

3. SOLUBILITY BY RADICALS

(WHY QUINTICS ARE NOT SOLUBLE BY RADICALS)

§3.1. The Quadratic Equation From An Advanced Standpoint

The formula for the solutions to a quadratic equation has been known since the time of the ancient Babylonians. Expressed in our modern day notation the solutions to $ax^2 + bx + c = 0$ are:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The usual method of obtaining the quadratic formula involves a method called *completing the square* which doesn't generalize to higher degree polynomials. The following derivation of the quadratic formula gets more to the heart of the matter.

Let the roots of $ax^2 + bx + c = 0$ be α and β . Then it is well known that the sum of the roots and the product of the roots can be expressed very simply in terms of the coefficients:

$$S = \alpha + \beta = \frac{-b}{a}$$

$$P = \alpha\beta = \frac{c}{a}$$

Both the sum of the roots and the product of the roots are symmetric in terms of α and β . If α and β are swapped they remain unchanged.

These two functions of the roots are called the *elementary symmetric functions* and other symmetric functions of the roots can be expressed in terms of them.

Example 1: Express each of the following symmetric functions in terms of the elementary symmetric ones:

(a) $\alpha^2\beta + \beta^2\alpha$, (b) $\frac{1}{\alpha} + \frac{1}{\beta}$, (c) $\alpha^2 + \beta^2$, (d) $\alpha^3 + \beta^3$.

Solution:

(a) $\alpha^2\beta + \beta^2\alpha = \alpha\beta(\alpha + \beta) = PS$;

(b) $\frac{1}{\alpha} + \frac{1}{\beta} = \frac{\alpha + \beta}{\alpha\beta} = \frac{S}{P}$;

(c) $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = S^2 - 2P$;

(d) $\alpha^3 + \beta^3 = (\alpha + \beta)^3 - 3(\alpha^2\beta + \alpha\beta^2) = S^3 - 3PS$.

It's obvious that any function which can be expressed in terms of $\alpha + \beta$ and $\alpha\beta$ must be symmetric in α and β . What is a little less well known is the fact that the converse holds. Every symmetric function in α and β can be expressed in terms of $\alpha + \beta$ and $\alpha\beta$. It follows that the value of such functions can be computed directly from the coefficients without having to solve the quadratic.

Now an expression such as $\alpha - \beta$ is not symmetric. Swapping α and β in fact changes the sign of the expression. However if we square $\alpha - \beta$, this change of sign disappears and we again get the symmetric function

$$\begin{aligned}(\alpha - \beta)^2 &= \alpha^2 + \beta^2 - 2\alpha\beta = (\alpha + \beta)^2 - 4\alpha\beta = S^2 - 4PS \\ &= \left(\frac{-b}{a}\right)^2 - 4\left(\frac{c}{a}\right) = \frac{b^2 - 4ac}{a^2}\end{aligned}$$

Hence we can find the values of $\alpha - \beta$ simply by taking square roots, getting

$$\alpha - \beta = \frac{\pm \sqrt{b^2 - 4ac}}{a}$$

Now $\alpha + \beta = \frac{-b}{a}$ and so adding these equations and dividing by 2 we get

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

This formula can be expressed as an algorithm:

- (1) Find $\Delta = b^2 - 4ac$;
- (2) Solve $z^2 = \Delta$;
- (3) Solve $2ax = z - b$.

Each step involves solving a linear equation or finding an n 'th root.

§3.2. The Cubic Equation

The general cubic equation has the form $ax^3 + bx^2 + cx + d = 0$. Let the zeros be α , β and γ . Then the elementary symmetric functions of these roots can be expressed directly in terms of the coefficients as follows:

$$S = \alpha + \beta + \gamma = \frac{-b}{a}$$

$$Q = \alpha\beta + \beta\gamma + \gamma\alpha = \frac{c}{a}$$

$$P = \alpha\beta\gamma = \frac{-d}{a}$$

As before, any symmetric function can be expressed in terms of these. For example:

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = S^2 - 2Q.$$

Example 2: Express the following symmetric functions in terms of P, Q, S:

(a) $\alpha^2 + \beta^2 + \gamma^2$, (b) $\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma}$, (c) $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha + \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$,

(d) $\alpha^3 + \beta^3 + \gamma^3$.

Solution:

(a) $\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = S^2 - 2Q;$

(b) $\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma} = \frac{\alpha\beta + \alpha\gamma + \beta\gamma}{\alpha\beta\gamma} = \frac{Q}{P};$

(c) $\alpha^2\beta + \alpha\beta^2 + \alpha^2\gamma + \alpha\gamma^2 + \beta^2\gamma + \beta\gamma^2 = (\alpha\beta + \alpha\gamma + \beta\gamma)(\alpha + \beta + \gamma) - 3\alpha\beta\gamma = QS - 3P;$

(d) $\alpha^3 + \beta^3 + \gamma^3 = (\alpha + \beta + \gamma)^3 - 3(\alpha^2\beta + \alpha\beta^2 + \alpha^2\gamma + \alpha\gamma^2 + \beta^2\gamma + \beta\gamma^2) - 6\alpha\beta\gamma$
 $= S^3 - 3(QS - 3P) - 6P = S^3 - 3QS + 3P.$

Other expressions have partial symmetry. For example consider:

$$\Delta_1 = \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha \text{ and}$$

$$\Delta_2 = \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2.$$

These are not completely symmetric because under the permutation $(\alpha \beta)$ the expressions Δ_1 and Δ_2 change into one another. But Δ_1 and Δ_2 are symmetric under the permutations $(\alpha \beta \gamma)$ and its inverse $(\alpha \gamma \beta)$. Including the *identity* permutation which keeps all of α , β and γ fixed we find that Δ_1 and Δ_2 are unchanged by three of the 6 permutations but are swapped by the other three. We could say that they have *half-symmetry*.

Other expressions have this half-symmetry. One notable example is the discriminant:

$$\Delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$$

which can be written as $\Delta_2 - \Delta_1$. For three of the 6 permutations on $\{\alpha, \beta, \gamma\}$ Δ is left fixed and for the other three Δ is sent to $-\Delta$.

This is just what we had with the quadratic discriminant. If we now *square* the discriminant we get something that is fully symmetric. And being fully symmetric we can express Δ^2 in terms of the elementary symmetric functions S, Q and P and hence we can find Δ^2 in terms of the coefficients. All we have to do is to take the square root and we have found Δ .

$$\Delta_1 = \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha; \quad \Delta_2 = \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2;$$

$$\Delta_1 + \Delta_2 = (\alpha\beta + \beta\gamma + \gamma\alpha)(\alpha + \beta + \gamma) - 3\alpha\beta\gamma = QS - 3P;$$

$$\Delta_1\Delta_2 = PS^3 + Q^3 - 6SPQ + 9P^2;$$

$$(\Delta_1 - \Delta_2)^2 = (\Delta_1 + \Delta_2)^2 - 4\Delta_1\Delta_2 = (QS - 3P)^2 - 4(PS^3 + Q^3 - 6SPQ + 9P^2)$$
$$= Q^2S^2 - 27P^2 - 4PS^3 + 18SPQ - 4Q^3.$$

From these equations we can find Δ_1 and Δ_2 .

Example 3: Find Δ_1 and Δ_2 for the polynomial $x^3 - 3x - 2$.

Solution: $S = 0, Q = -3, P = 2$.

$$\Delta_1 + \Delta_2 = QS - 3P = -6;$$

$$(\Delta_1 - \Delta_2)^2 = Q^2S^2 - 27P^2 - 4PS^3 + 18SPQ - 4Q^3 = -108 + 108 = 0$$

Hence $\Delta_1 - \Delta_2 = 0$ and so $\Delta_1 = \Delta_2 = -3$.

For the quadratic equation, the role of Δ_1 and Δ_2 was played by the roots α and β themselves. But with the cubic, we have a bit more work to do.

The expression $E = \alpha + \beta\omega + \gamma\omega^2$ is not symmetric. It's not even half-symmetric because the cycle $(\alpha \beta \gamma)$ changes E to $\omega^2 E = \beta + \gamma\omega + \alpha\omega^2$. Similarly the expression $F = \alpha + \beta\omega^2 + \gamma\omega$ changes to $\omega E = \beta + \gamma\omega^2 + \alpha\omega$. But watch!

If we *cube* E and F then ω and ω^2 will disappear and so E and F will be half-symmetric. Maybe we can express them in terms of S, Q, P plus the half-symmetric expressions Δ_1 and Δ_2 . If so then we can find the values of E and F .

$$\begin{aligned} \text{Now in fact: } E^3 &= (\alpha + \beta\omega + \gamma\omega^2)^3 = S^3 - 3QS + 9P + 3\omega^2\Delta_1 + 3\omega\Delta_2 \quad \text{and} \\ F^3 &= (\alpha + \beta\omega^2 + \gamma\omega)^3 = S^3 - 3QS + 9P + 3\omega\Delta_1 + 3\omega^2\Delta_2. \end{aligned}$$

Example 4: Find E and F for the polynomial $x^3 - 3x - 2$.

Solution: $E^3 = S^3 - 3QS + 9P + 3\omega^2\Delta_1 + 3\omega\Delta_2 = 0 - 0 + 18 - 9\omega^2 - 9\omega = 27 - 9(1 + \omega + \omega^2) = 27$ and similarly $F^3 = 27$.

Thus we have three possibilities for each of E and F :

$$E, F = 3, 3\omega \text{ or } 3\omega^2.$$

There are 9 combinations of these values but not all of them will produce solutions, but we won't go into that here. Once we have a finite number of possibilities to check it is a straight-forward matter to weed out any "spurious" solutions.

But having values for E and F , how do we get our hands on the roots α, β and γ ? That's easy! We have:

$$\begin{aligned} \alpha + \beta + \gamma &= S \\ \alpha + \beta\omega + \gamma\omega^2 &= E; \\ \alpha + \beta\omega^2 + \gamma\omega &= F. \end{aligned}$$

If we simply add these equations, and use the relationship $1 + \omega + \omega^2 = 0$, we get $3\alpha = S + E + F$ and so $\alpha = (S + E + F)/3$.

Example 5: Solve the cubic $x^3 - 3x - 2 = 0$.

Solution: Remember that $S = 0$, so $\alpha = (E + F)/3$. Taking $E = F = 3$ we get $\alpha = 2$. We can now substitute back into the above equations to get $\beta = \gamma = -1$. Verifying, we can then check that $x^3 - 3x - 2 = (x + 1)(x + 1)(x - 2)$.

It's possible to summarize the whole process into a single formula as follows. Firstly, in order to keep the formula simple, we divide through by the coefficient of x^3 to get the cubic in the form: $x^3 - Sx^2 + Qx - P$, so that S is the sum of the roots etc. Then, observing that the transformation $y = x - S/3$ leads to a cubic with no x^2 term, we can (without loss of generality) consider cubic equations of the form:

$$x^3 + Qx - P = 0$$

The zeros can be expressed by the formula:

$$\alpha, \beta, \gamma = \sqrt[3]{\frac{P}{2} + \sqrt{\frac{P^2}{4} + \frac{Q^3}{27}}} + \sqrt[3]{\frac{P}{2} - \sqrt{\frac{P^2}{4} + \frac{Q^3}{27}}}$$

The cube roots are computed over the complex field and are chosen so that the product of these terms is $-Q/3$

Example 6: Solve $x^3 - 6x - 6 = 0$.

Solution: $P = 6, Q = -6$ so one solution is $\sqrt[3]{4} + \sqrt[3]{2}$ (This is the only real solution.)

§3.3. A Short History of the Problem

The above formula for the roots of the cubic equation $ax^3 + bx^2 + cx + d = 0$ was discovered in 1515 by Scipio del Ferro. Notice that it enables the zeros of the polynomial to be computed in terms of the coefficients, a, b, c, \dots , and certain rational numbers $\frac{1}{2}, 27, \dots$ 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**. Certainly, as the above 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.

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, Evaristé Galois, then only 19, proved the insolubility of the quintic using different methods and established what is now known as Galois Theory. He went far beyond Abel by not simply showing that there is no *general* formula 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.

Example 7: Find the solutions to the equation $z^5 = 1$.

Solution: Trivially the polynomial $z^5 - 1$ is soluble by radicals because the zeros are the 5'th roots of unity. They are $z = e^{2\pi ik/5}$ for $k = 0, 1, 2, 3, 4$ with $k = 0$ giving $z = 1$. We could leave it at that. But we'll obtain another form.

Suppose $k \neq 1$ and put $c = \cos(2k\pi/5)$ and $s = \sin(2k\pi/5)$ we get $(c + is)^5 = 1$. If we now equate imaginary parts we get $5c^4s - 10c^2c^3 + s^5 = 0$. Dividing through by s (clearly $s \neq 0$) we get $5c^4 - 10c^2c^2 + s^4 = 0$. 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 $s = \pm \sqrt{\frac{5 \pm \sqrt{5}}{8}}$. There are 8 combinations here but some do not hold (by examining the real parts).

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

$$1, \quad \sqrt{\frac{3 - \sqrt{5}}{8}} \pm i \sqrt{\frac{5 + \sqrt{5}}{8}}, \quad \text{and} \quad -\sqrt{\frac{3 + \sqrt{5}}{8}} \pm i \sqrt{\frac{5 - \sqrt{5}}{8}}$$

In these notes 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.

§3.4. Radical Extensions of Fields

We now prepare to set up a precise definition of solubility of a polynomial by radicals in terms of field extensions. All fields, unless otherwise stated, are number fields, that is, subfields of the field of complex numbers.

$F[\alpha_1, \alpha_2, \dots, \alpha_n]$ denotes the smallest subfield of \mathbf{C} which contains the field F and the complex numbers $\alpha_1, \alpha_2, \dots, \alpha_n$.

Clearly $F[\alpha_1, \dots, \alpha_n][\beta_1, \dots, \beta_m] = F[\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m]$. That is extending by the α 's and then extending that field by the β 's is equivalent to extending by all the α 's and all the β 's in one operation. Also the field is the same if the extending complex numbers are simply rearranged.

If F is a number field $F[f(x) = 0]$ denotes $F[\alpha_1, \dots, \alpha_n]$ where $\alpha_1, \dots, \alpha_n$ are the zeros of $f(x)$ in \mathbf{C} . Such an extension is called a **polynomial extension** of F . An extension of a field F by the roots of a quadratic polynomial is called a **quadratic extension**.

Example 8: $\mathbf{Q}[x^2 + x + 1 = 0]$ is a (quadratic) polynomial extension of \mathbf{Q} .

A polynomial extension of the form $F[x^n - a = 0]$, which we shall also write as $F[x^n = a]$, is called a **radical extension** of F .

Example 9: $\mathbf{Q}[x^2 + x + 1] = \mathbf{Q}[\omega, \omega^2] = \mathbf{Q}[x^3 = 1]$ and so is a radical extension of \mathbf{Q} . It can also be written as

Since the roots of the quadratic $ax^2 + bx + c = 0$ are $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

$F[ax^2 + bx + c = 0] = F[x^2 = b^2 - 4ac]$, that every quadratic extension is a radical extension.

Example 10: $\mathbf{Q}[x^2 + x + 1] = \mathbf{Q}[\omega, \omega^2] = \mathbf{Q}\left[-\frac{1}{2} + \frac{\sqrt{3}i}{2}, -\frac{1}{2} - \frac{\sqrt{3}i}{2}\right] = \mathbf{Q}[\sqrt{3}i]$
 $= \mathbf{Q}[x^2 = -3]$.

§3.5. A Precise Statement of the Problem

The word “radical” is derived from the Latin word meaning “root” or “source”. The $\sqrt{\quad}$ symbol is called the “radical symbol” and any expression involving it is called a “radical” or a “surd”. Used on its own it denotes a square root, but more generally $\sqrt[n]{\quad}$ denote the n 'th root. The n 'th root of a positive real number y is that 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” 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. Galois was a “radical”, not only mathematically but politically as well.

A polynomial is defined to be **soluble by radicals** if its zeros can be expressed in terms of its coefficients, and certain rational numbers, using the operations of addition, subtraction, multiplication, division and extraction of roots.

Now field are closed under the first four of these operations, so combining the elements of a field by these operations keeps us within the field. But extracting an n 'th root may take 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.

Example 10: If $\alpha = \sqrt[3]{\sqrt{i + \sqrt[5]{3}} + \frac{\sqrt{5 - \sqrt[4]{7}}}{\sqrt[5]{3}}} + e^{2\pi i/5}$ we can reach a field containing α

from \mathbf{Q} through the following sequence of radical extensions:

$$F_0 = \mathbf{Q}$$

$$F_1 = \mathbf{Q}[x^5 = 1]$$

$$F_2 = F_1[x^5 = 3]$$

$$F_3 = F_2[x^2 = 5]$$

$$F_4 = F_3[x^4 = 7]$$

$$F_5 = F_4[x^4 = 1]$$

$$F_6 = F_5[x^2 = i + \sqrt[5]{3}]$$

$$F_7 = F_6 \left[x^3 = \sqrt{i + \sqrt[5]{3}} + \frac{\sqrt{5 - \sqrt[4]{7}}}{\sqrt[5]{3}} \right].$$

Then $e^{2\pi i/5} \in F_1$, $\sqrt[5]{3} \in F_2$, $\sqrt{5} \in F_3$, $\frac{\sqrt{5 - \sqrt[4]{7}}}{\sqrt[5]{3}} \in F_4$, $i \in F_5$, $i + \sqrt[5]{3} \in F_6$ and $\alpha \in F_7$.

So if a polynomial is soluble by radicals we can find a sequence of radical extensions where the first field is \mathbf{Q} extended by the coefficients of the polynomial and the last term contains all the roots.

Example 11: If $\alpha = \sqrt[4]{\sqrt{2} + \sqrt[3]{2}}$ then $(\alpha^4 - \sqrt{2})^3 = 2$. Thus $\alpha^{12} - 3\sqrt{2}\alpha^8 + 6\alpha^4 - 2\sqrt{2} = 8$ and so $\sqrt{2}(3\alpha^8 + 2) = \alpha^{12} + 6\alpha^4 - 8$. Hence $2(3\alpha^8 + 2)^2 = (\alpha^{12} + 6\alpha^4 - 8)^2$ and so

$$\alpha^{24} - 6\alpha^{16} - 16\alpha^{12} + 12\alpha^8 - 96\alpha^4 + 56 = 0.$$

The zeros of $(x^6 + 12x^4 - 4x^3 + 36x^2 - 24x + 4)^4$ are $\sqrt[4]{\sqrt{2} + \sqrt[3]{2}}$ where each n-th root includes all n possibilities. This gives all 24 zeros.

The field $\mathbf{Q}[x^3 = 2][x^2 = 2][x^4 = \sqrt{2} + \sqrt[3]{2}]$ contains them all and it can be reached from \mathbf{Q} by a sequence of radical extensions.

NOTE: It is important to go via $\mathbf{Q}[x^3 = 2][x^2 = 2]$ because we need to reach a field that contains $\sqrt{2} + \sqrt[3]{2}$ before extending by the zeros of $x^4 = \sqrt{2} + \sqrt[3]{2}$ can be considered as a radical extension.

This enables us to restate the definition of solubility by radicals in terms of field extensions.

The polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ is soluble by radicals (over \mathbf{Q}) if and only if there is a chain of fields:

$$F_0 < F_1 < \dots < F_m$$

such that:

- (1) $F_0 = \mathbf{Q}[a_0, a_1, \dots, a_n]$;
- (2) each F_{i+1} is a radical extension of F_i ;
- (3) $\mathbf{Q}[f(x) = 0] \leq F_m$.

The connection between this formal definition and the intuitive one in terms of formulae, is best explained by exhibiting the sequences of radical extensions involved in solving the quadratic and the cubic.

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

Define $F_0 = \mathbf{Q}[a, b, c]$ and $F_1 = F_0[x^2 = b^2 - 4ac]$.

According to the quadratic formula, the zeros of $f(x)$ belong to F_1 and so $\mathbf{Q}[f(x) = 0] \leq F_1$. Here the chain of radical extensions has just a single link.

Cubic: $f(x) = x^3 + qx - p$:

$$x = \sqrt[3]{\frac{p}{2} + \sqrt{\frac{p^2}{4} + \frac{q^3}{27}}} + \sqrt[3]{\frac{p}{2} - \sqrt{\frac{p^2}{4} + \frac{q^3}{27}}}$$

$ax^3 + bx^2 + cx + d$:

In the non-trivial case we take

$F_0 = \mathbf{Q}[p, q]$ which contains $\alpha = \frac{p^2}{4} + \frac{q^3}{27}$;

$F_1 = F_0[x^2 = \alpha]$ which contains $\beta = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} + \frac{q^3}{27}}$

$F_2 = F_1[x^3 = \beta]$.

The theorem we have set as our goal can be expressed as follows:

There is no sequence of fields $\mathbf{Q} = F_0 < F_1 < \dots < F_m$ such that each F_{i+1} is a radical extension of F_i and $\mathbf{Q}[3x^5 - 5x^3 + 1 =] \leq F_m$.

§3.6. Galois Groups of Field Extensions

We have just re-expressed the property of being soluble by radical in terms of field extensions. The next step is to translate these in terms of groups of field automorphisms.

An **automorphism of a field** F is a bijective (1-1 and onto) map $\theta: F \rightarrow F$ such that $(x + y)^\theta = x^\theta + y^\theta$ and $(xy)^\theta = x^\theta y^\theta$ for all $x, y \in F$.

Example 12: The map $\lambda: \mathbf{C} \rightarrow \mathbf{C}$ defined by $z^\lambda = \bar{z}$ is an automorphism of \mathbf{C} since $\overline{u + v} = \bar{u} + \bar{v}$ and $\overline{uv} = \bar{u}\bar{v}$ for all complex numbers u, v .

It is easy to check that the set of all automorphisms of F form a group with respect to multiplication of maps: $x^{\theta\phi} = (x^\theta)^\phi$ for all $x \in F$. It is called the **automorphism group** of the field and is denoted by $\text{Aut}(F)$.

Instead of focussing on fields themselves, and all their associated automorphisms, we consider field extensions $K:F$ and the subgroup of $\text{Aut}(K)$ consisting of those which fix every element of F .

If F is a subfield of K we define the Galois group of K over F to be:

$$\{\theta \in \text{Aut}(K) \mid x^\theta = x \text{ for all } x \in F.\}$$

It is easily seen to be a subgroup of $\text{Aut}(K)$ and it is denoted by $G(K/F)$.

Example 13: Find $G(\mathbf{C}/\mathbf{R})$.

Solution: The identity map 1 and the conjugation map λ are clearly in $G(\mathbf{C}/\mathbf{R})$ since they fix every real number. We now show that $G(\mathbf{C}/\mathbf{R}) = \{1, \lambda\}$, that is that every automorphism of \mathbf{C} which fixes \mathbf{R} is either 1 or λ .

Now $i^2 = -1$ so $(i^2)^\theta = (-1)^\theta = -1$. Thus $(i^\theta)^2 = -1$. There are thus only two possibilities for i^θ , namely $\pm i$.

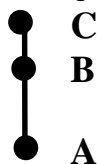
If $i^\theta = i$ then for any complex number $(a + bi)^\theta = a^\theta + b^\theta i^\theta = a + bi$ and so θ is the identity automorphism. On the other hand if $i^\theta = -i$ then for any complex number $(a + bi)^\theta = a^\theta + b^\theta i^\theta = a - bi$ and so $\theta = \lambda$.

Galois translated the property of a polynomial being soluble by radicals into a certain property of the Galois group (he didn't use the intermediate stage of field extensions — that came much later). This property is the existence of a sequence of subgroups, each normal in the next, with abelian quotients. This we recognise as the property of the group being soluble. In fact the word “soluble” as applied to groups was derived from its connection with solubility by radicals.

To prove that $3x^5 - 5x^3 + 1$ is not soluble by radicals we will compute its Galois group over \mathbf{Q} . This group turns out to be S_5 which, as we know, isn't soluble.

§3.7. Extending Isomorphisms

The heart of Galois Theory is the process of restricting and extending field automorphisms. Suppose we have a sequence of field extensions $A \leq B \leq C$.



There are three Galois groups we can form here: $G(\mathbf{C}/\mathbf{A})$, $G(\mathbf{B}/\mathbf{A})$ and $G(\mathbf{C}/\mathbf{B})$. Is there any connection between them? Indeed there is. In many cases it's a fact that the third one is isomorphic to the quotient of the first two. The trick to proving this is to consider the restriction of an automorphism of \mathbf{C} to the subfield \mathbf{B} .

Suppose $\theta \in \text{Aut}(\mathbf{C})$. If we restrict θ to \mathbf{B} we get an isomorphism between \mathbf{B} and $\text{im } \theta$. And if $\text{im } \theta = \mathbf{B}$ then the restriction is an automorphism of \mathbf{B} . Moreover if θ fixes the elements of \mathbf{A} then, of course, so will the restriction to \mathbf{B} . We've thus taken an element of the Galois group $G(\mathbf{C}/\mathbf{A})$ and, by restricting it to \mathbf{B} , come up with an element of $G(\mathbf{B}/\mathbf{A})$.

On the other hand, if $\varphi \in G(\mathbf{B}/\mathbf{A})$, can we extend it to an element of $G(\mathbf{C}/\mathbf{A})$. That is, can we define it consistently for elements of \mathbf{C} that lie outside of \mathbf{B} ?

Extending and restricting are reverse operations. If $\theta \in G(\mathbf{C}/\mathbf{A})$ can be restricted to $\varphi \in G(\mathbf{B}/\mathbf{A})$ (meaning that $\theta(x) = \varphi(x)$ for all $x \in \mathbf{B}$ but that θ is defined for other elements while φ is not) then φ can be extended to θ . Of course there may be several different automorphisms of \mathbf{C} which agree on the elements of \mathbf{B} and so we could have different automorphisms giving the same restriction. Looking at this another way, it might be possible to extend a given automorphism of \mathbf{B} in more than one way to an automorphism of \mathbf{C} .

Example 14: The set $C = \{0, 1, 2, 3\}$ is a field under the following operations.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

The set $B = \{0, 1\}$ is a subfield of C . In this simple example we'll take A to be $\{0, 1\}$ as well.

Now if θ is the map $\theta: C \rightarrow C$ defined by $0^\theta = 0, 1^\theta = 1, 2^\theta = 3, 3^\theta = 4$ and $\varphi: B \rightarrow B$ is the identity map then φ is the restriction of θ to B . Conversely, φ can be extended to θ . But this is not the only possible extension for φ can also be extended to the identity automorphism of C .

Restricting takes an automorphism of C to an automorphism of B so it can be thought of as a function from $G(C/A)$ to $G(B/A)$. We define $\rho: G(C/A) \rightarrow G(B/A)$ by $\theta^\rho = \theta$ restricted to B (assuming that $\text{im } \theta = B$). In other words we define $x^{\theta^\rho} = x$ for all $x \in B$. Clearly the restriction of a product of automorphisms is the product of their restrictions, so ρ is a homomorphism. The kernel consists of all those automorphisms of C whose restriction to B is the identity. But this is just $G(C/B)$.

We've got the makings of a First Isomorphism application here.

$$G(C/A)/\ker \rho \cong \text{im } \rho, \text{ that is, } G(C/A)/G(C/B) \cong \text{im } \rho.$$

Now $\text{im } \rho$ consists of all those elements of $G(C/A)$ which are the restriction of some automorphism of C . But this is the set of all those elements of $G(B/A)$ which can be extended to an automorphism of C . Perhaps they can all be extended in this way. In that case $\text{im } \rho$ is the whole of $G(B/A)$. That would make the following relationship hold between the three Galois groups involved:

$$G(C/A)/G(C/B) \cong G(B/A).$$

But there are two problems. An automorphism of C needn't restrict to an automorphism of B . It might map B to something other than B in which case it would be an isomorphism but not an automorphism. The second problem is that an automorphism of B needn't extend to an automorphism of C , in which case the image of ρ wouldn't be the whole of $G(B/A)$.

The amazing thing is that if C and B are both polynomial extensions of A then both problems are resolved. Every element of $G(C/A)$ does restrict to an element of $G(B/A)$ and every element of $G(B/A)$ extends back to an element of $G(C/A)$. This simple idea is what makes Galois Theory work!

Theorem 1: Suppose $\varphi: F \rightarrow F^\varphi$ is an isomorphism and that α is algebraic over F with minimum polynomial $p(x) \in F[x]$. If β is any zero of $p^\varphi(x)$ then φ can be extended to an isomorphism $\theta: F[\alpha] \rightarrow F^\varphi[\beta]$ such that $\alpha^\theta = \beta$.

Proof: $F[\alpha] \cong F[x]/p(x)F[x] \cong F^\varphi[x]/p^\varphi(x)F^\varphi[x] \cong F^\varphi[\beta]$. Moreover isomorphisms exist under which $\alpha \rightarrow x + p(x)F[x] \rightarrow x + p^\varphi(x)F[x] \rightarrow \beta$.

Theorem 2: Suppose that $\varphi: H \rightarrow K$ is an isomorphism and that $f(x) \in H[x]$ is non-zero. Then if $f(x) = f^\varphi(x)$, φ may be extended to an isomorphism $\theta: H[f(x) = 0] \rightarrow K[f(x) = 0]$

Proof: We proceed by induction on n , the number of zeros of $f(x)$, counting multiple zeros according to their multiplicities. By the Fundamental Theorem of Algebra this is in fact the degree of $f(x)$ but we do not assume this since we will prove the fundamental Theorem in the next chapter.

The theorem is trivial for $n = 0$. Suppose that $n \geq 1$ and that the theorem holds for polynomials with fewer than n zeros. Let α be one of the zeros of $f(x)$ and let $p(x)$ be the minimum polynomial of α over H . By Theorem 1 φ may be extended to $\sigma: H[\alpha] \rightarrow K[\alpha]$ such that $\alpha^\sigma = \alpha$.

Now by the remainder theorem applied to the field $H[\alpha]$ we may write $f(x) = (x - \alpha)g(x)$ for some $g(x) \in H[\alpha][x]$ that is, with coefficients in $H[\alpha]$. Since $g^\sigma(x) = g(x)$ it follows from the induction hypothesis that σ may be extended further to an isomorphism $\theta: H[\alpha][g(x) = 0] \rightarrow K[\alpha][g(x) = 0]$. But $H[\alpha][g(x) = 0] = H[f(x) = 0]$ and $K[\alpha][g(x) = 0] = K[f(x) = 0]$ and so the proof is complete.

Theorem 3: Suppose that $A \leq B \leq C$ is a chain of fields. If C is a polynomial extension of A , every element of $G(B/A)$ is the restriction of (i.e. may be extended to) an element of $G(C/A)$.

Proof: Suppose that $C = A[f(x) = 0]$ where $f(x) \in A[x]$, and that $\varphi \in G(B/A)$. Then $C = B[f(x) = 0]$ and $f^\varphi(x) = f(x)$. So by Theorem 2 φ may be extended to an automorphism $\theta \in G(C/A)$.

§3.8. Restricting Automorphisms

Theorem 4: If $f(x) \in F[x]$, every automorphism in the Galois group of $f(x)$ over F permutes the zeros of $f(x)$.

Proof: Since $f^\varphi(x) = f(x)$, $f(\alpha^\varphi) = f^\varphi(\alpha^\varphi) = f(\alpha)^\varphi$ and so $f(\alpha^\varphi) = 0$ if and only if $f(\alpha) = 0$.

Theorem 5: Suppose $A \leq B \leq C$. If B is a polynomial extension of A then every element of $G(C/A)$ can be restricted to (i.e. is an extension of) some element of $G(B/A)$.

Proof: Let $\varphi \in G(C/A)$ and suppose $B = A[f(x) = 0]$. Then $B^\varphi = A^\varphi[f^\varphi(x) = 0] = A[f(x) = 0] = B$.

Theorem 6: Suppose $A \leq B \leq C$ and that B, C are polynomial extensions of A . Then $G(C/B)$ is a normal subgroup of $G(C/A)$ and

$$G(C/A) / G(C/B) \cong G(B/A).$$

Proof: For $\theta \in G(C/A)$ define by θ^ρ to be $\theta|_B$. By theorem 5 $\theta^\rho \in G(B/A)$. It is easily checked that ρ is a homomorphism and $\ker \rho = G(C/B)$. By theorem 3 $\text{im } \rho = G(B/A)$. The theorem now follows from the first isomorphism theorem.

Theorem 7: Every finite-dimensional extension of a field is contained in some polynomial extension.

Proof: Let $A \leq B$ and suppose $[B:A] = n < \infty$. Let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be a basis for B over A . For each i , $A[\alpha_i]$, being a subspace of B has finite dimension over A . Let $f(x)$ be the product of the minimum polynomials of the α_i . Then $B \leq A[f(x) = 0]$.

§3.9. Galois Groups of Radical Extensions

We have expressed the solubility of a polynomial by radicals in terms of a sequence of radical extensions. We now calculate the Galois group of a radical extension.

There are two special types of radical extension. We can extend a field by the n 'th roots of unity. This we shall call a type 1 radical extension. Or we can extend a field that already contains the n 'th roots of unity by the n 'th roots of some other element. We shall call this a type 2 extension.

Any radical extension that is not of one or other of these special types can be split into a type 1 extension followed by a type 2 extension: $F \leq F[x^n = 1] \leq F[x^n = \alpha]$. So we shall concentrate on calculating the Galois groups of each type.

Theorem 8: If $B = A[\alpha_1, \alpha_2, \dots, \alpha_n]$ the identity automorphism is the only element of $G(B/A)$ which fixes all of the α_i .

Proof: Let $\theta \in G(B/A)$ and suppose that $\alpha_i^\theta = \alpha_i$ for each i . Then $F = \{x \in B \mid x^\theta = x\}$ is a subfield of B which contains F and each α_i . Since B is the smallest such field $F = B$ and so θ is the identity.

Theorem 9: $G(F[x^n = 1]/F)$ is abelian.

Proof: The n 'th roots of 1 are $1, \omega, \omega^2, \dots, \omega^{n-1}$ where $\omega = e^{2\pi i/n}$. Hence $F[x^n = 1] = F[\omega]$. Let $\theta, \phi \in G(F[\omega]/F)$. Since θ, ϕ permute the n 'th roots of 1, $\omega^\theta = \omega^r$ and $\omega^\phi = \omega^s$ for some integers r, s .

Now $\omega^{\theta\phi} = (\omega^r)^\phi = (\omega^r)^s = \omega^{rs}$ while $\omega^{\phi\theta} = \omega^{rs}$. Hence $\theta^{-1}\phi^{-1}\theta\phi$ fixes ω and the elements of F and so must be the identity.

Theorem 10: If F contains the number α and the n 'th roots of unity, $G(F[x^n = \alpha]/F)$ is abelian.

Proof: Let β be any n 'th root of α . Then the n 'th roots are $\beta, \beta\omega, \dots, \beta\omega^{n-1}$ where $\omega = e^{2\pi i/n}$. Thus $F[x^n = \alpha] = F[\beta]$. The rest of the proof is similar to theorem 9 and is left as an exercise.

§3.10. Solubility

Theorem 11: If $F = \mathbf{Q}[a_0, a_1, \dots, a_n]$ and $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ is soluble by radicals the $G(F[f(x) = 0]/F)$ is a soluble group.

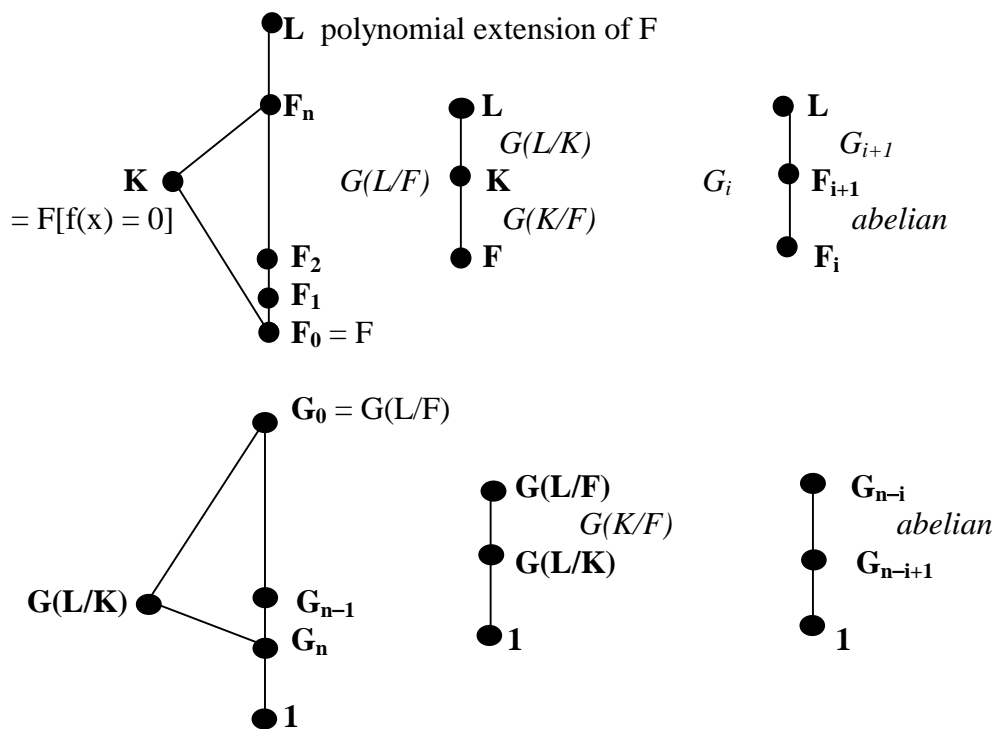
Proof: Suppose that $f(x)$ is soluble by radicals and that F is the extension of \mathbf{Q} by the coefficients. Then there is a sequence of fields $F_0 < F_1 < \dots < F_m$ such that:

- (1) $F_0 = F$;
- (2) each F_{i+1} is a radical extension of F_i ;
- (3) $F[f(x) = 0] \leq F_m$.

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). Another technical difficulty is that F_m might not be a polynomial extension of F . We need this to be able to use theorem 6. But we do know that F_m is a finite extension of F and therefore by theorem 7 it is contained in some polynomial extension L of F .

Let $K = F[f(x) = 0]$. Applying Theorem 6 to the chain $F \leq K \leq L$ we conclude that $G(K/F) \cong G(L/F)/G(L/K)$.

For each i , define $G_i = G(L/F_i)$. These form a chain $G_n \leq G_{n-1} \leq \dots \leq G_0$. Applying Theorem 6 to the chain $F_i \leq F_{i+1} \leq L$ 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 9 and 10 these quotients are all abelian. Hence $G_0^{(n)} \leq G_n$. Now $G_0 = G(L/F)$ and $G_n \leq G(L/K)$. Hence the n 'th derived subgroup of $G(K/F)$ is trivial and so this group is soluble.



§3.11. Permutations of the Roots of a Polynomial

In terms of our goal of proving that $3x^5 - 5x^3 + 1$ is not soluble by radicals we have proved that if it, then its Galois group must be soluble. The next stage is to show that its Galois group is isomorphic to S_5 . Since S_5 is not a soluble group we will have obtained our desired contradiction.

Theorem 12: If $f(x) \in F[x]$ and has n distinct zeros then its Galois group over F is isomorphic to a subgroup of S_n .

Proof: If X denotes the set of zeros of $f(x)$ then $\theta \rightarrow \theta | X$ is a homomorphism from $G(F[f(x) = 0])$ to a group of permutations on X (see Theorem 4). Its kernel is trivial by Theorem 8.

Theorem 13: $f(x) = 3x^5 - 5x^3 + 1$ has 3 real roots and 2 non-real roots.

Proof: $f'(x) = 15x^2(x^2 - 1)$. 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 less than -1 , one between 0 and 1, and one greater than 1). Thus there must be exactly two non-real zeros, forming a conjugate pair.

Fine, so we now know that the Galois group of $3x^5 - 5x^3 + 1$ over \mathbf{Q} is isomorphic to a subgroup of S_5 . What remains is to show that it is the whole of S_5 .

Theorem 14: If $f(x) \in F[x]$ is a prime polynomial over F with n distinct zeros the order of the Galois group is divisible by n .

Proof: Let $G = G(F[f(x) = 0]/F)$ and suppose that X is the set of n zeros of $f(x)$. G acts on X by the action $x * \theta = x^\theta$. By Theorems 1 and 2 any of these zeros can be mapped to any other by a suitable element of G so there is just one orbit of size n . Thus the index of the stabilizer of any root has index n in G and so n divides $|G|$.

In order to be able to apply the above theorem to $3x^5 - 5x^3 + 1$ we need to know that it is prime over \mathbf{Q} . There are a number of techniques for proving that a polynomial is prime over the rationals. The one we shall use is to consider the polynomial modulo a prime.

Theorem 15: $3x^5 - 5x^3 + 1$ is prime over \mathbf{Q} .

Proof: $3x^5 - 5x^3 + 1 \equiv x^5 + x^3 + 1 \pmod{2}$. Now $x^5 + x^3 + 1$ has no zeros in \mathbf{Z}_2 and so if it is not prime it must be the product of a prime quadratic and a prime cubic. However the only prime quadratic, modulo 2, is $x^2 + x + 1$ and the only prime cubics are $x^3 + x + 1$ and $x^3 + x^2 + 1$ and it is easy to check that $x^5 + x^3 + 1$ is neither of these products. Hence $x^5 + x^3 + 1$ is prime over \mathbf{Z}_2 and hence prime over \mathbf{Z} . By Gauss's Theorem it is prime over \mathbf{Q} .

We now apply Theorems 12, 14 to show that $G(\mathbf{Q}[3x^5 - 5x^3 + 1]/\mathbf{Q})$ is isomorphic to a subgroup of S_5 whose order is divisible by 5. That narrows things down a little. But we can do better by exploiting the conjugate pair of zeros.

Theorem 16: Let F be a subfield of \mathbf{R} and let $f(x) \in F[x]$ be a polynomial having exactly two non-real zeros α, β . Then $G(F[f(x) = 0])$ contains an automorphism which swaps α, β and fixes all the other zeros.

Proof: The conjugation automorphism, λ , is clearly an element of $G(\mathbf{C}/F)$. By Theorem 5 λ restricted to $F[f(x) = 0]$ is an element of $G(F[f(x) = 0]/F)$.

So this introduces a factor of 2 into the order of the Galois group of our polynomial $3x^5 - 5x^3 + 1$, showing that its order is divisible by 10. But there are still several soluble possibilities. For example S_5 has a subgroup of order 20 which is soluble. Might not the Galois group of $3x^5 - 5x^3 + 1$ be isomorphic to this? The answer is no, because the automorphism induced by complex conjugation is not just an element of order 2. It's a 2-cycle. This now seals the fate of $3x^5 - 5x^3 + 1$ and polynomials like it.

Theorem 17: A prime polynomial over \mathbf{Q} of prime degree p with exactly 2 non-real zeros and $p - 2$ real zeros has S_p as its Galois group over \mathbf{Q} .

Proof: The Galois group is isomorphic to a subgroup of S_p (by Theorem 12). Its order is divisible by p (by Theorem 14) and so by Cauchy's Theorem it has an element of order p , which must be a p -cycle. With the polynomial having exactly 2 non-real zeros this subgroup of S_p also contains a 2-cycle and so must be S_p itself.

Corollary: A prime polynomial of prime degree ≥ 5 is not soluble by radicals over \mathbf{Q} .

Proof: This follows from the theorem and the fact that S_p is not soluble for $p \geq 5$.

True or False Questions

- (1) $\mathbf{Q}[\sqrt{2}, \sqrt{3}] = \mathbf{Q}[\sqrt{6}]$.
- (2) $\mathbf{Q}[\sqrt{2}]$ is a polynomial extension of \mathbf{Q} .
- (3) Every polynomial extension is equivalent to a sequence of radical extensions.
- (4) If $G(\mathbf{Q}[f(x) = 0]/\mathbf{Q})$ is not soluble then $f(x)$ has no zeros in \mathbf{Q} .
- (5) The map $a + b\sqrt{2} \rightarrow a - b\sqrt{2}$ is an automorphism of $\mathbf{Q}[\sqrt{2}]$.
- (6) The Galois group of $\mathbf{Q}[x^5 = 1]$ over \mathbf{Q} is abelian.
- (7) The identity automorphism of \mathbf{Q} can be extended to an isomorphism $\theta: \mathbf{Q}[\sqrt{2}] \rightarrow \mathbf{Q}[\sqrt{3}]$ such that $(\sqrt{2})^\theta = \sqrt{3}$.
- (8) If $H \leq K \leq L$ then $G(L/K) \leq G(L/H)$.
- (9) The order of the Galois group of $\mathbf{Q}[x^3 = 3]$ over \mathbf{Q} is equal to 9.
- (10) The order of the Galois group of $\mathbf{Q}[x^5 = 1]$ over \mathbf{Q} divides 24.

Exercises

- (1) Show that $\mathbf{Q}[x^3 = 4] = \mathbf{Q}[2^{1/3}, \omega]$.
- (2) Show that $\mathbf{Q}[2^{1/3}, \omega]$ is not a radical extension of \mathbf{Q} .
- (3) Show that $\mathbf{Q}[2^{1/3}, \sqrt{3}, i]$ is a polynomial extension of \mathbf{Q} .
- (4) Find the order of the Galois group of $\mathbf{Q}[x^6 = 1]$ over \mathbf{Q} .
- (5) Show that the Galois group of $\mathbf{Q}[x^5 = 1]$ over \mathbf{Q} is isomorphic to C_4 .
- (6) Prove that the map $a + bi + c\sqrt{2} + di\sqrt{2} \rightarrow a - bi - c\sqrt{2} - di\sqrt{2}$ is an automorphism of $\mathbf{Q}[i, \sqrt{2}]$.
- (7) Show that $\mathbf{Q}[x^8 = 1] = \mathbf{Q}[i, \sqrt{2}]$.
- (8) Find the Galois group of $\mathbf{Q}[x^8 = 1]$ over \mathbf{Q} .
- (9) Find the order of the Galois group of $\mathbf{Q}[x^8 = 4]$ over \mathbf{Q} .
- (10) Show that $x^5 + 5x^2 - 1$ is not soluble by radicals over \mathbf{Q} .

Problems

- (1) Prove that for all rational numbers q , $\mathbf{Q}[e^{2\pi i q}]$ is a radical extension of \mathbf{Q} .
- (2) Prove that the identity map is the only automorphism of \mathbf{Q} .
- (3) Find $G(\mathbf{Q}[2^{1/3}]/\mathbf{Q})$.
- (4) Prove that if $\alpha, \beta \in K$, where K is a polynomial extension of H , then α, β have the same minimum polynomial over H if and only if $\alpha^\theta = \beta$ for some $\theta \in G(K/H)$.

(5) Prove that $G(\mathbf{Q}[x^n = 1]/\mathbf{Q}) \cong \mathbf{Z}^\#$, the group of units (elements with multiplicative inverses) of \mathbf{Z}_n . [You may assume that if $\text{GCD}(r, n) = 1$ then $e^{2\pi ri/n}$ and $e^{2\pi i/n}$ have the same minimum polynomial over \mathbf{Q} .

(6) Prove that if p is an odd prime and $\alpha \in \mathbf{Q}$ with no rational p 'th roots then $G(\mathbf{Q}[x^p = \alpha]/\mathbf{Q}[x^p = 1]) \cong C_p$ and that $G(\mathbf{Q}[x^p = \alpha]/\mathbf{Q})$ is a non-abelian group of order $p(p-1)$.

(7) Prove that if a, b, c are odd integers such that $ab > 0$ and $\frac{a^3 c^2}{b^5} < 0.003456$ then $ax^5 - bx^3 + c$ is not soluble by radicals over \mathbf{Q} .

(8) Prove that for every $n \geq 5$ there is a polynomial $f(x) \in \mathbf{Q}[x]$ of degree n which is not soluble by radicals.

(9) Prove that $G(\mathbf{Q}[x^4 = a]/\mathbf{Q})$ is given by the following table:

		GALOIS GROUP
$a = 0$		1
$a = r^4$ for $r > 0$	$r \in \mathbf{Q}$	C_2
	$r \notin \mathbf{Q}$ but $r^2 \in \mathbf{Q}$	V_4
	$r^2 \notin \mathbf{Q}$	D_8
$a = -r^4$	$r\sqrt{2} \in \mathbf{Q}$	C_2
	$r\sqrt{2} \notin \mathbf{Q}$ but $r^2 \in \mathbf{Q}$	V_4
	$r\sqrt{2} \notin \mathbf{Q}$ and $r^2 \notin \mathbf{Q}$	D_8

ANSWERS TO THE TRUE/FALSE QUESTIONS

(1) F ($\sqrt{2} \notin \mathbf{Q}[\sqrt{6}]$); (2) T ($\mathbf{Q}[\sqrt{2}] = \mathbf{Q}[x^2 = 2]$); (3) F ($\mathbf{Q}[3x^5 - 5x^3 + 1]$ can't be reached by a chain of radical extensions since it is not soluble by radicals); (4) F; (5) T; (6) T; (7) F (if $(\sqrt{2})^\theta = \sqrt{3}$ then $2^\theta = 3$); (8) T; (9) F (it's 6); (10) T (it's 4).

HINTS TO THE EXERCISES

- (1) To show that $\mathbf{Q}[\alpha, \beta] \leq \mathbf{Q}[\gamma, \delta]$ you must show that α, β can each be expressed in terms of γ, δ using only the four field operations.
- (2) Use Theorem 5 with $A = \mathbf{Q}, B = \mathbf{Q}[2^{1/3}\omega], C = \mathbf{C}$.
- (3) Find a rational polynomial which has $2^{1/3}, \sqrt{3}$ and i as its zeros and examine its other zeros.
- (4) Theorem 17 might help.
- (5) What are the possibilities for ω^θ ?
- (6) It's just a matter of churning through the necessary calculations. Or is there an easier way using automorphisms we already know about?
- (7) Just work out the zeros of $x^8 = 1$.
- (8) Exercise 6 gives you one and the identity is another. Now find two more.
- (9) You've got all the elements of $\mathbf{Q}[x^8 = 1]/\mathbf{Q}$ in exercise 8.
- (10) See theorems 13, 15 and 17.

HINTS TO THE PROBLEMS

- (1) Put $q = m/n$ where m, n are coprime. Show that $e^{2\pi i/n}$ is a power of $e^{2\pi i q}$.
- (2) If θ is an automorphism of \mathbf{Q} , first note that $1^\theta = 1$, then $(1 + 1)^\theta = 1^\theta + 1^\theta = 1 + 1$ etc or show that $\{q \in \mathbf{Q} \mid q^\theta = q\}$ is a subfield of \mathbf{Q} .
- (3) Every such automorphism fixes the rational numbers. What can it do with $2^{1/3}$ (within $\mathbf{Q}[2^{1/3}]$)?
- (4) Use Theorems 1, 2 for one direction. For the other, use the fact that $p(\alpha)^\theta = p^\theta(\alpha^\theta)$ for $p(x) \in \mathbf{H}[x]$.
- (5) Show that if $\theta \in G(\mathbf{Q}[x^n = 1]/\mathbf{Q})$ then $\omega^\theta = \omega^r$ for some $r \in \mathbf{Z}_n^\#$. Define $\Omega: G(\mathbf{Q}[x^n = 1]/\mathbf{Q}) \rightarrow \mathbf{Z}_n^\#$ by $\theta^\Omega = r$. Check that Ω is a homomorphism, that it has trivial kernel (see Theorem 8) and that it is onto (use Theorem 1 and the statement given at the end of the problem).
- (6) Examine the proof of Theorem 10 for some clues to the first part. use problem 4 for the second, and Theorem 6 will go part of the way to proving the third.
- (7) A mysterious problem isn't it? Note that $0.003456 = \frac{2^2 3^3}{5^5}$. You need to ensure that under these conditions, $ax^5 - bx^3 + c$ is prime over \mathbf{Q} and that it has 3 real zeros and 2 non-real ones. Theorem 17 takes care of the rest.
- (8) The polynomial need not be prime (it can be done in this case but it's much harder). Try a polynomial of the required degree which has an insoluble quintic as a factor.
- (9) No hints!

SOLUTION OF THE CUBIC

$ax^3 + bx^2 + cx + d$	$x^3 - 4x^2 + 4x - 3$
a	1
b	-4
c	4
d	-3
$S = -b/a$	4
$Q = c/a$	4
$P = -d/a$	3
$s = \Delta_1 + \Delta_2 = QS - 3P$	7
$(\Delta_1 - \Delta_2)^2 = Q^2S^2 - 27P^2 - 4PS^3 + 18SPQ - 4Q^3$	-147
$t = \Delta_1 - \Delta_2 = \text{square root}$	$7\sqrt{3}i$
$\Delta_1 = \frac{s+t}{2}$	$\frac{7(1+\sqrt{3}i)}{2} = -7\omega^2$
$\Delta_2 = \frac{s-t}{2}$	$\frac{7(1-\sqrt{3}i)}{2} = -7\omega$
$E^3 = S^3 - 3QS + 9P + 3\omega^2\Delta_1 + 3\omega\Delta_2$	64
$F^3 = S^3 - 3QS + 9P + 3\omega\Delta_1 + 3\omega^2\Delta_2$	1
S	4
E = cube roots of E^3	4 4ω $4\omega^2$
F = cube roots of F^3	1 ω^2 ω
$\alpha = \frac{S + E + F}{3}$	3 $\frac{1+\sqrt{3}i}{2}$ $\frac{1-\sqrt{3}i}{2}$