of a quintic must be isomorphic to a subgroup of $\mathbf{S}_5$. If it was $\mathbf{S}_5$ itself we'd know that this quintic isn't soluble by radicals. And, of course, if the zeros of this particular quintic are not expressible by radicals over $\mathbb{Q}$ there can't be a formula for solving the general quintic along the lines that we have described.

But how do you compute the Galois group of a polynomial whose zeros we can't get hold of? Normally we find the zeros of the polynomial and construct the Galois group from there. In the case of an insolvable polynomial we have to compute its Galois group indirectly.

Theorem 4: If p is prime, a subgroup of $\mathbf{S}_p$ that contains a p-cycle and a 2-cycle must be $\mathbf{S}_p$ itself.

Proof: Let $H \leq \mathbf{S}_p$ and suppose that H contains $a = (x_1 x_2 \ldots x_p)$ and $b = (x_i x_j)$.

Since a cycle can be written with any of its symbols at the start we may renumber the symbols so that:

$a = (x_1 x_2 \ldots x_p)$ and $b = (x_1 x_r)$ for some $r > 1$.

Since $a^{r-1}$is a p-cycle that maps x_1 to x_r we may renumber the symbols so that:

$$a = (1\ 2 \ldots p) \text{ and } b = (1\ 2).$$

Now $ab = (2\ 3\ \ldots\ p)$ and so $(ab)^{-1}b(ab) = (1\ 3)$. Remember that the conjugate a permutation has the same cycle structure as the original permutation and that we obtain the conjugate by mapping each symbol in the cycle structure using the conjugating permutation.

In general $(ab)^{-(k-2)}b(ab)^{k-2} = (1\ k)$ for $k = 1, 2, \ldots, p$.

So H contains all the 2-cycles of the form $(1\ k)$.

But if $h \neq k$, $(h\ k) = (1\ h)(1\ k)(1\ h) \in$ H.
So H contains *all* 2-cycles.
But every permutation is a product of 2-cycles so H contains every permutation. In other words H = $\mathbf{S}_p$.

Theorem 5: A prime polynomial over $\mathbb{Q}$ of prime degree p with exactly 2 non-real zeros and $p - 2$ real zeros has $\mathbf{S}_p$ as its Galois group over $\mathbb{Q}$.
Proof: The Galois group, G, is isomorphic to a subgroup, H, of $\mathbf{S}_p$. By Theorem 9 of §7.4, |H| is divisible by p and so by Cauchy's Theorem H has an element of order p which, in S_p, must be a p-cycle. Since the polynomial has exactly 2 non-real zeros this subgroup of $\mathbf{S}_p$ also contains a 2-cycle, corresponding to the conjugation automorphism. By Theorem 4, H = $\mathbf{S}_p$.
Corollary: If $p \geq 5$ then such a polynomial is not soluble by radicals over $\mathbb{Q}$.

Theorem 6: $f(x) = 3x^5 - 5x^3 + 1$ is not soluble by radicals over $\mathbb{Q}$.

Proof: $f(x)$ has prime degree 5.

Modulo 2 it is $x^5 + x^3 + 1$. It has no zeros in $\mathbb{Z}_2$. So if it is composite it must be a prime quadratic times a prime cubic. The only prime quadratic is $x^2 + x + 1$ and the only prime cubics are $x^3 + x + 1$ and $x^3 + x^2 + 1$. Neither product gives $x^5 + x^3 + 1$.

So $f(x)$ is prime over $\mathbb{Z}_2$ and hence prime over $\mathbb{Q}$.

Now $f'(x) = 15x^2(x^2 - 1)$. The stationary points are thus a local maximum at $(-1, 3)$, a stationary point of inflection at $(0, 1)$ and a local minimum at $(1, -1)$.

From elementary calculus we can see that $f(x)$ has exactly 3 real roots (one below -1, one between 0 and 1, and one greater than 1). Thus there must be exactly two non-real zeros, forming a conjugate pair.

EXERCISES FOR CHAPTER 10

Exercise 1:

(i) Show that $x = \mathrm{i}$ is a zero of the polynomial

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

(ii) Hence factorise $f(x)$ over $\mathbb{Q}$.

(iii) Show that $\mathbb{Q}[f(x) = 0] = \mathbb{Q}[\alpha, \sqrt{q}, \mathrm{i}]$ for some $\alpha \in \mathbb{C}$ and some $q \in \mathbb{Q}$.

(iv) By finding a suitable chain of subgroups show that $f(x)$ is soluble by radicals over $\mathbb{Q}$.

Exercise 2: Let $h(x) = x^5 + 6x^4 + 6x^3 + 6x^2 + 8x - 8$.
(i) Show that $h(x)$ is prime over $\mathbb{Q}$.
(ii) Find the number of real zeros of $h(x)$.
(iii) Show that $h(x)$ is not soluble by radicals over $\mathbb{Q}$.
(iv) Show that there exists $\alpha \in \mathbb{Q}[f(x) = 0]$ such that $\alpha \notin \mathbb{Q}$ but $\alpha^2 \in \mathbb{Q}$.

Exercise 3:
Show that if p is a prime and $p \geq 5$ then the polynomial $f(x) = x^5 - 5p^4x + p$ is not soluble by radicals over $\mathbb{Q}$**.**

SOLUTIONS FOR CHAPTER 10

Exercise 1:
(i) $f(i) = -1 - 4 + 2 + 3 = 0$.

(ii) Hence $x^2 + 1$ is a factor.
$f(x) = (x^4 - 5x^2 + 3)(x^2 + 1)$.
(ii) The zeros of $f(x)$ are $\pm\alpha, \beta, \pm i$ where:

$$\alpha = \sqrt{\frac{5 + \sqrt{13}}{2}} \text{ and } \beta = \sqrt{\frac{5 - \sqrt{13}}{2}}.$$

Hence $\mathbb{Q}[f(x) = 0] = \mathbb{Q}[\alpha, \beta, i]$.
Now $\alpha\beta = \sqrt{3}$, so $\mathbb{Q}[f(x) = 0] = \mathbb{Q}[\alpha, \sqrt{3}, i]$.

(iii) Let $F_0 = \mathbb{Q}$,
$F_1 = \mathbb{Q}[\sqrt{13}]$,
$F_2 = \mathbb{Q}[\alpha]$,

$F_3 = \mathbb{Q}[\alpha, \sqrt{3}]$,
$F_4 = \mathbb{Q}[\alpha, \sqrt{3}, i]$.

Then $\mathbb{Q} = F_0 \leq F_1 \leq F_2 \leq F_3 \leq F_4 = \mathbb{Q}[f(x) = 0]$ is a sequence of radical extensions and so $f(x)$ is soluble by radicals.

Exercise 2:
(i) mod 3, h(x) becomes $x^5 + 2x + 1$.
This has no zeros over $\mathbb{Z}_3$ and so no linear factors.
The monic prime quadratics over $\mathbb{Z}_3$ are:

$$x^2 + 1,\ x^2 + x + 2 \text{ and } x^2 + 2x + 2.$$

None of these divide $x^5 + 2x + 1$ and so this has no quadratic factors. It must therefore be prime over $\mathbb{Z}_3$ and hence prime over $\mathbb{Q}$.

(ii) Since h(–5) = –23 and h(–4) = 184 there is at least one real zero between –5 and –4.
Since h(–2) = 16 and h(–1) = –11 there is at least one real zero between –2 and –1.
Since h(0) = –8 and h(1) = 19 there is at least one real zero between 0 and 1.
Hence h(x) has at least 3 real zeros.

Now $h'(x) = 5x^4 + 24x^3 + 18x^2 + 12x + 8$
$h''(x) = 20x^3 + 72x^2 + 36x + 12$
$h'''(x) = 60x^2 + 144x + 36 = 12(x^2 + 12x + 3)$
which has zeros at $x = \dfrac{-6 \pm \sqrt{33}}{5}$.

At both these values $h''(x) > 0$ so $h''(x)$ has exactly one real zero.

Hence $h'(x)$ has exactly one stationary point and so at most two real zeros.

Hence $h(x)$ has at most two stationary points and so at most 3 real zeros.

We have thus shown that $h(x)$ has exactly 3 real zeros.

(iii) $h(x)$ must therefore have exactly 2 non-real zeros. Since it is prime over $\mathbb{Q}$ and has prime degree 5, its Galois group is isomorphic to $\mathbf{S}_5$ and so is not soluble. Thus $h(x)$ is not soluble by radicals over $\mathbb{Q}$.

(iv) Since the Galois group is isomorphic to $\mathbf{S}_5$ it has a normal subgroup isomorphic to $\mathbf{A}_5$. The corresponding fixed field must have degree 2 over $\mathbb{Q}$ and so must have the form $\mathbb{Q}[x^2 = a]$ for some $a \in \mathbb{Q}$ whose square roots are irrational.

Exercise 3:

If a polynomial has prime degree p, is prime over $\mathbb{Q}$ and has exactly 2 non-real zeros then its Galois group over $\mathbb{Q}$ is isomorphic to $\mathbf{S}_p$. If $p \geq 5$ then S_p is not a soluble group and hence the polynomial is not soluble by radicals over $\mathbb{Q}$. Now $f(x)$ has prime degree 5 and is prime over $\mathbb{Q}$ by Eisenstein, using the prime p itself.

Furthermore, $f'(x) = 5x^4 - 5p^4$.

The real zeros of $f'(x)$ are $x = \pm p$.

f(–p) = – p^5 + 5p^5 + p = p + 4p^5 > 0 and
f(p) = p^5 – 5p^5 + p = p – 4p^5 < 0 so f(x) has 3 real zeros (one before – p, one between – p and p and one after p).

Hence f(x) is not soluble by radicals over $\mathbb{Q}$.