MAS 442 GALOIS THEORY
MAS 6310 ALGEBRA I

Notes by A. F. Jarvis, with some reworking by K. Mackenzie
and A. Weiss

These notes contain all the basic material of the course.

It is a good idea to create your own set of notes after each lecture, combining these printed notes with the notes you made during the lecture.

You can annotate this pdf, or print it out and write in the margins during lectures if you like — I have left a wide margin to make this easy.

The course web page is at

`http://ariel-weiss.postgrad.shef.ac.uk/teaching/galois-theory`

Any corrections to these notes will be posted there.

There are no documents for this course on MOLE.

Introduction

Given a polynomial, Galois theory associates a group to it, the properties of which reflect (some of) the properties of the polynomial. The Galois group is, in an algebraic sense, the symmetry group of the roots of the polynomial, and these symmetries act on the collection of roots. One can read off a lot of information about the polynomial from knowing how this symmetry group acts. Most importantly, the polynomial is soluble in terms of radicals (that is, using square roots, cube roots and higher roots) if and only if its Galois group is *soluble* in the sense of group theory (we'll define this later).

Linear polynomials are trivial, and the solution to quadratic polynomials was known to the ancient Babylonians. Cubics and quartics are harder; these were solved by del Ferro (c.1510) and Ferrari (c.1540) respectively. These formulae prompted a long search for general solutions in terms of radicals to equations of higher degree. Abel (1824) proved that there exist quintics not soluble by radicals (following an earlier flawed attempt by Ruffini (1799)), and very soon after, Galois (1831) gave a complete characterisation of all polynomials soluble by radicals, in terms of these symmetry groups.

Broadly, one starts with a polynomial f whose coefficients lie in a field K. So $f \in K[x]$. Let L be a larger field in which all the roots of f lie. Then $K \subseteq L$ is a field extension, and to any field extension we associate a group $\mathrm{Gal}(L/K)$, called the *Galois group* of the extension. It turns out that the group theory of $\mathrm{Gal}(L/K)$ reflects many of the properties of the original polynomial. For example, the Galois group of a quadratic polynomial will be trivial if the polynomial factors (as then $L = K$) and will be cyclic with 2 elements otherwise.

We begin by reviewing the solution of equations of small degree.

§ 1 Polynomials of degree $\leqslant 4$

We begin by solving equations of degrees up to 4. By dividing through by the leading coefficient, we may always assume that the equation is *monic*, that is, has leading coefficient 1:

$$x^d + a_1 x^{d-1} + \cdots + a_d = 0.$$

Throughout the course we suppose our polynomials defined over a subfield K of $\mathbb{C}$.

Degree 1

The trivial case; clearly

$$x + a = 0$$

has solution $x = -a$. Note that (of course!) we do not have to extend the field K to find a root, so the roots of the polynomial lie in an extension of degree 1 over K – i.e., in K itself.

Degree 2

This has also been known for thousands of years! By completing the square, we transform

$$x^2 + ax + b = 0$$

into

$$\left(x + \frac{a}{2}\right)^2 = \frac{a^2}{4} - b,$$

by adding $\frac{a^2}{4} - b$ to each side. Take square roots, to get

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

Then the solutions are given by

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

Note that in general, the roots are contained in an extension of degree 2 over K, obtained by adjoining the root of the discriminant $a^2 - 4b$ to K.

Degree 3

The case of cubic equations is a little harder; it was not until about 1510 that del Ferro (subsequently rediscovered by Tartaglia, and published by Cardano) showed how to solve this equation. Again we start by attempting to complete the cube, replacing the variable x by $x + \frac{a}{3}$. Then

$$x^3 + ax^2 + bx + c = 0$$

may be rewritten

$$\left(x + \frac{a}{3}\right)^3 + \left(b - \frac{a^2}{3}\right)\left(x + \frac{a}{3}\right) + \left(c - \frac{ab}{3} + \frac{2a^3}{27}\right) = 0.$$

(Exercise: verify this!) Write X for $x + \frac{a}{3}$, B for $b - \frac{a^2}{3}$ and C for $c - \frac{ab}{3} + \frac{2a^3}{27}$. Thus we need to solve

$$X^3 + BX + C = 0.$$

By trying to complete the cube, we can only eliminate the square term. Here's the clever idea: we write $X = u + v$. Expanding, this gives:

$$(u + v)^3 + B(u + v) + C = 0,$$

or

$$u^3 + v^3 + 3uv(u + v) + B(u + v) + C = 0.$$

We equate the terms involving $u + v$ and those without, and try to solve

$$\begin{aligned} u^3 + v^3 + C &= 0, \\ 3uv + B &= 0. \end{aligned}$$

Rewriting this gives:

$$\begin{aligned} u^3 + v^3 &= -C, \\ u^3 v^3 &= -\frac{B^3}{27}. \end{aligned}$$

It follows that u^3 and v^3 are solutions of the quadratic

$$y^2 + Cy - \frac{B^3}{27} = 0,$$

so u^3 and v^3 are

$$\frac{-C \pm \sqrt{C^2 + \frac{4B^3}{27}}}{2}.$$

Then u may be taken to be one of the three complex cube roots of

$$\frac{-C+\sqrt{C^2+\frac{4B^3}{27}}}{2}$$

and once you've chosen u, then the value of v is given from the equation

$$3uv+B=0.$$

More precisely, let u_0, u_1 and u_2 be the three cube roots of $\frac{-C+\sqrt{C^2+\frac{4B^3}{27}}}{2}$. Then define v_i by $3u_iv_i+B=0$. The three solutions to

$$X^3+BX+C=0$$

are given by u_0+v_0, u_1+v_1 and u_2+v_2. Note that if u_0 is one cube root, then the others are got by multiplying by cube roots of unity. Thus $u_1=\omega u_0$ and $u_2=\omega^2u_0$, where $\omega=e^{\frac{2\pi i}{3}}=\frac{-1+\sqrt{-3}}{2}$ and $\omega^2=e^{\frac{4\pi i}{3}}=\frac{-1-\sqrt{-3}}{2}$. But then we find that $v_1=-\frac{B}{3u_1}=-\frac{B}{3\omega u_0}=\frac{1}{\omega}\left(-\frac{B}{3u_0}\right)=\omega^2v_0$, and similarly $v_2=\omega v_0$. Recalling that $X=x+\frac{a}{3}$, we can recover the solutions to the original cubic equation.

Note that to write the roots, we first take a square root, of $C^2+\frac{4B^3}{27}$, to get a quadratic extension of K, and then take a cube root of something in this extension. Then the roots must lie in this extension, which is in general of degree 6 over K, since we've had to take a square root and then a cube root, to find a field in which to write the roots.

Example 1.1 Consider the following cubic.

$$x^3-3x-18=0.$$

Clearly $x=3$ is a solution, and is real. But applying Cardan's method gives

$$x=\sqrt[3]{9+\sqrt{80}}+\sqrt[3]{9-\sqrt{80}}.$$

If you attempt to simplify this, you will reach a point where you have to find the real solution of $x^3-3x-18=0$. You can check numerically that this is close to 3, but this is not a proof. The other roots are a pair of complex conjugates (find them!). ⊠

Compare this situation with the solution for quadratic equations: if a quadratic equation with real coefficients has real solutions then the formula gives real formulas for these solutions.

So the Cardano formula is of limited practical usefulness. However at least it shows that the cubic may be solved in terms of cube and square roots and the usual operations of arithmetic.

Degree 4

Another Italian mathematician, Ferrari, solved the general quartic around 1540, at about the same time as Tartaglia rediscovered del Ferro's solution to the cubic. Ferrari's original method is not so amenable to analysis by Galois theory, so we give an alternative.

Given a general quartic,

$$x^4 + ax^3 + bx^2 + cx + d = 0,$$

we first "complete the quartic", replacing x by $X = x + \frac{a}{4}$ to remove the term in x^3. We get a quartic

$$X^4 + pX^2 + qX + r = 0.$$

Let α_1, α_2, α_3 and α_4 denote the roots of this quartic in a larger field L. Note that

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0.$$

Write

$$\begin{aligned} \beta &= \alpha_1 + \alpha_2 \\ \gamma &= \alpha_1 + \alpha_3 \\ \delta &= \alpha_1 + \alpha_4 \end{aligned}$$

Then observe that

$$\begin{aligned} \alpha_1 &= (\beta + \gamma + \delta)/2, \\ \alpha_2 &= (\beta - \gamma - \delta)/2, \\ \alpha_3 &= (-\beta + \gamma - \delta)/2, \\ \alpha_4 &= (-\beta - \gamma + \delta)/2, \end{aligned}$$

so that the roots lie in $K(\beta, \gamma, \delta)$, i.e., if we know the values of β, γ and δ, we can get α_1, α_2, α_3 and α_4.

Further,

$$\beta^2 = (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$

and similarly $\gamma^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$ and $\delta^2 = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$. One computes easily that

$$\begin{aligned} \beta^2 + \gamma^2 + \delta^2 &= -2p \\ \beta^2\gamma^2 + \beta^2\delta^2 + \gamma^2\delta^2 &= p^2 - 4r \\ \beta\gamma\delta &= -q \end{aligned}$$

so that β^2, γ^2 and δ^2 are the three roots of

$$Y^3 + 2pY^2 + (p^2 - 4r)Y - q^2 = 0.$$

This cubic is known as the *resolvent cubic*.

We may now compute β and γ by choosing square roots of β^2 and γ^2; finally, $\delta = -\frac{q}{\beta\gamma}$, and then we can recover the roots α_i.

So here is the full algorithm to solve the quartic.

1. Change x into $X = x + \frac{a}{4}$ to get rid of the term in x^3; we get a quartic of the form
$$X^4 + pX^2 + qX + r = 0.$$
2. Form the resolvent cubic
$$Y^3 + 2pY^2 + (p^2 - 4r)Y - q^2 = 0.$$
3. Solve the resolvent cubic – the roots are β^2, γ^2 and δ^2.
4. Take square roots of β^2 and γ^2 to get the values of β and γ, and read off the value of δ from the equation $\beta\gamma\delta = -q$.
5. Recover the values of α_1, α_2, α_3 and α_4 given the values of β, γ and δ.

You can see from the algorithm that to write down the formula for the roots, in terms of the coefficients (like the quadratic formula) would be far too difficult and would probably take several pages! But note that the method requires us to take a cube root and a square root in order to solve the resolvent cubic, and two further square roots in step (4), making one cube root and three square roots in total. This means that the solutions lie in a field extension of degree $3 \times 2^3 = 24$.

It looks as if the roots of an equation of degree n are going to lie in some field extension of degree $n!$. So a quintic equation should have its roots lying in some extension of degree 120. If we are going to find some formula to solve the quintic, we would need to take a fifth root, a cube root and three square roots. We will prove the first remark here fairly soon. However, we are going to prove that there is no formula to solve the quintic.

The main idea

How are we going to prove this result? The main idea is to use the notion of a *Galois group* of a field extension. In a sense which we will explain later, it will be a symmetry group of the extension.

Now suppose we have some polynomial whose roots can be expressed in terms of square, cube and higher roots. For example, a root might be
$$\alpha = \sqrt[7]{11 - 3\sqrt[3]{5 + 2\sqrt[5]{2}}}.$$

Then α lies in the field $\mathbb{Q}(\alpha)$. We can build up this field successively, first by adjoining $\sqrt[5]{2}$ to $\mathbb{Q}$ to get the field $\mathbb{Q}(\sqrt[5]{2})$. Then this field contains $5+2\sqrt[5]{2}$, and we can adjoin its cube root to get the next field $\mathbb{Q}(\sqrt[3]{5+2\sqrt[5]{2}})$. Finally, this field contains $11-3\sqrt[3]{5+2\sqrt[5]{2}}$, and we can adjoin its 7th root to get the field $\mathbb{Q}(\alpha)$. We have thus obtained a sequence of fields

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[5]{2}\right) \subseteq \mathbb{Q}\left(\sqrt[3]{5+2\sqrt[5]{2}}\right) \subseteq \mathbb{Q}\left(\sqrt[7]{11-3\sqrt[3]{5+2\sqrt[5]{2}}}\right) = \mathbb{Q}(\alpha)$$

in which each field is obtained from the one before by adjoining a root of something.

The idea of Galois theory is to each field extension, we can associate a group, called the Galois group, and its properties will reflect the properties of the extension. Given a sequence of extensions as above, in which at each step we adjoin a root, we get a corresponding sequence of Galois groups. This means that the Galois group of the whole extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ can be broken up into smaller chunks corresponding to each of the steps in the extension. This means that if a polynomial is soluble by radicals (i.e., we can express its roots using square, cube and higher roots), then its roots lie in some extension whose Galois group has a particular form. We will end the course by showing that the Galois group of a quintic need not have this special form, and therefore the roots of a quintic need not be expressible in radicals.

As you can see, the theory is going to mix some easy theory of equations, with some field theory and some group theory.

§ 2 Fields

In this course, all fields will be subfields of $\mathbb{C}$. In particular, every field will contain $\mathbb{Q}$, and will therefore be infinite. This is not really necessary, but it leads to an easier presentation for many of the results. In any case, we are mostly going to be interested in solving polynomials with coefficients in $\mathbb{Z}$ (so certainly in $\mathbb{Q}$), and not in more general situations.

Basic material on field extensions

The Galois group of a polynomial consists of "symmetries of field extensions". In this section, we will give some (mostly) elementary results that we will need for our study. Some were in MAS 333/438, and these are the ones we will begin with.

Definition 2.1 Let K be a field. A *field extension* $K \subseteq L$, or L/K, is a field L that contains K.

It follows that L may be thought of as a K-vector space. An extension L/K is said to be *finite* if L is finite dimensional as a K-vector space. In this case, the *degree* $[L : K]$ of the extension L/K is defined to be the dimension of L as a K-vector space. ▲

Then we have the following results:

Theorem 2.2 *Suppose α is algebraic over the field K (i.e., satisfies a polynomial with coefficients in K). Then the degree $[K(\alpha) : K]$ is equal to the degree of the minimal polynomial of α over K.*

If this degree is n, recall that this follows from the observation that every element of $K(\alpha)$ can be written as a polynomial $a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_0$, and so $\{1, \alpha, \ldots, \alpha^{n-1}\}$ form a basis of $K(\alpha)$ over K.

Theorem 2.3 (Degrees) *Suppose $K \subseteq M \subseteq L$ are field extensions. Then*

$$[L : K] = [L : M][M : K].$$

It will be rather convenient at a couple of points in the course to know that every finite extension of fields can be generated by a single element. Before we prove this, here's an example from MAS 333/438:

Example 2.4 The field $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. For this, it suffices to verify that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. From MAS 333/438, we only have to check that $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (which is obvious) and that $\sqrt{2}$, $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Write α for $\sqrt{2} + \sqrt{3}$. Then

$$\alpha^3 = 11\sqrt{2} + 9\sqrt{3},$$

so that $\sqrt{2} = \frac{\alpha^3 - 9\alpha}{2}$. Thus $\sqrt{2} \in \mathbb{Q}(\alpha)$, and also $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$. ⊠

The theorem mentioned above, known as the 'Theorem of the Primitive Element' was covered in MAS 333/438. We will abbreviate this theorem to TPE. The proof is quite intricate so we give it here.

Recall that $\mathbb{C}$ is *algebraically closed*, so that every polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$. It follows inductively that a polynomial of degree n defined over $\mathbb{C}$ has n roots in $\mathbb{C}$.

Theorem 2.5 (Theorem of the Primitive Element) *Suppose $K \subseteq L$ is a finite extension of fields, and that $K, L \subseteq \mathbb{C}$. Then $L = K(\gamma)$ for some element $\gamma \in L$.*

PROOF. Suppose L is generated over K by m elements. We'll first treat the case $m = 2$. So suppose $L = K(\alpha, \beta)$, and let f and g denote the minimal polynomials of α and β over K. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ be the roots of f in $\mathbb{C}$, and let $\beta_1 = \beta, \beta_2, \ldots, \beta_t$ be the roots of g. Irreducible polynomials always have distinct roots. Thus $X = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$ is the only solution (if $j \neq 1$) to

$$\alpha_i + X\beta_j = \alpha_1 + X\beta_1.$$

Choosing a $c \in K$ different from each of these X's, then each $\alpha_i + c\beta_j$ is different from $\alpha + c\beta$. We claim that $\gamma = \alpha + c\beta$ generates L over K. Certainly $\gamma \in K(\alpha, \beta) = L$. Recall from MAS 333/438 that it suffices to verify that $\alpha, \beta \in K(\gamma)$.

The polynomials $g(x)$ and $f(\gamma - cx)$ both have coefficients in $K(\gamma)$, and have β as a root. The other roots of $g(x)$ are $\beta_2, \ldots, \beta_t$, and, as $\gamma - c\beta_j$ is not any α_i, unless $i = j = 1$, β is the only common root of $g(x)$ and $f(\gamma - cx)$. Thus, $(x - \beta)$ is the highest common factor of $g(x)$ and $f(\gamma - cx)$. But the highest common factor is a polynomial defined over any field containing the coefficients of the original two polynomials (think about how the Euclidean algorithm works for polynomials). In particular, it follows that $x - \beta$ has coefficients in $K(\gamma)$, so that $\beta \in K(\gamma)$. Then $\alpha = \gamma - c\beta \in K(\gamma)$. The result follows for $m = 2$.

More generally, if $L = K(\alpha_1, \ldots, \alpha_m)$, we can view this as $K(\alpha_1, \ldots, \alpha_{m-2})(\alpha_{m-1}, \alpha_m)$, and the case $m = 2$ allows us to write this as $K(\alpha_1, \ldots, \alpha_{m-2})(\gamma_{m-1})$. Again we can rewrite this as $K(\alpha_1, \ldots, \alpha_{m-3})(\alpha_{m-2}, \gamma_{m-1})$, and use the case $m = 2$ to reduce the number further still. Continuing in this way, we eventually get down to just one element. ⊠

So every field extension $K \subseteq L$ can be generated by a single element γ.

Splitting fields

The splitting field of a polynomial $f \in K[x]$ is basically just the smallest field extension of K containing all the roots of f. Such fields always exist, and are of finite degree over K.

Definition 2.6 Let $f \in K[x]$. A field L containing K is said to *split* f if f factors in $L[x]$ into linear factors, $c\prod(x-\alpha_i)$, with $\alpha_i \in L$. If L is generated by the α_i over K, then L is said to be a *splitting field* for f over K. ▲

Note that this last sentence simply says that if f is a polynomial over K, then its splitting field is got by adjoining to K all of its roots. Let $\alpha_1, \ldots, \alpha_n$ denote the roots of f in $\mathbb{C}$, where $n = \deg f$. Then form the field $L = K(\alpha_1, \ldots, \alpha_n)$; clearly L splits f and L is generated over K by the roots of f, so L is the splitting field of f over K.

Examples 2.7

1. Suppose $f(x) = x^2 + 1$ over $\mathbb{R}$. Then the roots of f in $\mathbb{C}$ are $\pm i$, so that the splitting field of f over $\mathbb{R}$ is $\mathbb{R}(i, -i) = \mathbb{C}$.

2. Suppose $f(x) = x^2 + 1$ over $\mathbb{Q}$. Then the roots of f in $\mathbb{C}$ are $\pm i$, so that the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(i)$.

3. Suppose $f(x) = x^3 - 1$ over $\mathbb{Q}$. Then f factors as $(x-1)(x^2+x+1)$, and the roots are 1, ω and ω^2, where $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$. Thus the splitting field is $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$.

4. Suppose $f(x) = x^3 - 2$ over $\mathbb{Q}$. Then the roots of f in $\mathbb{C}$ are $\alpha, \omega\alpha, \omega^2\alpha$, where $\alpha = \sqrt[3]{2}$ is the positive real cube root of 2, and $\omega = e^{\frac{2\pi i}{3}}$ as before. Then the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2) = \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

Lemma 2.8 Suppose that $f \in K[x]$ is a polynomial of degree n. If L denotes a splitting field for f, then $[L : K] \leqslant n!$.

PROOF. L may be obtained by successively adjoining roots of f. Suppose that the roots are $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then $[K(\alpha_1) : K] \leqslant n$, by Theorem 2.2 (as α_1 is a root of f, its minimal polynomial must divide f, so be of degree at most that of f). The remaining roots $\alpha_2, \ldots, \alpha_n$ are roots of the polynomial $f(x)/(x-\alpha_1)$, of degree $n-1$ and defined over $K(\alpha_1)$. Thus adjoining α_2 gives a field extension with $[K(\alpha_1, \alpha_2) : K(\alpha_1)] \leqslant n-1$. Now the root α_3 is a root of $f(x)/(x-\alpha_1)(x-\alpha_2)$, a polynomial of degree $n-2$ over $K(\alpha_1, \alpha_2)$. Continuing in this way, we see that

$$\begin{aligned}
[L : K] &= [K(\alpha_1, \ldots, \alpha_n) : K] \\
&= [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] \ldots [K(\alpha_1) : K] \\
&\leqslant 1.2 \ldots n = n!
\end{aligned}$$

using the Degrees Theorem 2.3. ⊠

You might have expected to get $[L : K] \leqslant n$, not $n!$, in the above lemma. Sometimes this will be true, but usually it will not. Here is an example.

Example 2.9 Consider the polynomial $x^3 - 2$ over $\mathbb{Q}$. Let's carry out the procedure in the proof above. We start by finding a root: let's take $\alpha = \sqrt[3]{2}$ to be the real cube root of 2. Then

$$x^3 - 2 = (x - \alpha)(x^2 + x\alpha + \alpha^2)$$

is a factorisation into irreducible polynomials over $\mathbb{Q}(\alpha)$; note that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ as $x^3 - 2$ is the minimal polynomial of α over $\mathbb{Q}$. So

$$\frac{x^3 - 2}{x - \alpha} = x^2 + x\alpha + \alpha^2.$$

Clearly this is irreducible over $\mathbb{Q}(\alpha)$ – its roots are $\omega\alpha$ and $\omega^2\alpha$ (where as before $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$) which are not real, so cannot lie in $\mathbb{Q}(\alpha)$. To get the splitting field, we need also to factor $x^2 + x\alpha + \alpha^2 = (x - \alpha\omega)(x - \alpha\omega^2)$, and to adjoin a root, $\alpha\omega$ say, to $\mathbb{Q}(\alpha)$. Then the splitting field is $\mathbb{Q}(\alpha, \omega)$, and

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2.3 = 6.$$

⊠

§ 3 Field extensions and automorphisms

Now that we have defined field extensions, we have to study their "symmetries". Recall (from MAS 220 or 346, for example) that geometrical figures, such as polygons, cubes and so on, have groups of symmetries consisting of reflections and rotations and so on, which act on the points of the figure. In this section we will define similar ideas for field extensions; if L/K is a field extension, we will associate to it a group, called the Galois group, whose elements act on the elements of L, fixing every element in the bottom field K.

Automorphisms of field extensions

Our first task will be to define the notion of an automorphism of a field extension.

Definition 3.1 Let L/K be a field extension. Then a *K-automorphism of L* is a map $\varphi : L \longrightarrow L$ which fixes every element of K and satisfies the following rules:

1. if ℓ_1 and ℓ_2 are in L, then
$$\varphi(\ell_1 + \ell_2) = \varphi(\ell_1) + \varphi(\ell_2),$$
that is, φ is an additive homomorphism from L to itself.
2. if ℓ_1 and ℓ_2 are in L, then
$$\varphi(\ell_1\ell_2) = \varphi(\ell_1)\varphi(\ell_2),$$
that is, φ is a multiplicative homomorphism from L to itself.
3. φ is a bijection, so it is both injective (1-1) and surjective (onto).
4. if $\ell \in K$, then $\varphi(\ell) = \ell$.

▲

These K-automorphisms of L are the "symmetries" of the field extension L/K.

Remark 3.2 Remember that a homomorphism $\theta : L \longrightarrow M$ of fields is always injective. To see this, suppose that a non-zero element $a \in L$ is mapped to 0_M, then every element is mapped to 0_M, because each element $\ell \in L$ is a multiple of a, namely $(\ell a^{-1})a$. But $\theta(1_L) = 1_M$, so $1_L \notin \ker\theta$. Thus the kernel cannot contain non-zero elements, so must be $\{0_L\}$. Thus θ is injective.

It follows that in the third condition of Definition 3.1, we only need to check that φ is surjective, as injectivity is automatically satisfied.

However, homomorphisms of fields need not be surjective; for example, any inclusion of fields, such as $\mathbb{R} \hookrightarrow \mathbb{C}$, is a homomorphism which is not surjective.

Examples 3.3 1. Suppose $L = K$. Then the only K-automorphism of L is the identity map, because such a map must fix every element of $K = L$.

2. The identity map on L is always a K-automorphism of L for any subfield K of L.

3. Suppose $L = \mathbb{C}$, $K = \mathbb{R}$. Then there are exactly two possible K-automorphisms of L, namely

$$\begin{array}{rccc} \mathrm{id} : \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \mapsto & z \end{array}$$

and

$$\begin{array}{rccc} \mathrm{conj} : \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \mapsto & \overline{z} \end{array}$$

To see this, note that any $\mathbb{R}$-automorphism of $\mathbb{C}$ must fix every real number. Then if a and b are real, the axioms imply that

$$\varphi(a + ib) = \varphi(a) + \varphi(i)\varphi(b) = a + \varphi(i)b,$$

so that φ is determined by its effect on i. But also,

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$$

as -1 is real. So $\varphi(i)$ must be a square root of -1, and must therefore be $\pm i$. If $\varphi(i) = i$, then φ is the identity map, whereas, if $\varphi(i) = -i$, it is complex conjugation. (Exercise: check that both of these are indeed $\mathbb{R}$-automorphisms of $\mathbb{C}$.)

4. Following the last example, show that if $L = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}$, then there are precisely two K-automorphisms of L, namely

$$\begin{array}{rccc} \varphi_1 = \mathrm{id} : \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} & \mapsto & a + b\sqrt{2} \end{array}$$

and

$$\begin{array}{rccc} \varphi_2 : \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} & \mapsto & a - b\sqrt{2} \end{array}$$

5. If $L = \mathbb{Q}(\sqrt[3]{2})$ and $K = \mathbb{Q}$, then the only K-automorphism of L is the identity. For this, we use a similar method as above to see that if θ is an automorphism, then $\theta(\sqrt[3]{2})$ must again be a cube root of 2 contained in L. But there is only one cube root of 2 contained in L, namely $\sqrt[3]{2}$ itself; the other roots are complex, whereas $L \subset \mathbb{R}$. It follows that not only does θ fix $\mathbb{Q}$, but it also fixes $\sqrt[3]{2}$, and so it fixes all of L.

6. If $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}$, then, as above, a K-automorphism maps $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$. This gives four K-automorphisms of L.

Galois groups of field extensions

Now we come to the central definition of the course.

Definition 3.4 Let $K \subseteq L$ be a field extension. The *Galois group* of L over K is the group of all K-automorphisms of L, and is denoted $\mathrm{Gal}(L/K)$. ▲

Given θ and φ in $\mathrm{Gal}(L/K)$, and $a \in L$, define

$$(\theta\varphi)(a) = \theta(\varphi(a)).$$

That is, the multiplication of elements of the Galois group is composition of maps. Remember, for $\theta\varphi$ one applies φ first, and then applies θ to the result.

Proposition 3.5 Let $K \subseteq L$ be a field extension. Then $\mathrm{Gal}(L/K)$ is a group under composition of maps.

PROOF. The set of bijections $L \longrightarrow L$ forms a group, and so we can use the subgroup criterion. This is easy and left as an exercise. One has to check, for example, that if θ and φ are both K-automorphisms of L, then so is $\theta\varphi$, which means that we must verify all the conditions of Definition 3.1, all of which are easy:

$$(\theta\varphi)(\ell_1)+(\theta\varphi)(\ell_2) = \theta(\varphi(\ell_1))+\theta(\varphi(\ell_2)) = \theta(\varphi(\ell_1)+\varphi(\ell_2)) = \theta(\varphi(\ell_1+\ell_2)) = (\theta\varphi)(\ell_1+\ell_2).$$

The other conditions are just as easy. ⊠

Example 3.6 Suppose $K = \mathbb{R}$, and $L = \mathbb{C}$. We have already seen that the only two $\mathbb{R}$-automorphisms of $\mathbb{C}$ are the identity and complex conjugation. It follows that $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is a group with 2 elements, hence is cyclic, generated by the complex conjugation (and indeed, conjugating a complex number twice returns you to the original number). ⊠

Example 3.7 In the same way, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2$, the generator being the conjugation map $\mathrm{conj} : a + b\sqrt{2} \mapsto a - b\sqrt{2}$. ⊠

Example 3.8 Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. Then, as we have already seen, $\mathrm{Gal}(L/K)$ is trivial (i.e., just has the identity automorphism of L), as there are no non-trivial K-automorphisms of L. ⊠

Now we prove an important result explaining how roots of polynomials behave under these symmetries.

Lemma 3.9 Suppose $K \subseteq L$ is a field extension, and that $\alpha \in L$ satisfies a polynomial equation $f(x) = 0$, where f has coefficients in K. If θ is a K-automorphism of L, then $\theta(\alpha)$ is also a root of f.

PROOF. Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. If α is a root of f, then $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Applying θ,

$$\theta(a_n)\theta(\alpha)^n + \theta(a_{n-1})\theta(\alpha)^{n-1} + \cdots + \theta(a_0) = \theta(0) = 0,$$

as θ is an automorphism. Then as θ fixes every element of K, we see that

$$0 = a_n\theta(\alpha)^n + a_{n-1}\theta(\alpha)^{n-1} + \cdots + a_0,$$

so that $\theta(\alpha)$ is also a root of f. ⊠

We will refer to the following special case as 'APR' ('**A**utomorphisms **P**ermute **R**oots').

Theorem 3.10 (APR) *Let $K \subseteq L$ be a field extension, and let $\alpha \in L$ be algebraic over K with minimal polynomial $f \in K[x]$ over K. If $\theta \in \mathrm{Gal}(L/K)$, then $\theta(\alpha)$ is also a root of f.*

Let's restate the above result:

> a K-automorphism of L maps any element of L to another element with the same minimal polynomial over K.

We have already seen lots of examples of this. For example, if $L = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}$, then the two automorphisms map $\sqrt{2}$ to $\pm\sqrt{2}$, which are the two roots of the minimal polynomial $x^2 - 2$ of $\sqrt{2}$ over $\mathbb{Q}$. This shows that there can't be too many K-automorphisms of L when L/K is a field extension, as each element of L can only be mapped to a finite number of elements of L. If L/K is finite, so generated by a single element, $L = K(\gamma)$, say, then every automorphism is then completely determined by its effect on γ, and so there are only a finite number of K-automorphisms of L.

We'll now prove a bound for the size of the Galois group. For this, we'll begin by proving a fairly general result (which we will also need in §5), and then state a special case from which we can deduce our bound.

Remember that a field homomorphism $\varphi : K_1 \longrightarrow K_2$ is a map satisfying

$$\begin{gathered}\varphi(k + k') = \varphi(k) + \varphi(k') \text{ for all } k, k' \in K_1;\\ \varphi(kk') = \varphi(k)\varphi(k') \text{ for all } k, k' \in K_1;\\ \varphi(1) = 1.\end{gathered}$$

Theorem 3.11 *Let α be algebraic over K with minimal polynomial $f \in K[x]$, and consider the extension $K \subseteq K(\alpha)$. Let $K \subseteq L$. Then there is a bijection between the set of homomorphisms $\theta : K(\alpha) \longrightarrow L$ that fix elements of K and the set of distinct roots of $f(x)$ in L.*

PROOF. Write

$$H = \{\text{homomorphisms } \theta : K(\alpha) \longrightarrow L \text{ that fix elements of } K\}$$

and

$$R = \{\text{distinct roots of } f(x) \text{ in } L\}.$$

We define a map $R \to H$. Take $\beta \in R$. We will define a homomorphism $\theta_\beta \colon K(\alpha) \to L$.

Remember that the elements of $K(\alpha)$ are all $\sum_{i=0}^{n} a_i \alpha^i$ where n is the degree of f and $a_i \in K$.

Define

$$\theta_\beta : K(\alpha) \longrightarrow L, \qquad \sum_{i=0}^{n} a_i \alpha^i \mapsto \sum_{i=0}^{n} a_i \beta^i.$$

This clearly fixes every element of K. It is an easy exercise to see that θ_β is a homomorphism. (Note that if β is not a root of f, then $\theta_\beta(f(\alpha)) = f(\beta)$, so that $\theta_\beta(0) \neq 0$, so the map is not a homomorphism.)

Conversely, given a homomorphism $\theta : K(\alpha) \longrightarrow L$, we must have

$$\theta\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} \theta(a_i)\theta(\alpha)^i = \sum_{i=0}^{n} a_i \theta(\alpha)^i.$$

Write $f(x) = \sum_{i=0}^{n} c_i x^i$. Then $\sum_{i=0}^{n} c_i \alpha^i = 0$. Applying θ, we have that

$$\sum_{i=0}^{n} c_i \theta(\alpha)^i = 0,$$

so $\theta(\alpha)$ is a root of $f(x)$.

Finally, it is an easy exercise to check that the maps $\beta \mapsto \theta_\beta$ and $\theta \mapsto \theta(\alpha)$ are mutually inverse. ⊠

Corollary 3.12 Let α be algebraic over K. Then $|\mathrm{Gal}(K(\alpha)/K)|$ is equal to the number of distinct roots of the minimal polynomial m_α of α over K in $K(\alpha)$.

If β is such a root, the corresponding automorphism maps α to β.

PROOF. This is just a special case of Theorem 3.11, when $L = K(\alpha)$, except that Theorem 3.11 uses homomorphisms, while the Galois group consists of automorphisms. We have to check that homomorphisms from $K(\alpha)$ to itself are necessarily bijections. But we have already explained in Remark 3.2 that homomorphisms are necessarily injective. However, we can regard a homomorphism as a linear map of vector spaces over K. Since the kernel is trivial, the rank-nullity theorem shows that the dimension of the image is equal to the dimension of $K(\alpha)$; since the image is contained in $K(\alpha)$, they must be equal, and so homomorphisms are necessrily also surjective. ⊠

Immediately we get a bound on the size of the Galois group:

Corollary 3.13 Let $K \subseteq L$ be a finite extension of fields. Then

$$|\mathrm{Gal}(L/K)| \leqslant [L : K].$$

PROOF. By TPE (Theorem 2.5), we may assume $L = K(\alpha)$ for some $\alpha \in L$. Let $f \in K[x]$ denote the minimal polynomial of α over K. Then the degree of f is $[L : K]$, using Theorem 2.2.

But $|\mathrm{Gal}(K(\alpha)/K)|$ is the number of roots of f in $K(\alpha)$, and this is bounded by the degree of f, which is $[L : K]$, as already remarked. ⊠

Next, we need to consider the case of splitting field extensions and in particular the action of the Galois group on the roots of the polynomial.

Example 3.14 We compute the Galois group of the extension L/K where $K = \mathbb{Q}$ again, and where L is the splitting field of $x^3 - 2$, namely $L = \mathbb{Q}(\alpha, \omega)$, where $\alpha = \sqrt[3]{2}$ and $\omega = e^{\frac{2\pi i}{3}}$. An automorphism θ of $\mathrm{Gal}(L/K)$ must send $\sqrt[3]{2}$ to another cube root of 2 in L, i.e., $\omega^i\alpha$ for $i = 0$, 1 or 2, and also must send ω to another root of $x^2 + x + 1$, so either fixes ω or sends it to its conjugate, $\overline{\omega} = \omega^2$. There are therefore six K-automorphisms of L, given by

$$\begin{aligned}
\alpha &\mapsto \alpha, \quad \omega \mapsto \omega \\
\alpha &\mapsto \alpha, \quad \omega \mapsto \omega^2 \\
\alpha &\mapsto \omega\alpha, \quad \omega \mapsto \omega \\
\alpha &\mapsto \omega\alpha, \quad \omega \mapsto \omega^2 \\
\alpha &\mapsto \omega^2\alpha, \quad \omega \mapsto \omega \\
\alpha &\mapsto \omega^2\alpha, \quad \omega \mapsto \omega^2
\end{aligned}$$

Note that if φ and ψ denote the second and third of these automorphisms, then the automorphisms are id, φ, ψ, $\psi\varphi$, ψ^2 and $\varphi\psi$ respectively. It follows that the Galois group is generated by φ and ψ of order 2 and 3 respectively, and one easily verifies that $\varphi\psi\varphi = \psi^{-1}$, so that the group is isomorphic to D_3, the dihedral group with 6 elements. One can also view D_3 as S_3, as D_3 is the group of symmetries of a triangle, and each symmetry gives a permutation of the three vertices.

The roots of $x^3 - 2$ are given by $\alpha_1 = \alpha$, $\alpha_2 = \omega\alpha$ and $\alpha_3 = \omega^2\alpha$. Let's work out how these automorphisms act on the roots of the equation. For example, consider the automorphism which sends $\alpha \mapsto \omega\alpha$ and $\omega \mapsto \omega^2$. Then this sends $\alpha_1 = \alpha$ to $\omega\alpha = \alpha_2$, $\alpha_2 = \omega\alpha$ to $\omega^2.\omega\alpha = \alpha = \alpha_1$, and $\alpha_3 = \omega^2\alpha$ to $(\omega^2)^2.\omega\alpha = \omega^2\alpha = \alpha_3$. Thus it exchanges the first two roots, and we regard it as the permutation $(1\ 2)$ in S_3. With this notation, we see that the six permutations correspond to the elements

$$\mathrm{id}, \quad (2\ 3), \quad (1\ 2\ 3), \quad (1\ 2), \quad (1\ 3\ 2), \quad (1\ 3)$$

in S_3 respectively. This proves that the Galois group $\mathrm{Gal}(L/K)$ is equal to S_3. ⊠

Example 3.15 Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let φ be a K-automorphism of L. Since $(\sqrt{2})^2 = 2$, we see that $\varphi(\sqrt{2})^2 = \varphi(2) = 2$, so that $\varphi(\sqrt{2}) = \pm\sqrt{2}$, and similarly, $\varphi(\sqrt{3}) = \pm\sqrt{3}$. There are thus 4 K-automorphisms of L, induced by:

$$\begin{aligned}
\sqrt{2} &\mapsto \sqrt{2}, & \sqrt{3} &\mapsto \sqrt{3} \qquad \text{(the identity)}\\
\sqrt{2} &\mapsto \sqrt{2}, & \sqrt{3} &\mapsto -\sqrt{3}\\
\sqrt{2} &\mapsto -\sqrt{2}, & \sqrt{3} &\mapsto \sqrt{3}\\
\sqrt{2} &\mapsto -\sqrt{2}, & \sqrt{3} &\mapsto -\sqrt{3}
\end{aligned}$$

Let's first regard L as the splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$. If the roots are $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$, then the four automorphisms permute the α_i as id, $(3\ 4)$, $(1\ 2)$, $(1\ 2)(3\ 4)$ respectively. This shows that the Galois group has four elements and looks like the subgroup of S_4 isomorphic to $C_2 \times C_2$ generated by two disjoint transpositions.

But we can also regard $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. The minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is $x^4 - 10x^2 + 1$ (exercise), whose four roots are given by

$$\beta_1 = \sqrt{2} + \sqrt{3}, \quad \beta_2 = \sqrt{2} - \sqrt{3}, \quad \beta_3 = -\sqrt{2} + \sqrt{3}, \quad \beta_4 = -\sqrt{2} - \sqrt{3}.$$

Then the four K-automorphisms of L are given by

$$\begin{array}{llll}
\beta_1 \mapsto \beta_1, & \beta_2 \mapsto \beta_2, & \beta_3 \mapsto \beta_3, & \beta_4 \mapsto \beta_4\\
\beta_1 \mapsto \beta_2, & \beta_2 \mapsto \beta_1, & \beta_3 \mapsto \beta_4, & \beta_4 \mapsto \beta_3\\
\beta_1 \mapsto \beta_3, & \beta_2 \mapsto \beta_4, & \beta_3 \mapsto \beta_1, & \beta_4 \mapsto \beta_2\\
\beta_1 \mapsto \beta_4, & \beta_2 \mapsto \beta_3, & \beta_3 \mapsto \beta_2, & \beta_4 \mapsto \beta_1
\end{array}$$

Here, the four automorphisms act by the following permutations: id, $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$, which is the well-known Klein 4-subgroup V_4 of S_4. Note that it is also isomorphic to $C_2 \times C_2$, generated by two elements of order 2, although the actual permutations involved look different.

So the Galois group is isomorphic to $C_2 \times C_2$, but, depending on how we regard L as a splitting field, we can realise this group in different ways as subgroups of S_4. ⊠

These examples indicate how we can regard the K-automorphisms of L, in the case where L is a splitting field of some polynomial over K, as being permutations of the roots of the polynomial. Let's record this formally.

Lemma 3.16 Suppose L is the splitting field of a polynomial f of degree n over K. List the roots of f in L as $\{\alpha_1, \ldots, \alpha_n\}$. Then the action of $\mathrm{Gal}(L/K)$ on the roots gives an injective homomorphism of groups

$$\mathrm{Gal}(L/K) \longrightarrow S_n,$$

where S_n is the group of permutations of n objects.

Here, $\varphi \in \mathrm{Gal}(L/K)$ gives us a permutation σ in S_n if φ acts on $\{\alpha_1, \ldots, \alpha_n\}$ by the permutation σ, i.e., if $\varphi(\alpha_i) = \alpha_{\sigma(i)}$.

PROOF. $L = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f in L. We can look at the action $\varphi \in \mathrm{Gal}(L/K)$ on the roots of f. By APR (Theorem 3.10), $\varphi(\alpha_i)$ is also a root of f, so is one of $\{\alpha_1, \ldots, \alpha_n\}$. As φ is injective, φ is a permutation of the set of α_i. In this way, we obtain a homomorphism $\mathrm{Gal}(L/K) \longrightarrow S_n$. It is injective – if θ lies in the kernel, then θ is mapped to the trivial permutation, so that it sends each α_i to itself, as well as fixing K, so it therefore fixes all of L. ⊠

§ 4 Example: Cyclotomic polynomials, roots of unity

This section is not completely central to our goal of proving the unsolvability of the quintic. However, it is an important family of examples in Galois theory.

We will consider in a little more detail the Galois groups associated to roots of unity. We start with an example.

Example 4.1 Let $\zeta \in \mathbb{C}$ be a primitive 5th root of unity. The minimal polynomial of ζ over $\mathbb{Q}$ is $\frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$. The remaining roots of this polynomial are the other three primitive 5th roots of unity. If ξ is one of them, then $\xi = \zeta^j$ for some j. It follows that $\mathbb{Q}(\xi) = \mathbb{Q}(\zeta)$. It follows easily from Corollary 3.12 that if ξ is any primitive 5th root of unity, then there is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta)$ sending ζ to ξ. Thus

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\theta_1, \theta_2, \theta_3, \theta_4\}$$

where θ_i is the $\mathbb{Q}$-automorphism sending ζ to ζ^i.

Note that $\theta_1 = \mathrm{id}$, and that

$$\begin{aligned} \theta_2^2(\zeta) &= \theta_2(\zeta^2) = (\zeta^2)^2 = \zeta^4, \\ \theta_2^3(\zeta) &= \theta_2(\zeta^4) = (\zeta^4)^2 = \zeta^8 = \zeta^3, \end{aligned}$$

(so $\theta_2^2 = \theta_4$ and $\theta_2^3 = \theta_3$) so that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic with 4 elements, and is generated by θ_2 ($\theta_2^2 = \theta_4$ and $\theta_2^3 = \theta_3$). ⊠

In order to state the most general result, we need to define cyclotomic polynomials.

Definition 4.2 Let $n \geq 1$. Define the nth *cyclotomic polynomial* by

$$\lambda_n(x) = \prod_{\text{primitive } n\text{th roots of unity}} (x - \zeta).$$

▲

Let's write down the first few:

$$\begin{aligned} \lambda_1(x) &= x - 1 \\ \lambda_2(x) &= x + 1 \\ \lambda_3(x) &= (x-\omega)(x-\omega^2) = x^2 + x + 1 \\ \lambda_4(x) &= (x+i)(x-i) = x^2 + 1 \\ \lambda_5(x) &= \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1 \\ \lambda_6(x) &= (x+\omega)(x+\omega^2) = x^2 - x + 1 \end{aligned}$$

where ω denotes a primitive cube root of unity. In general, one can see that $\lambda_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + 1$ when p is a prime.

We have the following formula, which allows us to compute the cyclotomic polynomials inductively:

Lemma 4.3

$$x^n - 1 = \prod_{d|n} \lambda_d(x).$$

PROOF. An nth root of unity will be a primitive dth root for some $d|n$. Conversely, if $d|n$, a primitive dth root of unity is an nth root of unity. ⊠

For example, if $n = 6$, the 6th roots of unity are 1, -1, $\pm\omega$ and $\pm\omega^2$. We split these into the primitive 1st roots, i.e., 1, the primitive square roots, i.e., -1, the primitive cube roots, i.e., ω and ω^2, and the primitive 6th roots, $-\omega$ and $-\omega^2$. It is clear then that the product of the cyclotomic polynomials λ_d for $d|6$ is $x^6 - 1$. Indeed, since the roots of $x^6 - 1$ are the sixth roots of unity, we have:

$$\begin{aligned} x^6 - 1 &= (x-1)(x - e^{\frac{2\pi i}{6}})(x - e^{\frac{4\pi i}{6}})(x - e^{\frac{6\pi i}{6}})(x - e^{\frac{8\pi i}{6}})(x - e^{\frac{10\pi i}{6}}) \\ &= (x-1)(x+\omega^2)(x-\omega)(x+1)(x-\omega^2)(x+\omega) \\ &= (x-1)(x+1)[(x-\omega)(x-\omega^2)][(x+\omega)(x+\omega^2)] \\ &= \lambda_1(x)\lambda_2(x)\lambda_3(x)\lambda_6(x). \end{aligned}$$

Remark 4.4 Note that the nth roots of unity are $e^{\frac{2\pi i m}{n}}$ for $m = 0, \ldots, n-1$. Further, $e^{\frac{2\pi i m}{n}}$ is primitive if m and n are coprime. It follows that the number of primitive nth roots of unity is

$$\varphi(n) = |\{0 \leqslant m \leqslant n-1 \mid m \text{ and } n \text{ are coprime}\}|.$$

As there is a factor of λ_n for every primitive nth root of unity, it follows that $\deg \lambda_n = \varphi(n)$. Incidentally, if we look at the degrees of the polynomials in Lemma 4.3, we deduce that $n = \sum_{d|n} \varphi(d)$, which is an interesting number-theoretic result in its own right.

Proposition 4.5 λ_n is a monic polynomial with integer coefficients.

PROOF. By induction on n. Note $\lambda_1 = x - 1$ satisfies the Proposition. Let $f(x) = \prod_{d|n, d<n} \lambda_d(x)$. Then by induction, f is monic with integer coefficients. By Lemma 4.3, $x^n - 1 = f\lambda_n$. Now we use the following:

Claim. If $p = qr$ is a product of polynomials, where p and q are monic with integer coefficients, then so is r.

Proof. Suppose

$$\begin{aligned} p(x) &= x^{s+t} + p_1 x^{s+t-1} + \cdots + p_{s+t} \\ q(x) &= x^s + q_1 x^{s-1} + \cdots + q_s \\ r(x) &= r_0 x^t + r_1 x^{t-1} + \cdots + r_t \end{aligned}$$

By comparing coefficients of x^{s+t}, we see $r_0 = 1$, so r is monic. Also, suppose we have shown that $r_0, \ldots r_{k-1} \in \mathbb{Z}$. Then, comparing coefficients of x^{s+t-k}, we see that

$$p_k = q_k + q_{k-1}r_1 + \cdots + q_1 r_{k-1} + r_k,$$

so we see $r_k \in \mathbb{Z}$. Inductively, each $r_i \in \mathbb{Z}$, so $r \in \mathbb{Z}[x]$. This proves the claim.

Now apply this with $p = x^n - 1$, $q = f$ and $r = \lambda_n$, to see that $\lambda_n \in \mathbb{Z}[x]$. ⊠

Fact 4.6 λ_n is irreducible in $\mathbb{Q}[x]$ and hence is the minimal polynomial of any primitive nth root of unity. (In practice, one can often use Eisenstein's criterion after replacing x with $x+1$ or $x-1$ to deduce the irreducibility of λ_n.)

Definition 4.7 If ζ is a primitive nth root of unity, then the extension $\mathbb{Q}(\zeta)$ is the *nth cyclotomic extension* of $\mathbb{Q}$. ▲

Note that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. Finally, we can give the structure of the Galois group of these cyclotomic extensions.

Theorem 4.8 $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(\mathbb{Z}_n)$*, the multiplicative group of integers modulo n and prime to n.*

PROOF. As already remarked, the primitive roots of unity are exactly ζ^r, with $(r, n) = 1$. Further, $\mathbb{Q}(\zeta^r) = \mathbb{Q}(\zeta)$ for such r. Then

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\varphi_r \mid 1 \leqslant r \leqslant n, (r, n) = 1\},$$

where φ_r is the $\mathbb{Q}$-automorphism mapping ζ to ζ^r. As $\zeta^r = \zeta^s$ whenever $r \equiv s \pmod{n}$, we should really write φ_r as $\varphi_{\overline{r}}$. Thus we get a bijection

$$\begin{array}{ccc} U(\mathbb{Z}_n) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ \overline{r} & \mapsto & \varphi_{\overline{r}} \end{array}$$

As $\varphi_{\overline{r}} \circ \varphi_{\overline{s}} = \varphi_{\overline{rs}}$, because $(\zeta^s)^r = \zeta^{rs}$, it is a group homomorphism, and the result follows. ⊠

Remark 4.9 It follows that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic when $U(\mathbb{Z}_n)$ is cyclic. This is true when n is prime but not true if n is divisible by two or more distinct odd primes.

While we are thinking about roots of unity, we'll end the section with a couple of easy results which we'll need later.

Lemma 4.10 Let $n \geq 1$ be an integer, and let L be the splitting field over K of $x^n - 1$. Then $\mathrm{Gal}(L/K)$ is abelian.

PROOF. If $\zeta = e^{\frac{2\pi i}{n}}$ denotes a primitive nth root of unity in L, then $L = K(\zeta)$, and all K-automorphisms of L are given by $\zeta \mapsto \zeta^i$ for i prime to n. Composing any two automorphisms of this form is independent of the order of composition (as $(\zeta^i)^j = (\zeta^j)^i$), so that $\mathrm{Gal}(L/K)$ is abelian. ⊠

Lemma 4.11 Let K be a field containing the nth roots of unity. Let $a \in K$. If L denotes the splitting field of $x^n - a$ over K, then $\mathrm{Gal}(L/K)$ is cyclic (of order dividing n).

PROOF. Let α denote any root of $x^n - a$ in L. Then all roots are given by $\zeta^j\alpha$, where $\zeta = e^{\frac{2\pi i}{n}} \in K$, for $j = 0, \ldots, n-1$. Hence the splitting field L is $K(\alpha)$, and the map $\theta \mapsto \frac{\theta(\alpha)}{\alpha}$ gives an injective homomorphism from $\mathrm{Gal}(L/K) \longrightarrow \langle\zeta\rangle$. ⊠

§ 5 Galois extensions

Let $f(x) \in K[x]$ be a polynomial with splitting field K_f/K. Recall that our goal for the course is to use the group theoretic properties of $\mathrm{Gal}(K_f/K)$ to understand the properties of f.

So far, we have attached a Galois group to any field extension L/K. In this section, we will see that a certain class of field extensions, the *Galois* extensions, will be the right extensions to study.

Normal extensions and Galois extensions

Example 5.1 Consider the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. This field extension behaves badly in a number of ways:

1. The minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $f(x) = x^4 - 2$. The field $\mathbb{Q}(\sqrt[4]{2})$ does not contain all of the roots of f: it contains neither $i\sqrt[4]{2}$ nor $-i\sqrt[4]{2}$.

   In particular, the field extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ does not capture all of the information coming from the polynomial f. Indeed, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not the splitting field of *any* polynomial.

2. The Galois group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is

   $$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \{\mathrm{id}, \mathrm{conj}\},$$

   where id is the identity, and $\mathrm{conj} : \sqrt[4]{2} \mapsto -\sqrt[4]{2}$.

   However, if we consider $\mathbb{Q}(\sqrt[4]{2})$ as an extension of $\mathbb{Q}(\sqrt{2})$, then the Galois group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is

   $$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})) = \{\mathrm{id}, \mathrm{conj}\},$$

   and hence,

   $$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})) = \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}).$$

   In particular, the Galois group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ does not capture all of the information of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Rather, it only sees the subextension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$.

3. The order of the Galois group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is 2, which is smaller than the degree $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$.

Based on this example, the right extensions to study will be those without these bad properties.

Definition 5.2 A finite extension $K \subseteq L$ is *normal* if for every $\ell \in L$, the minimal polynomial f of ℓ over K splits into linear factors in L.

Equivalently, if $f(x) \in K[x]$ is a polynomial, then L either contains all the roots of f or none of the roots of f. ▲

Examples 5.3 1. The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal, since it does not contain all the roots of $x^4 - 2$.

2. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal. Indeed, every element of $\mathbb{Q}(\sqrt{2})$ is of the form $a + b\sqrt{2},\ a, b \in \mathbb{Q}$, and the second root of the minimal polynomial of $a + b\sqrt{2}$ is $a - b\sqrt{2}$.

3. A similar argument shows that every extension L/K of degree 2 is normal. In particular, the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is normal.

Definition 5.4 A finite extension $K \subseteq L$ of fields is *Galois* if

$$|\mathrm{Gal}(L/K)| = [L : K].$$

▲

Examples 5.5 1. The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois.

2. The extension $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cubed root of unity, is Galois.

3. Every extension L/K of degree 2 is Galois. Indeed, we can write $L = K(\sqrt{\beta})$ for some $\beta \in L$, and
$$\mathrm{Gal}(L/K) = \{\mathrm{id}, \mathrm{conj}\},$$
where id is the identity, and $\mathrm{conj} : \sqrt{\beta} \mapsto -\sqrt{\beta}$, so
$$|\mathrm{Gal}(L/K)| = [L : K] = 2.$$

Definition 5.6 Let L be a field, and let S be a finite set of automorphisms L. The *fixed field* of S

$$L^S = \{x \in L : \theta(x) = x \text{ for all } \theta \in S\}.$$

▲

(To see that L^S is a field, use the subfield criterion, noting that by definition $L^S \subseteq L$.)

Examples 5.7 1. If $L = \mathbb{Q}(\sqrt[4]{2})$, then

$$L^{\mathrm{Gal}(L/\mathbb{Q})} = L^{\{\mathrm{id},\mathrm{conj}\}} = \mathbb{Q}(\sqrt{2}).$$

2. If $L = \mathbb{Q}(\sqrt{2}))$, then

$$L^{\mathrm{Gal}(L/\mathbb{Q})} = L^{\{\mathrm{id},\mathrm{conj}\}} = \mathbb{Q}.$$

We have the following theorem:

Theorem 5.8 *Let $K \subseteq L$ be a finite extension of fields. Assume that $K, L \subseteq \mathbb{C}$. The following are equivalent:*

1. *L/K is Galois;*
2. *L is the splitting field of an irreducible polynomial $f \in K[x]$;*
3. *L/K is normal;*
4. *$K = L^{\mathrm{Gal}(L/K)}$.*

This equivalence is one of our first indications that a statement purely about fields ("L is the splitting field of a polynomial over K") is equivalent to a statement about the Galois group ("$|\mathrm{Gal}(L/K)| = [L : K]$"). We will prove that $(1) \implies (2) \implies (3) \implies (1)$ and that $(1) \iff (4)$. We first prove $(1) \implies (2)$.

Lemma 5.9 Suppose $K \subseteq L$ is an extension of fields. If L/K is Galois, then L is the splitting field of an irreducible polynomial over K.

PROOF. By TPE (Theorem 2.5), there exists an $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over K. We know:

- $[L : K]$ is equal to the degree of f (Theorem 2.2),
- $|\mathrm{Gal}(L/K)|$ is equal to the number of distinct roots of f in L (Corollary 3.12).

So we see that $[L : K] = |\mathrm{Gal}(L/K)|$ implies that the number of roots of f in L is equal to the degree of f, i.e., if f factorises over L into distinct linear factors. We have therefore shown that if L/K is Galois, then L is the splitting field of a polynomial over K. ⊠

Next, we prove that $(2) \implies (3)$.

Lemma 5.10 Let L be the splitting field of an irreducible polynomial over K. Then L/K is normal.

PROOF. Suppose L is the splitting field of a polynomial $f \in K[x]$. Let $g \in K[x]$ be any other polynomial with a root $\alpha \in L$. Suppose that β is another root of g. We need to show that $\beta \in L$.

By Theorem 3.11, there is an isomorphism $\theta : K(\alpha) \to K(\beta)$ which fixes K and maps $\alpha \mapsto \beta$.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of f. Then it is a fact that we can define a homomorphism

$$\varphi : K(\alpha, \alpha_1, \ldots, \alpha_n) \to K(\beta, \alpha_1, \ldots, \alpha_n)$$

that maps $\alpha \mapsto \beta$. Note that φ is a map $L \to L(\beta)$.

But by APR (Theorem 3.10), φ must map each of the roots of f to another root of f. Since L is generated by the roots of f, it follows that $\varphi(L) \subseteq L$. Hence $L(\beta) = L$, so $\beta \in L$, as required. ⊠

We now prove that $(3) \implies (1)$.

Lemma 5.11 Suppose $K \subseteq L$ is an extension of fields, and that $K, L \subseteq \mathbb{C}$. If L/K is normal, then L/K is Galois.

PROOF.

By TPE (Theorem 2.5), there exists an $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over K. We know:

- $[L : K]$ is equal to the degree of f (Theorem 2.2);
- $|\mathrm{Gal}(L/K)|$ is equal to the number of distinct roots of f in L (Corollary 3.12).

Since L/K is normal and $\alpha \in L$, L must contain all the roots of f. Hence,

$$|\mathrm{Gal}(L/K)| = \#\{\text{roots of } f\} = \deg(f) = [L : K],$$

so L/K is Galois. ⊠

We complete the proof of Theorem 5.8 by proving $(1) \iff (4)$.

PROOF OF THEOREM 5.8.

We'll first show that $(1) \implies (4)$. Assume that L/K is Galois, and let $G = \mathrm{Gal}(L/K)$. We need to show that $L^G = K$.

Consider the Galois group $\mathrm{Gal}(L/L^G)$. Then $G \subseteq \mathrm{Gal}(L/L^G)$. Indeed, G acts on L and fixes L^G.

However, we have $K \subseteq L^G \subset L$. So

$$|G| \leqslant |\mathrm{Gal}(L/L^G)| \leqslant [L : L^G] \leqslant [L : K].$$

Since L/K is Galois, $|G| = [L : K]$, and hence $[L : L^G] = [L : K]$. so $L^G = K$ as required.

We'll now show that $(4) \implies (1)$. Write $G = \mathrm{Gal}(L/K)$ and suppose that $L^G = K$. We need to show that L/K is Galois. By TPE (Theorem 2.5), there exists an $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over K.

Consider the polynomial

$$g(x) = \prod_{\varphi \in \mathrm{Gal}(L/K)} (x - \varphi(\alpha)) \in L[x],$$

i.e. the polynomial in $L[x]$ whose roots are $\varphi(\alpha)$ for all $\varphi \in \mathrm{Gal}(L/K)$. We will show that $g(x) \in K[X]$.

Suppose that $\theta \in \mathrm{Gal}(L/K)$. Then

$$\begin{aligned} \theta(g(x)) &= \theta \left(\prod_{\varphi \in \mathrm{Gal}(L/K)} (x - \varphi(\alpha)) \right) \\ &= \prod_{\varphi \in \mathrm{Gal}(L/K)} (x - \theta\varphi(\alpha)) \\ &= \prod_{\psi \in \mathrm{Gal}(L/K)} (x - \psi(\alpha)) \qquad \text{where } \psi = \theta\varphi \\ &= g(x). \end{aligned}$$

Hence, θ fixes all the coefficients of $g(x)$, so $g(x) \in L^G[x]$. Since $L^G = K$, we have $g(x) \in K[X]$.

But α is a root of $g(x)$, so we must have $f(x) \mid g(x)$. Hence,

$$[L : K] = \deg(f) \leqslant \deg(g) = |\mathrm{Gal}(L/K)| \leqslant [L : K],$$

from which it follows that $|\mathrm{Gal}(L/K)| = [L : K]$. Hence, L/K is Galois. ⊠

Subextensions of Galois extensions

Remember from the sketch of our plan that we are going to try to build up larger extensions from small ones. This means that it is important to consider chains of extensions.

Corollary 5.12 Suppose L/K is a Galois extension, and that $K \subseteq M \subseteq L$ is an intermediate field. Then L/M is Galois.

PROOF. Suppose that L is the splitting field of some polynomial $f \in K[x]$. Then certainly $f \in M[x]$, as $K \subseteq M$; but L splits f and is generated over K by the roots, so it is also generated over M by the roots. Thus L is the splitting field for f over M, and is therefore Galois by Theorem 5.8. ⊠

Note that any automorphism of L which fixes every element of M will certainly fix every element of K. It follows that $\mathrm{Gal}(L/M)$ is a subset (and therefore a *subgroup*) of $\mathrm{Gal}(L/K)$.

However, in general, M/K need not be Galois. We have already seen a simple example:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega).$$

Let's now think about the case of field extensions $K \subseteq M \subseteq L$, in which L/K is Galois (and therefore so is L/M). Remarkably, the condition that M/K should be Galois has a simple reformulation in terms of groups.

Lemma 5.13 Let $K \subseteq M \subseteq L$ be finite extensions of fields. If M/K is Galois, then $\varphi(M) = M$ for all $\varphi \in \mathrm{Gal}(L/K)$.

PROOF. We may suppose that $M = K(\alpha)$ is the splitting field for the irreducible polynomial m_α by TPE (Theorem 2.5). The element φ must map α to another root of m_α by APR (Theorem 3.10); but this root, β say, is also in M, because M splits m_α. It then follows that $\varphi(M) \subseteq M$, and similarly $\varphi^{-1}(M) \subseteq M$, so $\varphi(M) = M$. ⊠

The situation when M/K is Galois is explained by the following theorem.

Theorem 5.14 *Let $K \subset L$ be a Galois extension, and let M be an intermediate field. Then M/K is Galois if and only if $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$. In this case, there is an isomorphism*

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Gal}(M/K).$$

We will prove each direction of this if and only if statement separately.

Theorem 5.15 *Let $K \subset L$ be a Galois extension, and let M be an intermediate field. Then if M/K is Galois, $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$, and there is an isomorphism*

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Gal}(M/K).$$

PROOF. If M/K is Galois, then $\varphi(M) = M$ for all $\varphi \in \mathrm{Gal}(L/K)$, by the preceding Lemma. That is, given $m \in M$, $\varphi(m) \in M$ also. Since any θ in $\mathrm{Gal}(L/M)$ will fix all elements of M, we see that $\theta(\varphi(m)) = \varphi(m)$ for all $m \in M$, $\theta \in \mathrm{Gal}(L/M)$ and $\varphi \in \mathrm{Gal}(L/K)$. Therefore $\varphi^{-1}\theta\varphi(m) = m$, and so $\varphi^{-1}\theta\varphi$

fixes every element of M. It follows that $\varphi^{-1}\theta\varphi \in \mathrm{Gal}(L/M)$, and therefore $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$.

For the second part, define a map

$$\begin{array}{rcl} \Phi : \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(M/K) \\ \varphi & \mapsto & \varphi|_M \end{array}$$

where $\varphi|_M$ is the restriction of φ to $M \to M$ (recall that $\varphi(M) = M$). So $\varphi|_M \in \mathrm{Gal}(M/K)$, as required. The map that sends each φ to $\varphi|_M$ is easily seen to be a group homomorphism, and its kernel consists of all φ such that $\varphi|_M(m) = m$ for all $m \in M$, i.e., $\varphi \in \mathrm{Gal}(L/M)$.

Then the first isomorphism theorem for groups gives:

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Im}\,\Phi \subseteq \mathrm{Gal}(M/K).$$

However, if we compare the sizes of the two sides, bearing in mind that L/K and L/M are both Galois (by Corollary 5.12):

$$|\mathrm{Im}\,\Phi| = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|} = \frac{[L:K]}{[L:M]} = [M:K] = |\mathrm{Gal}(M/K)|$$

using the Degrees Theorem 2.3, and so $\mathrm{Im}\,\Phi = \mathrm{Gal}(M/K)$. ⊠

Theorem 5.16 *Suppose that L/K is Galois, and let M be an intermediate field. If $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$, then M/K is Galois.*

Proof. Note that

$$\begin{array}{ll} & \mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K) \\ \iff & \varphi^{-1}\theta\varphi \in \mathrm{Gal}(L/M) \text{ for all } \theta \in \mathrm{Gal}(L/M), \varphi \in \mathrm{Gal}(L/K) \\ \iff & \varphi^{-1}\theta\varphi(m) = m \text{ for all } m \in M, \theta \in \mathrm{Gal}(L/M), \varphi \in \mathrm{Gal}(L/K) \\ \iff & \theta\varphi(m) = \varphi(m) \text{ for all } m \in M, \theta \in \mathrm{Gal}(L/M), \varphi \in \mathrm{Gal}(L/K) \\ \iff & \varphi(M) \subseteq L^{\mathrm{Gal}(L/M)} \text{ for all } \varphi \in \mathrm{Gal}(L/K) \\ \iff & \varphi(M) \subseteq M \text{ for all } \varphi \in \mathrm{Gal}(L/K) \text{ by Theorem 5.8} \\ \iff & \varphi(M) = M \text{ for all } \varphi \in \mathrm{Gal}(L/K) \end{array}$$

As in Theorem 5.15, define

$$\begin{array}{rcl} \Phi : \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(M/K) \\ \theta & \mapsto & \theta_M \end{array}$$

where $\theta_M(m) = \theta(m)$ for $m \in M$. As $\theta(M) = M$, $\theta_M \in \mathrm{Gal}(M/K)$, as required. Also, one easily sees that Φ is a group homomorphism. Further, its kernel is $\mathrm{Gal}(L/M)$. The first isomorphism theorem gives

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Im}\,\Phi \subseteq \mathrm{Gal}(M/K).$$

and, as in the proof of Theorem 5.15,

$$[M : K] \geq |\mathrm{Gal}(M/K)| \geq \left|\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)}\right| = \frac{[L : K]}{[L : M]} = [M : K],$$

and so $[M : K] = |\mathrm{Gal}(M/K)|$, and M/K is therefore Galois. ⊠

§ 6 The Galois correspondence

Before we look at the principal application, to the insolubility of the quintic, we will look at the Galois correspondence. The main theorem of the theory is that a polynomial is soluble if and only if the Galois group of its splitting field has a particular property (also called solubility). One result, that there exist polynomials whose Galois groups are not soluble, does not require the Galois correspondence. However, the converse, that if the Galois group of a polynomial is soluble, then the polynomial is soluble, does require the correspondence.

The Fundamental Theorem of Galois Theory

The aim of the fundamental theorem of Galois theory is to compare, in the case where L/K is Galois, intermediate subfields $K \subseteq M \subseteq L$ and subgroups of $\mathrm{Gal}(L/K)$. The answer is as nice as one could hope for, although the proof (see Theorem 12.2) is quite long.

Definition 6.1 Let L/K be a Galois extension, and let H be a subgroup of $\mathrm{Gal}(L/K)$. Then we write L^H for

$$L^H = \{\ell \in L \mid \theta(\ell) = \ell \text{ for all } \theta \in H\},$$

the *fixed field* of H. ▲

(To see that L^H is a field, use the subfield criterion, noting that by definition $L^H \subseteq L$.)

Theorem 6.2 (Fundamental Theorem of Galois Theory) *Let L be a Galois extension of K, and let $G = \mathrm{Gal}(L/K)$. There is a bijection from*

$$\mathscr{S} := \{\textit{subgroups of } G\}$$

to

$$\mathscr{F} := \{\textit{intermediate fields } K \subseteq M \subseteq L\}$$

given by $H \mapsto L^H$ with inverse $M \mapsto \mathrm{Gal}(L/M)$.

Moreover, the correspondence is inclusion reversing, that is,

$$H_1 \supseteq H_2 \iff L^{H_1} \subseteq L^{H_2},$$

and indexes equal degrees, that is,

$$\frac{|H_1|}{|H_2|} = [L^{H_2} : L^{H_1}].$$

Finally, normal subgroups of G correspond to intermediate fields $K \subseteq M \subseteq L$ such that M/K is Galois.

Terminology: for any inclusion of subgroups of any group, $\frac{|H_1|}{|H_2|}$ is called the *index of H_2 in H_1*. It is the number of cosets $h_1 H_2$ for $h_1 \in H_1$.

PROOF. Let H be a subgroup of G, and let M be an intermediate subfield $K \subseteq M \subseteq L$. To prove that $\mathscr{S}$ and $\mathscr{F}$ are in bijection, we need to show that the maps we've constructed are mutually inverse, i.e. that

- $L^{\mathrm{Gal}(L/M)} = M$;
- $\mathrm{Gal}(L/L^H) = H$.

For the first part, by Corollary 5.12, L/M is Galois. Hence, by part (4) of Theorem 5.8, $L^{\mathrm{Gal}(L/M)} = M$.

For the second part, first observe that $H \subseteq \mathrm{Gal}(L/L^H)$—indeed, H acts on L and fixes L^H. We will show that $|\mathrm{Gal}(L/L^H)| \leqslant |H|$, so that this inclusion is an equality. Our argument will mimic the proof of $(4) \implies (1)$ in Theorem 5.8.

Let $M = L^H$. Then by Corollary 5.12, L/M is Galois. By TPE (Theorem 2.5), there exists an $\alpha \in L$ such that $L = M(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over M.

Consider the polynomial

$$g(x) = \prod_{\varphi \in H} (x - \varphi(\alpha)) \in L[x],$$

i.e. the polynomial in $L[x]$ whose roots are $\varphi(\alpha)$ for all $\varphi \in H$. We will show that $g(x) \in M[X]$.

Suppose that $\theta \in H$. Then

$$\begin{aligned} \theta(g(x)) &= \theta\left(\prod_{\varphi \in H} (x - \varphi(\alpha))\right) \\ &= \prod_{\varphi \in H} (x - \theta\varphi(\alpha)) \\ &= \prod_{\psi \in H} (x - \psi(\alpha)) \qquad \text{where } \psi = \theta\varphi \\ &= g(x). \end{aligned}$$

Hence, θ fixes all the coefficients of $g(x)$, so $g(x) \in L^H[x] = M[x]$. But α is a root of $g(x)$, so we must have $f(x) \mid g(x)$. Hence,

$$[L : M] = \deg(f) \leqslant \deg(g) = |H|,$$

from which it follows that $\mathrm{Gal}(L/M) = H$, as required.

It follows that the two maps $H \mapsto L^H$ and $M \mapsto \mathrm{Gal}(L/M)$ are inverse bijections.

For the other part, observe that if $H_1 \supseteq H_2$, we have $L^{H_1} \subseteq L^{H_2}$ (anything in L fixed by H_1 will be fixed by H_2); conversely, if $L^{H_1} \subseteq L^{H_2}$, the first part of the theorem shows that then $\mathrm{Gal}(L/L^{H_1}) \supseteq \mathrm{Gal}(L/L^{H_2})$, and also that $\mathrm{Gal}(L/L^{H_i}) = H_i$, so that $H_1 \supseteq H_2$.

For the assertion about indexes and degrees, first observe that it is immediate if $H_2 = 1$. In this case, $L^{H_2} = L$, and

$$(H_1 : 1) = |H_1| = |\mathrm{Gal}(L/L^{H_1})| = [L : L^{H_1}].$$

Now consider the general case. We use the special case above to see that $|H_i| = [L : L^{H_i}]$. But also we have:

$$|H_1| = |H_2|(H_1 : H_2) \quad \text{and} \quad [L : L^{H_1}] = [L : L^{H_2}][L^{H_2} : L^{H_1}]$$

(by the Degrees Theorem 2.3). Comparing these gives the result.

⊠

Example 6.3 We are now going to look at the Galois theory of the polynomial $x^3 - 2$. Its splitting field is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cube root of unity, so this is Galois over $\mathbb{Q}$. Let's first look at all of the subfields of this field. I claim that the *subfield lattice* is:

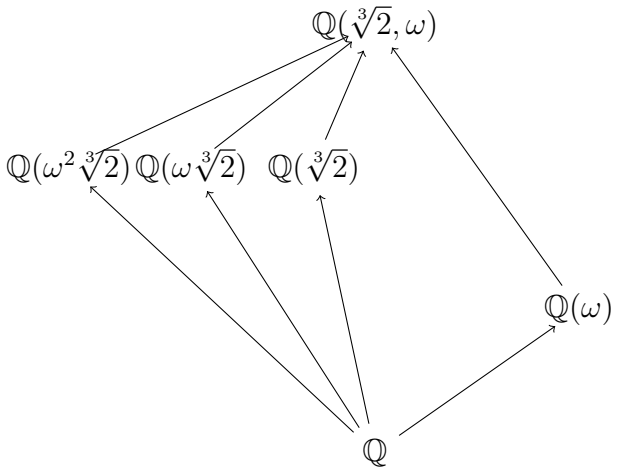

Figure 1: Lattice of subfields of $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

(One pictures the lattice of subfields of a field L by drawing a line between two subfields K and M whenever $K \subset M$ and there are no subfields strictly between K and M. Further, one arranges it so that M is higher up on the page than K.)

$\mathbb{Q}$-auto	effect on $\sqrt[3]{2}$	effect on ω	permutation
1	$\sqrt[3]{2}$	ω	id
φ	$\sqrt[3]{2}$	ω^2	(2 3)
ψ	$\omega\sqrt[3]{2}$	ω	(1 2 3)
$\psi\varphi$	$\omega\sqrt[3]{2}$	ω^2	(1 2)
ψ^2	$\omega^2\sqrt[3]{2}$	ω	(1 3 2)
$\varphi\psi$	$\omega^2\sqrt[3]{2}$	ω^2	(1 3)

Table 1

The idea of Galois theory is that this is reflected by the group theoretical structure of the subgroups of the Galois group. We have already seen that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ is S_3. Now S_3 has the (upside-down) subgroup lattice shown in Figure 2.

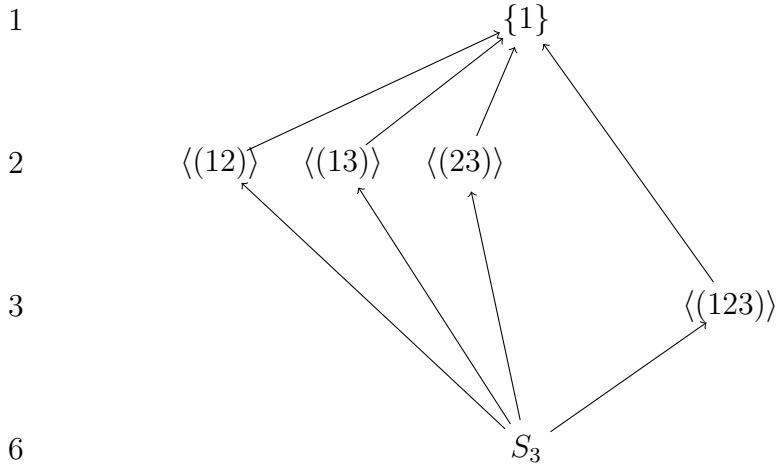

Figure 2: Subgroup lattice of S_3.

Note that the pictures look alike!

So the Galois correspondence is between the six subfields of $\mathbb{Q}(\sqrt[3]{2},\omega)$ and the six subgroups of S_3.

We now check that the above pictures correspond.

Table 1 shows the isomorphism $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}) \cong S_3$.

Thus, if we consider the subfield $\mathbb{Q}(\omega)$ of $\mathbb{Q}(\sqrt[3]{2},\omega)$, then we can see that $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\sqrt[3]{2},\omega)^{\langle(123)\rangle}$. This is because $\psi(\omega) = \omega$. Note that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

Now we use the Galois correspondence to see that the degree equals the index, and so we see that we have an equality $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt[3]{2},\omega)^{\langle(123)\rangle}$.

In a similar way, we can identify the fixed field of each subgroup of S_3, and they correspond as in the picture. (Exercise: which of the fields are Galois extensions of $\mathbb{Q}$?) ⊠

Example 6.4 Let $L = \mathbb{Q}(\sqrt[4]{2}, i)$, the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Thus $\mathbb{Q} \subseteq L$ is Galois. $[L : \mathbb{Q}] = 8$, as $[L : \mathbb{Q}(\sqrt[4]{2})] = 2$ and $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Then $|\mathrm{Gal}(L/\mathbb{Q})| = 8$.

Now $\sqrt[4]{2}$ has minimal polynomial $x^4 - 2$, whose roots are $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$ and $-i\sqrt[4]{2}$. Further, i has minimal polynomial $x^2 + 1$, whose roots are $\pm i$.

The eight possible $\mathbb{Q}$-automorphisms of M are given in the following table:

$\mathbb{Q}$-auto	effect on $\sqrt[4]{2}$	effect on i	permutation	remarks
1	$\sqrt[4]{2}$	i	id	
r	$i\sqrt[4]{2}$	i	(1 2 3 4)	$r^4 = 1$
r^2	$-\sqrt[4]{2}$	i	(1 3)(2 4)	
r^3	$-i\sqrt[4]{2}$	i	(1 4 3 2)	
s	$\sqrt[4]{2}$	$-i$	(2 4)	$s^2 = 1$
rs	$i\sqrt[4]{2}$	$-i$	(1 2)(3 4)	
r^2s	$-\sqrt[4]{2}$	$-i$	(1 3)	
r^3s	$-i\sqrt[4]{2}$	$-i$	(1 4)(2 3)	$r^3s = sr$

It follows that $\mathrm{Gal}(L/\mathbb{Q}) = \langle r, s \mid r^4 = s^2 = 1, r^3s = sr\rangle \cong D_4$. The (upside-down) subgroup lattice of D_4 is shown in Figure 3.

The subfield lattice of L is shown in Figure 4.

We leave it as an exercise to verify the correspondence. We give just one example, namely, the field $M = \mathbb{Q}((1+i)\sqrt[4]{2})$. We first prove it is fixed by rs.

$$rs((1+i)\sqrt[4]{2}) = rs(\sqrt[4]{2}) + rs(i\sqrt[4]{2}) = i\sqrt[4]{2} + \sqrt[4]{2} = (1+i)\sqrt[4]{2}.$$

Next we check that it is not fixed by r^2:

$$r^2((1+i)\sqrt[4]{2}) = r^2(\sqrt[4]{2}) + r^2(i\sqrt[4]{2}) = -\sqrt[4]{2} - i\sqrt[4]{2} = -(1+i)\sqrt[4]{2}.$$

It follows that the subgroup of D_4 corresponding to M must be a subgroup containing rs but not r^2. A quick examination of the list of subgroups shows that the only possibility is $\{1, rs\}$. The other correspondences are similar. ⊠

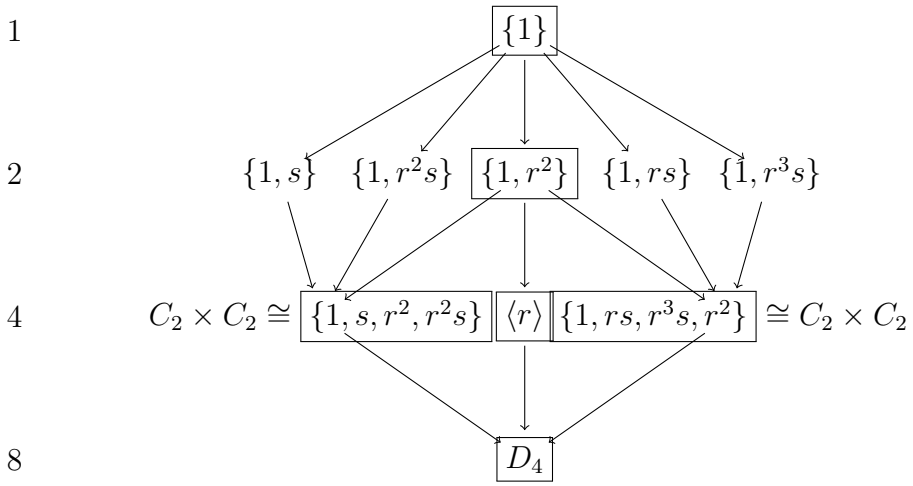

Figure 3: The subgroup lattice of D_4. The normal subgroups are boxed.

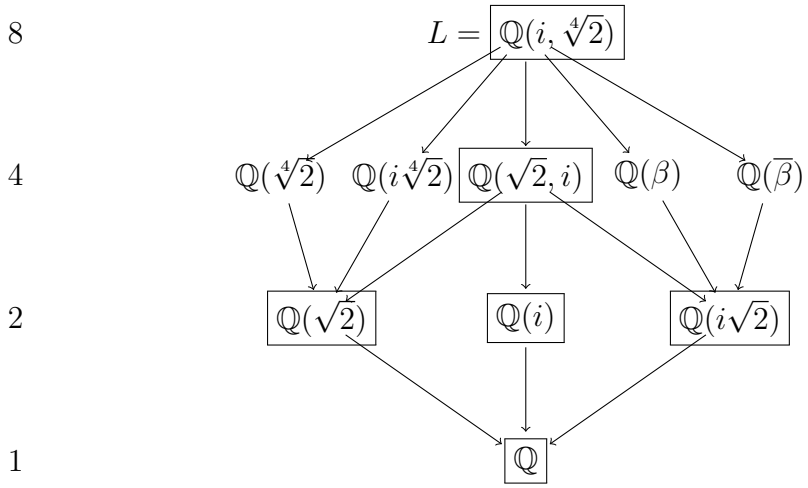

Figure 4: The subfield lattice of $L = \mathbb{Q}(i, \sqrt[4]{2})$. The subfields of L which are Galois extensions of $\mathbb{Q}$ are boxed. Note $\beta = (1+i)\sqrt[4]{2}$.

§ 7 Soluble groups

Remember our plan for proving the insolubility of the quintic. The basic idea is the following. Suppose that a polynomial is soluble by radicals (we'll make this more precise later). This implies that all of its roots have a certain form, and thus that the splitting field extension has a certain structure. We will see that this implies that the corresponding Galois group has a similar sort of structure. By exhibiting explicit examples of quintics whose Galois groups do not have this structure, we will see that not every quintic is soluble by radicals. We first need a digression in group theory.

In this section we develop the group theory necessary for applications to Galois theory. We begin with a summary of the results from this section that we will need for applications to Galois theory.

Definition 7.1 A group G is *soluble* provided it has a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_n = \{1\}$$

with each $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian. ▲

We start by recalling the first isomorphism theorem for groups (we've already used it, in fact!):

Theorem 7.2 *Let $\varphi : G \longrightarrow H$ be a group homomorphism. Then $\ker \varphi$ is a normal subgroup of G and there is an isomorphism $G/\ker \varphi \to \operatorname{Im} \varphi$.*

As corollaries, we deduce the second and third isomorphism theorems. Let's start with the second.

If H is a subgroup of G, and $N \lhd G$, then write

$$HN = \{hn : h \in H, n \in N\}.$$

It is a subgroup of G.

Theorem 7.3 *Let H and N be subgroups of G with $N \lhd G$. Then $H \cap N \lhd H$ and*

$$H/H \cap N \cong HN/N.$$

PROOF. Define a map $\Phi : H \longrightarrow HN/N$ by $h \mapsto hN$. It is not hard to see that Φ is a surjective homomorphism with kernel $H \cap N$. The result follows from the first isomorphism theorem. ⊠

Next, we do the third isomorphism theorem.

Theorem 7.4 *Let H and N be normal subgroups of G with $H \supseteq N$. Then $H/N \lhd G/N$ and*

$$(G/N)/(H/N) \cong G/H.$$

PROOF. Define a map $\Psi : G/N \to G/H$ by $\Psi(gN) = gH$. It is easy to check that Ψ is a well-defined surjective homomorphism with kernel H/N. Now use the first isomorphism theorem. ⊠

Having proven these technical results, we can now return to the study of soluble groups.

Theorem 7.5 *Let G be a group and H, N subgroups of G with $N \lhd G$. Then*

1. *if G is soluble then H is soluble;*
2. *if G is soluble then G/N is soluble;*
3. *if N and G/N are soluble then G is soluble.*

PROOF. 1. By definition, G has a chain

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

with each G_i/G_{i+1} abelian. Set $H_i = G_i \cap H$. So we have

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_r = \{1\}$$

(where we have deleted any redundant terms).

Note that $H_{i+1} = G_{i+1} \cap H = (G_i \cap H) \cap G_{i+1}$. Thus, by the second isomorphism theorem (7.3),

$$H_i/H_{i+1} = (G_i \cap H)/((G_i \cap H) \cap G_{i+1}) \cong (G_i \cap H)G_{i+1}/G_{i+1}.$$

This last group is a subgroup of the abelian group G_i/G_{i+1} and so is abelian. This proves 1.

2. Again G has the chain of 1. Apply the canonical homomorphism $\pi : G \to G/N$ sending g to gN. Then we get

$$G/N = G_0N/N \rhd G_1N/N \rhd \cdots \rhd G_nN/N = \{1_{G/N}\}$$

(discarding redundant terms). Now,

$$(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N,$$

by the third isomorphism theorem (7.4). On the other hand, the latter group is

$$G_i(G_{i+1}N)/G_{i+1}N \cong G_i/G_i \cap (G_{i+1}N),$$

by the second isomorphism theorem. Finally, by the third isomorphism theorem, we have

$$G_i/G_i \cap G_{i+1}N \cong (G_i/G_{i+1})/((G_i \cap G_{i+1}N)/G_{i+1}))$$

which (being a quotient of the abelian group G_i/G_{i+1}) is abelian.

3. Let $\overline{G}$ denote the quotient G/N. Suppose

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = \{1\}$$

and

$$N \triangleright N_1 \triangleright \cdots \triangleright N_m = \{1\}$$

with all successive quotients being abelian. Let

$$G_i = \{g \in G \mid gN \in \overline{G}_i\}.$$

Firstly, we see that G_i is a subgroup of G. For this, we use the subgroup criterion. Clearly $1 \in G_i$. Let g_1, $g_2 \in G_i$. Consider $g_1 g_2^{-1}$. Then

$$(g_1 g_2^{-1})N = (g_1 N)(g_2 N)^{-1} \in \overline{G}_i$$

as $\overline{G}_i$ is a group. It follows that $g_1 g_2^{-1} \in G_i$, and, by the subgroup criterion, G_i is a group.

Next we check that $G_i/N = \overline{G}_i$. The quotient G_i/N consists of all cosets gN with $g \in G_i$ – but the defining property of this group is that these cosets all lie in $\overline{G}_i$. It follows that $G_i/N \subseteq \overline{G}_i$. Conversely, every element of $\overline{G}_i$ is some coset gN, and then the corresponding g must lie in G_i, whereupon the inclusion $G_i/N \longrightarrow \overline{G}_i$ is surjective.

Lastly, we claim that $G_{i+1} \lhd G_i$. Let $g \in G_{i+1}$, and $\gamma \in G_i$. Then we want to show that $\gamma^{-1} g \gamma \in G_{i+1}$. But

$$(\gamma^{-1} g \gamma)N = (\gamma N)^{-1}(gN)(\gamma N) \in \overline{G}_{i+1}$$

because $\overline{G}_{i+1} \lhd \overline{G}_i$. It follows that $\gamma^{-1} g \gamma \in G_{i+1}$, as required. By the third isomorphism theorem, we also see that

$$\frac{\overline{G}_i}{\overline{G}_{i+1}} = \frac{G_i/N}{G_{i+1}/N} \cong \frac{G_i}{G_{i+1}},$$

so that each quotient G_i/G_{i+1} is abelian. Then the sequence

$$G \triangleright G_1 \triangleright \cdots \triangleright G_n = N \triangleright N_1 \triangleright \cdots \triangleright N_m = \{1\}$$

is a series whose successive quotients are all abelian. Thus G is soluble. ⊠

Remark 7.6 1. Abelian groups are soluble (consider the series $G \triangleright \{1\}$).

2. S_3 is soluble. A suitable chain is given by:

$$S_3 \triangleright \langle (123) \rangle \triangleright \{1\}.$$

3. S_4 is soluble. Here, a suitable chain is given by:

$$S_4 \triangleright A_4 \triangleright V_4 \triangleright \{1\},$$

where $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$.

4. D_4 is soluble. (It is a subgroup of S_4.)

5. A group G is called $simple$ if it is non-trivial and it has no normal subgroups besides $\{1\}$ and G. A group which is soluble and simple is easily seen to be cyclic of prime order.

6. If $n \geq 5$ then A_n is simple and so A_n is not soluble, for $n \geq 5$.

7. If $n \geq 5$, it follows that S_n is not soluble (if S_n were to be soluble, then its subgroup A_n would be soluble, and it isn't).

The crucial result is that S_1, S_2, S_3 and S_4 are soluble groups, but S_5 is not. This will reflect the fact that polynomials of degree up to 4 are soluble by radicals, but that quintics are not in general.

§ 8 Solubility of polynomials

Let's start by making the (now obvious) definition of the Galois group of a polynomial.

Definition 8.1 Let K be a field, and let $f \in K[x]$. Let L be the splitting field of f over K. Define the *Galois group of* f to be $\mathrm{Gal}(L/K)$. (Note that L/K is Galois as L is a splitting field (Theorem 5.8).) We will denote this group $\mathrm{Gal}(f/K)$. ▲

We will explain that many of the properties of f will be reflected in properties of its Galois group. Most importantly, we will see that if the polynomial is soluble in radicals then its Galois group is a soluble group. In fact, the converse is also true, and is proven in Appendix C. As we have produced examples of non-soluble groups, this may indicate that not every polynomial is soluble by radicals. To confirm this, we will give an explicit quintic whose Galois group is S_5.

Let's first recall some earlier results, Lemma 4.10 and Lemma 4.11.

Lemma 4.10. *Let $n \geq 1$ be an integer, and let L be the splitting field over K of $x^n - 1$. Then $\mathrm{Gal}(L/K)$ is abelian.*

Lemma 4.11. *Let K be a field containing the nth roots of unity. Let $a \in K$. If L denotes the splitting field of $x^n - a$ over K, then $\mathrm{Gal}(L/K)$ is cyclic (of order dividing n).*

If the conditions of Lemma 4.11 hold, we call L/K a *Kummer* extension.

Now we turn to solubility by radicals.

Definition 8.2 Let K be a field, and let $f \in K[x]$. The equation $f(x) = 0$ is said to be *soluble by radicals over* K if there is an extension field M of K such that

1. M splits f
2. M has a chain of subfields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m = M$$

such that, for each i, $K_{i+1} = K_i(d_i)$ with $d_i^{n_i} \in K_i$ for some positive integer n_i.

▲

Remark 8.3 Then f is soluble by radicals if and only if the roots of f are given by expressions involving elements of K and $+$, $-$, $\times$, $/$, and nth roots.

Now we can prove the theorem which will imply the insolubility of the general quintic.

Theorem 8.4 *If a polynomial $f \in K[x]$ is soluble by radicals, then $\mathrm{Gal}(f/K)$ is a soluble group.*

PROOF. We first find a Galois extension $\widetilde{L}$ of K with $\mathrm{Gal}(\widetilde{L}/K)$ soluble and such that $\widetilde{L}$ splits f.

This suffices to show that $\mathrm{Gal}(f/K)$ is soluble, because if L is the splitting field of f, we have $K \subseteq L \subseteq \widetilde{L}$, and then by Theorem 5.15, $\mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$ is a quotient of $\mathrm{Gal}(\widetilde{L}/K)$ – and quotients of soluble groups by normal subgroups are again soluble (by Theorem 7.5 (2)).

We are given that f splits in an extension $M = K_m$ of K with the following property: $K_m = K(d_1, \ldots, d_m)$ and, for all i, there exists a positive integer n_i such that $d_i^{n_i} \in K(d_1, \ldots, d_{i-1})$. As before, let ζ denote a primitive nth root of unity, where $n = \prod_i n_i$.

Let $\widetilde{L}$ be the smallest Galois extension of K which contains $K_m(\zeta)$. Then certainly $\widetilde{L}$ splits f (as it contains K_m).

Suppose $\mathrm{Gal}(\widetilde{L}/K) = \{\theta_1 = \mathrm{id}, \theta_2, \ldots, \theta_r\}$. Then each $\theta_i(\zeta)$ (necessarily a power of ζ by APR 3.10) and each $\theta_i(d_j)$ necessarily also lies in $\widetilde{L}$. Conversely, $\widetilde{L}$ is generated by these elements.

Adjoining the generating elements

$$\zeta, d_1, d_2, \ldots, d_m, \theta_2(d_1), \theta_2(d_2), \ldots, \theta_r(d_m)$$

one at a time, we get a sequence of fields

$$K \subseteq K(\zeta) \subseteq K(\zeta, d_1) \subseteq K(\zeta, d_1, d_2) \subseteq \cdots \subseteq \widetilde{L}$$

in which the first extension is Galois and abelian (by Lemma 4.10) and each subsequent non-trivial extension is Galois with cyclic Galois group (by Lemma 4.11).

This corresponds to the chain of subgroups

$$\mathrm{Gal}(\widetilde{L}/K) \triangleright \mathrm{Gal}(\widetilde{L}/K(\zeta)) \triangleright \mathrm{Gal}(\widetilde{L}/K(\zeta, d_1)) \triangleright \cdots \triangleright \mathrm{Gal}(\widetilde{L}/\widetilde{L}) = \{1\}$$

shows that $\mathrm{Gal}(\widetilde{L}/K)$ is soluble, as each successive non-trivial quotient after the first (which is abelian) is cyclic (using Theorem 5.15). ⊠

The converse theorem

The converse of this theorem is also true. Hence a polynomial is soluble by radicals if and only if its Galois group is soluble. To prove this fact, we will some auxiliary lemmas.

Lemma 8.5 Let G be a finite abelian group. Then there exists a chain of subgroups (each necessarily normal in G)

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$$

with each G_i/G_{i+1} cyclic of prime order.

Example 8.6 If $G = \langle a \rangle$ is cyclic of order 30 then one gets such a chain by

$$\langle a \rangle \triangleright \langle a^2 \rangle \triangleright \langle a^6 \rangle \triangleright \{1\}.$$

Here, the factors are C_2, C_3 and C_5. ⊠

PROOF. If G is trivial or cyclic of prime order then the result holds trivially. Otherwise G has a non-trivial, proper subgroup G_1. Choose G_1 to be maximal (i.e., there is no subgroup N with $G \triangleright N > G_1$). By induction on the order of G, the subgroup G_1 has an appropriate chain of subgroups

$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\}.$$

Furthermore, G/G_1 has no non-trivial, proper subgroups and so is cyclic of prime order. The result follows. ⊠

As a result of this lemma, we can give an alternative characterisation of when groups are soluble.

Corollary 8.7 A finite group G is soluble if and only if there is a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_n = \{1\}$$

with each $G_{i+1} \lhd G_i$ and G_i/G_{i+1} cyclic of prime order.

PROOF. ($\Longleftarrow$) is clear.

($\Longrightarrow$) Let G be finite and soluble. Take a series

$$G \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\}.$$

The successive quotients are abelian. In particular, the quotient $\overline{G} = G/G_1$ is abelian. By the previous lemma, there is a sequence

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_m = \{1\}$$

in which each quotient is a cyclic group of prime order. By the same technique as Theorem 7.5 (3), we can lift this to a series

$$G \triangleright G_{11} \triangleright \cdots \triangleright G_{1m} = G_1$$

and all successive quotients are cyclic of prime order. Similarly, between G_1 and G_2 we can construct a sequence

$$G_1 \triangleright G_{21} \triangleright \cdots \triangleright G_{2r} = G_2,$$

and so on between each pair of terms. Stringing these together gives a sequence of the desired type. ⊠

Our next result gives a converse to Lemma 4.11.

Lemma 8.8 (Kummer Theory) Let ζ be a primitive n^{th} root of unity, and let $K \subseteq \mathbb{C}$ be a field such that $K \supset \mathbb{Q}(\zeta)$. Suppose that L/K is a Galois extension with Galois group C_n. Then L/K is a Kummer extension—i.e. there exists $\alpha \in K$ such that

$$L = K(\sqrt[n]{\alpha}).$$

PROOF. Write $\mathrm{Gal}(L/K) = \langle\varphi\rangle$ for a choice of generator $\varphi \in \mathrm{Gal}(L/K)$.

Suppose that we could find an element $\beta \in L^\times$ such that $\varphi(\beta) = \zeta\beta$. Then:

- The elements $\varphi^i(\beta) = \zeta^i\beta$ would give n distinct elements of K. Moreover, by Theorem 3.10 (APR), these elements are roots of the minimal polynomial of β. It follows that $[K(\beta) : K] \geq n$. Since $[L : K] = n$, it follows that $L = K(\beta)$.
- We have $\varphi(\beta^n) = \varphi(\beta)^n = \beta^n$, so that $\beta^n \in L^{\{\varphi\}} = L^{\mathrm{Gal}(L/K)} = K$.

Writing $\alpha = \beta^n$, we would therefore be able to deduce that $L = K(\sqrt[n]{\alpha})$.

Hence, it is sufficient to prove that there is an element $\beta \in L^\times$ such that $\varphi(\beta) = \zeta\beta$. Equivalently, viewing φ as a K-linear map $L \to L$, it is sufficient to prove that φ has ζ as an eigenvalue.

Write μ_n for the multiplicative group of n^{th} roots of 1. Let Λ denote the set of eigenvalues of φ. It's clear that if $\Lambda \subset \mathbf{mu}_n$. Indeed, if $\lambda \in \Lambda$ has eigenvector $\beta \in L^\times$, then

$$\beta = \varphi^n(\beta) = \lambda^n\beta,$$

from which it follows that $\lambda^n = 1$.

Moreover, Λ is a group under multiplication: if $\lambda_1, \lambda_2 \in \Lambda$, and λ_i has eigenvector β_i, then because φ is also a field homomorphism,

$$\varphi(\beta_1\beta_2^{-1}) = \varphi(\beta_1)\varphi(\beta_2)^{-1} = \lambda_1\lambda_2^{-1}(\beta_1\beta_2^{-1}),$$

so that $\lambda_1\lambda_2^{-1} \in \Lambda$.

The subgroups of μ_n are exactly the groups μ_d for $d \mid n$. Suppose that $\Lambda = \mu_d$ for some $d \mid n$. Since $\varphi^n = 1$, φ is diagonalisable. And since $\Lambda = \mu_d$, then φ^d is a diagonalisable linear map with eigenvalues all 1. So $\varphi^d = 1$. Hence, we must have $d = n$. The result follows. ⊠

Theorem 8.9 *Let $f \in K[x]$. If $\mathrm{Gal}(f/K)$ is soluble, then f is soluble by radicals.*

PROOF. Write L for the splitting field of f. By the assumption that $\mathrm{Gal}(L/K)$ is soluble combined with Lemma 13.3, we can find

$$\mathrm{Gal}(L/K) = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

such that G_i/G_{i+1} is cyclic of order n_i. Applying the fundamental theorem of Galois theory, we can find

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

such that $\mathrm{Gal}(K_i/K_{i+1}) = G_i/G_{i+1}$.

Let $K_i' = K_i(\zeta)$ with ζ is a primitive $\prod_i n_i$th root of 1. So we have

$$K \subset K(\zeta) \subset K_1(\zeta) \subset \cdots \subset K_n(\zeta) = L(\zeta).$$

Clearly $L(\zeta)$ splits f over K, so it remains to show that for each i, $K_i' = K_{i+1}'(\sqrt[n_i]{(d_i)})$ for some $d_i \in K_{i+1}'$. Now, for each i, the map

$$\mathrm{Gal}(K_i'/K_{i+1}') \to \mathrm{Gal}(K_i/K_{i+1})$$

given by $\varphi \mapsto \varphi|_{K_i}$ is an injection: by Theorem 2.5 (TPE), $K_i = K_{i+1}(\gamma)$ for some $\gamma \in K_{i+1}$, $K_i' = K_{i+1}'(\gamma)$ by definition, and hence, any $\varphi \in \mathrm{Gal}(K_i'/K_{i+1}')$ is determined by $\varphi(\gamma)$. Moreover, K_i'/K_{i+1}' is Galois, since it is the splitting field of the minimal polynomial of γ.

Hence, by Lemma 8.8, each K_i'/K_{i+1}' is a Kummer extension. The result follows. ⊠

§ 9 Polynomials again

Let $f \in K[x]$ be a polynomial of degree n and let L be its splitting field. We have already seen the following:

- The Galois group $\mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$ may be regarded as a subgroup of the symmetric group S_n (Lemma 3.16), simply by looking at the action of each automorphism on the n roots of f in L;
- f is soluble by radicals implies that $\mathrm{Gal}(f/K)$ is a soluble group (Theorem 8.4), and in Appendix C we prove the converse (Theorem 13.10);
- S_n is soluble for $n = 1, 2, 3, 4$ and is not soluble for $n \geq 5$ (Remark 7.6);
- Any subgroup of a soluble group is again soluble (Theorem 7.5(1)).

Together, these imply that any polynomial of degree up to 4 is soluble by radicals, which, of course, we saw in Chapter 1. We'll make a few remarks on the process for finding roots from a more Galois-theoretic point of view.

Later in the section, we will explain how to construct polynomials whose Galois group is S_5, and which are therefore not soluble by radicals.

Transitivity

Suppose that $f(x) \in K[x]$ is an irreducible polynomial of degree n. Then we know that $\mathrm{Gal}(f/K) \subset S_n$. But clearly, there are restrictions on what the Galois group of f can be! For example, if $\mathrm{Gal}(f/K)$ is the trivial group, then that means f must have been completely reducible. In this subsection, we will prove that the Galois group of an irreducible polynomial of degree n is a *transitive* subgroup of S_n. Roughly, this means that given any two roots of f, there is an element of the Galois group which maps the first root to the second root.

Definition 9.1 We say that a subgroup $G \subseteq S_n$ is *transitive* if for any pair i, $j \in \{1, \ldots, n\}$, there is a permutation $\rho \in G$ such that ρ maps i to j. ▲

Then we have

Proposition 9.2 Let $f \in K[x]$ have only simple roots. Then $f(x)$ is irreducible if and only if $\mathrm{Gal}(f/K)$ permutes the roots of f transitively.

Proof. First suppose f is irreducible. Let L denote a splitting field for f over K. If α and β are any two roots in L of f, then there is a K-automorphism of L mapping α to β. It follows that $\mathrm{Gal}(f/K)$ acts transitively on the roots.

Conversely, if f is reducible, and α is a root of f, let g denote the minimal polynomial of α over K. As $f(\alpha) = 0$, we have that $g|f$; further $f \neq g$ as f is reducible and g is irreducible. So $f = gh$ with $\deg h \geq 1$. By APR (Theorem 3.10), automorphisms of L permute the roots of g. So automorphisms of L can only map α to other roots of g; if β is a root of h, there is no automorphism mapping α to β. ⊠

Example 9.3 We illustrate this with one of the earlier examples. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We saw earlier that $\mathrm{Gal}(L/K) = V_4$, and computed the action of the group of the roots of $(x^2 - 2)(x^2 - 3)$ and on the roots of $x^4 - 10x^2 + 1$, the minimal polynomial of $\sqrt{2} + \sqrt{3}$. We saw that in the first case, the action was not transitive, and corresponded to the subgroup generated by $(1\ 2)$ and $(3\ 4)$, whereas in the second case, it was transitive, and corresponded to the subgroup of S_4 generated by $(1\ 2)(3\ 4)$ and $(1\ 3)(2\ 4)$. ⊠

Polynomials of degree $\leqslant 4$

Degree 1

Note that when solving an equation of degree 1 over a field K, the root also lies in K. So the splitting field of a degree 1 polynomial over K is K itself. And indeed this also follows from the Galois-theoretic observation that the Galois group $\mathrm{Gal}(f/K)$ is a subgroup of the 1-element group S_1.

Degree 2

Since the solutions to

$$x^2 + ax + b = 0$$

are

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

in general, the roots are contained in an extension of degree 2 over K, obtained by adjoining the root of the discriminant $a^2 - 4b$ to K. Again, this could have been expected from the Galois theory, as S_2 is a group with 2 elements. If the square root lies in K (equivalently, if the quadratic factors), then the splitting field is K itself, and the Galois group of the polynomial is trivial, otherwise, it has 2 elements, and is therefore cyclic.

Degree 3

Remember that we solved the cubic as follows. We started by completing the cube, replacing the variable x by $x + \frac{a}{3}$. Then

$$x^3 + ax^2 + bx + c = 0$$

may be put in the form

$$X^3 + BX + C = 0.$$

Then we wrote $X = u + v$, and derived a pair of equations

$$\begin{aligned} u^3 + v^3 + C &= 0, \\ 3uv + B &= 0. \end{aligned}$$

This led to a quadratic whose roots were u^3 and v^3:

$$y^2 + Cy - \frac{B^3}{27} = 0,$$

so u^3 and v^3 are

$$\frac{-C \pm \sqrt{C^2 + \frac{4B^3}{27}}}{2}.$$

Then u may be taken to be one of the three complex cube roots of

$$\frac{-C + \sqrt{C^2 + \frac{4B^3}{27}}}{2}$$

and the choice of v may be read off from the equation $3uv + B = 0$.

Now, suppose that we're given an irreducible polynomial $f(x) = x^3 + Bx + C \in K[x]$ of degree 3. Let's see how we can use Galois theory to rederive this method. Let L be the splitting field of f, and let $M = L(\omega)$, where ω is a primitive cubed root of 1. Then we have

$$K \subset K(\omega) \subset M.$$

We know that $\mathrm{Gal}(M/K(\omega))$ is a transitive subgroup of S_3, so is either $A_3 = \langle (123) \rangle$ or S_3. Either way, by the Galois correspondence, we can find an intermediate extension

$$K(\omega) \subset K_1 \subset M,$$

where K_1 is the fixed field M^{A_3}.

Now suppose that f has roots $\alpha_1, \alpha_2, \alpha_3 \in M$. Equating $x^3 + bx + C = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, we find that

$$\begin{aligned} 0 &= \alpha_1 + \alpha_2 + \alpha_3 \\ B &= \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 \\ C &= -\alpha_1\alpha_2\alpha_3. \end{aligned}$$

We want to find a generator for $K_1/K(\omega)$. Since $K_1 = M^{(123)}$, and (123) acts on $\{\alpha_1, \alpha_2, \alpha_3\}$, we should look for combinations of $\alpha_1, \alpha_2, \alpha_3$ which are fixed by (123). Consider the elements

$$u = \frac{1}{3}(\alpha_1 + \omega\alpha_2 + \omega^2\alpha^3)$$

$$v = \frac{1}{3}(\alpha_1 + \omega^2\alpha_2 + \omega\alpha^3)$$

in M. We will make a few observations:

- We can recover $\alpha_1, \alpha_2, \alpha_3$ from u, v. Indeed,

$$\begin{aligned}\alpha_1 &= u + v\\ \alpha_2 &= \omega^2 u + \omega v = \omega^2(u + \omega^2 v)\\ \alpha_3 &= \omega u + \omega^2 v = \omega(u + \omega v).\end{aligned}$$

- We have $(123)u = \omega u$, so that $(123)u^3 = u^3$. Hence, $u^3 \in M^{(123)} = K_1$. Similarly, $v^3 \in K_1$.

- We have

$$\begin{aligned}u^3 + v^3 = (u + v)(u + \omega v)(u + \omega^2 v) &= \alpha_1\alpha_2\alpha_3 = -C\\ uv = \frac{1}{9}(\alpha_1^3 + \alpha_2^3 + \alpha - 3^3 + (\omega + \omega^2)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)&\\ = \frac{1}{9}((\alpha_1 + \alpha_2 + \alpha_3)^3 - 3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1))&\\ = -\frac{1}{3}B.&\end{aligned}$$

  Hence u^3 and v^3 are roots of the polynomial

$$y^2 + Cy - \frac{B^3}{27} = 0.$$

We find that

$$K \subset K(\omega) \subset K(u^3) = K(\sqrt{C^2 + \frac{4B^3}{27}}) \subset K(u) = M.$$

This shows that f is soluble by radicals, as well as giving a method to solve f by finding u and v.

Degree 4

To solve the quartic we started by constructing the resolvent cubic:

$$X^4 + pX^2 + qX + r = 0,$$

we started by constructing the resolvent cubic:

$$Y^3 + 2pY^2 + (p^2 - 4r)Y - q^2 = 0.$$

The roots of this cubic were β^2, γ^2 and δ^2, where $\beta = \alpha_1 + \alpha_2$, $\gamma = \alpha_1 + \alpha_3$ and $\delta = \alpha_1 + \alpha_4$. The procedure to write down the roots of the quartic is as follows. Firstly, solve the resolvent cubic, which, as we saw above, means that we must first adjoin a square root, and then a cube root. This gives values of β^2, γ^2 and δ^2. To get the possible values of β and γ, we have to adjoin square roots of β^2 and γ^2. Then the value of δ can be read off, and the roots of the quartic can be recovered from just knowing β, γ and δ (and the fact that the sum of the roots, $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$).

Now let's see how we can rederive this from a Galois theoretic point of view. Suppose that f is irreducible. If M is the splitting field of f over K, then $\mathrm{Gal}(M/K)$ is a transitive subgroup of S_4. Moreover, S_4 is solvable, and

$$S_4 \rhd A_4 \rhd V_4 \rhd C_2 \rhd \{1\}.$$

In fact $V \lhd S_4$ and $S_4/V \cong S_3$. This suggests that we can solve f by combining the solutions of a cubic polynomial (to give the V to S_4 part) and two quadratic polynomials (to give the $\{1\}$ to C_2 to V_4 part).

Assume that K contains enough roots of unity (we need 12^{th} roots). If not, we can just add these roots to K as before. Then we can find subfields

$$K \subset M^{V_4} \subset M^{V_2} \subset M,$$

where each extension is obtained by adding an n^{th} root. Our goal is to find these generators. Note that these extensions may be trivial, depending on the Galois group of f.

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of f. As before, $\mathrm{Gal}(f/K)$ acts on the roots of f. In order to find M^{V_4}, we should look for elements of M that are fixed by $(12)(34), (13)(24), (14)(23) \in V_4$. Consider the elements

$$\begin{aligned}
\beta &= \alpha_1 + \alpha_2 = -\alpha_3 - \alpha_4 \\
\gamma &= \alpha_1 + \alpha_3 = -\alpha_2 - \alpha_4 \\
\delta &= \alpha_1 + \alpha_4 = -\alpha_2 - \alpha_3
\end{aligned}$$

As before, we can recover the α_i from β, γ, δ. For example,

$$\alpha_1 = \frac{1}{2}(\beta + \gamma + \delta).$$

In addition, for each $\varphi \in V_4$ we have $\varphi(\beta) = \pm\beta$, $\varphi(\gamma) = \pm\gamma$ and $\varphi(\delta) = \pm\delta$. Hence, $\beta^2, \gamma^2, \delta^2 \in M^{V_4}$. We can show computationally that $\beta^2, \gamma^2, \delta^2$ solve a cubic equation over K.

Hence, we can start by solving this cubic, to find the extension $K_1 = M^{V_4} = K(\beta^2, \gamma^2, \delta^2)$. In general this requires an extension of degree 6, and $\mathrm{Gal}(K_1/K) \cong S_3$. Having done this, we choose a square root β of β^2 and a square root γ of γ^2. So the field $M = K(\beta, \gamma, \delta)$, in which all the roots α_i lie, is obtained from M by adjoining two further square roots. The group $\mathrm{Gal}(M/K_1)$ is in general isomorphic to V_4. This fits in with the series

$$1 \lhd C_2 \lhd V_4 \lhd A_4 \lhd S_4;$$

solving the cubic corresponds to the group $S_4/V_4 \cong S_3$, and then the two further square roots corresponds to the group $V_4 = C_2 \times C_2$.

Insolubility of the general quintic

From the patterns emerging above, one might guess that the Galois group for the general quintic should be isomorphic to S_5, and therefore not be a soluble group. By the above, this would imply that the general quintic has no solution in terms of radicals. In fact, it is not too hard to show that the general polynomial of degree n has Galois group S_n. Here, however, we will give an explicit example of a polynomial not soluble by radicals.

We first use a group theoretical lemma.

Lemma 9.4 Let p be a prime number. Let G be a subgroup of S_p which is transitive and contains a transposition. Then $G = S_p$.

PROOF. Let $S = \{1, \ldots, p\}$, and define a relation $\sim$ on S by $i \sim j$ if and only if $i = j$ or $(i\ j) \in G$. $\sim$ is clearly reflexive and symmetric. Further, if $i \sim j$ and $j \sim k$, then either $i = j$, $i = k$ or $j = k$ (in which case it is easy to see that $i \sim k$) or $(i\ k) = (i\ j)(j\ k)(i\ j) \in G$. So $\sim$ is an equivalence relation.

If $a \in S$, denote its equivalence class by $\overline{a}$. Let $b \in S$. As G is transitive, there exists $\theta \in G$ with $\theta(a) = b$.

Let $c \in \overline{a}$. Either $c = a$ or $(a\ c) \in G$. Consider $\theta(c)$. Either $\theta(c) = \theta(a)$ or $(\theta(a)\ \theta(c)) = \theta(a\ c)\theta^{-1} \in G$.

In either case, $\theta(c) \sim b$. It follows that θ gives a bijection from the equivalence class of a to the equivalence class of b. So $|\overline{a}| = |\overline{b}|$. But S is partitioned into equivalence classes, and $|S| = p$, so either all classes have 1 element each, or there is only one class with p elements. The first case is ruled out because G contains a transposition. Thus all transpositions $(i\ j)$ lie in G. But S_p is generated by the transpositions. ⊠

Example 9.5 Let $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Then $f(x) = 0$ is not soluble by radicals over $\mathbb{Q}$. ⊠

PROOF. Note that $f'(x) = 5x^4 - 6$ and so has two real zeros. By Rolle's theorem, between any two real roots of f, there is a real root of f'. Thus f has at most three real zeros.

$f(-2) = -17$, $f(-1) = 8$, $f(1) = -2$ and $f(2) = 23$, so f has exactly three real roots.

Let $G = \mathrm{Gal}(f/\mathbb{Q})$. f is irreducible by Eisenstein ($p = 3$), so G acts transitively on the roots of f (by Proposition 9.2). Also, complex conjugation fixes the three real roots amd interchanges the other two, so G contains a transposition. By the lemma, $G = S_5$. Thus f is not soluble in radicals. ⊠

Note that the same argument shows the following: suppose $f(x) \in \mathbb{Q}[x]$ is a polynomial such that

- $\deg f = p$, a prime at least 5,
- f is irreducible over $\mathbb{Q}$,
- f has $p - 2$ real roots, and one pair of complex conjugate roots.

Then f is not soluble by radicals over $\mathbb{Q}$.

For this, the second and third hypotheses show that $\mathrm{Gal}(f/\mathbb{Q})$ is a transitive subgroup of S_p which contains a transposition. Given that p is prime, the lemma now implies that $\mathrm{Gal}(f/\mathbb{Q}) = S_p$. As $p \geq 5$, we know that S_p is not a soluble group, and we conclude that f is not soluble by radicals.

(Note that it is important that p be prime – the polynomial $x^4 - 2$ is irreducible over $\mathbb{Q}$, and has two real roots and one pair of complex conjugate roots, but its Galois group is D_4, not S_4.)

§ 10 Some extensions of small degree

Proposition 10.1 Let K be a field and let L be an extension of K of degree two.

(a) There is an element $\alpha \in L \setminus K$ such that $L = K(\alpha)$ and $\alpha^2 \in K$.

(b) The element α has the following uniqueness property: if $L = K(\beta)$ for some other element $\beta \in L \setminus K$ with $\beta^2 \in K$, then $\beta = q\alpha$ for some $q \in K$.

(c) There is an automorphism $\sigma\colon\ L \to L$ that acts as the identity on K and satisfies $\sigma(\alpha) = -\alpha$.

(d) We have $\sigma^2 = 1$ and $G(L/K) = \{1, \sigma\} \simeq C_2$.

PROOF: First choose any element $\lambda \in L \setminus K$. We claim that 1 and λ are linearly independent over K. To see this, consider a linear relation $a.1 + b\lambda = 0$ with $a, b \in K$. If $b \neq 0$ we can rearrange to get $\lambda = -ab^{-1} \in K$, contrary to assumption. We therefore have $b = 0$ so the original relation reduces to $a = 0$ as required. As $\dim_K(L) = 2$ this means that $\{1, \lambda\}$ is a basis for L over K.

We can therefore write $-\lambda^2$ in terms of this basis, say as $-\lambda^2 = b\lambda + c$, or equivalently $\lambda^2 + b\lambda + c = 0$. Next put $\alpha = \lambda + b/2 \in L$. We find that $\alpha^2 = \lambda^2 + b\lambda + b^2/4 = -c + b^2/4 \in K$. By the same logic as for λ we also see that $\{1, \alpha\}$ is a basis for L and so $L = K(\alpha)$, which proves (a).

Now suppose we have another element $\beta \in L \setminus K$ with $\beta^2 \in K$. We can write $\beta = x + y\alpha$ for some $x, y \in K$. As $\beta \notin K$ we have $y \neq 0$. This gives

$$\beta^2 = (x^2 + y^2 a) + 2xy\alpha,$$

which is assumed to lie in K, so we must have $2xy = 0$. As $y \neq 0$ this gives $x = 0$ and thus $\beta = y\alpha$, proving (b).

Next, as $\{1, \alpha\}$ is a basis, we can define a K-linear map $\sigma\colon\ L \to L$ by

$$\sigma(x + y\alpha) = x - y\alpha,$$

for any $x, y \in K$. This satisfies $\sigma(\sigma(x + y\alpha)) = \sigma(x - y\alpha) = x + y\alpha$, so $\sigma^2 = \mathrm{id}$. It also has $\sigma(0) = 0$ and $\sigma(1) = 1$. Now consider elements $\mu = u + v\alpha$ and $\nu = x + y\alpha$ in L. We have

$$\begin{aligned} \mu\nu &= (ux + vya) + (vx + uy)\alpha, \\ \sigma(\mu\nu) &= (ux + vya) - (vx + uy)\alpha, \\ \sigma(\mu)\sigma(\nu) &= (u - v\alpha)(x - y\alpha) = (ux + vya) - (vx + uy)\alpha = \sigma(\mu\nu), \end{aligned}$$

so σ is a field automorphism.

Now let τ be any other automorphism of L with $\tau|_K = \mathrm{id}$. Write $a = \alpha^2 \in K$. We can apply τ to the equation $\alpha^2 - a = 0$ to get $\tau(\alpha)^2 - a = 0$, or in other words $\tau(\alpha)^2 - \alpha^2 = 0$, or in other words $(\tau(\alpha) - \alpha)(\tau(\alpha) + \alpha) = 0$, so either $\tau(\alpha) = \alpha$ or $\tau(\alpha) = -\alpha$. In the first case we have $\tau = \mathrm{id}$, and in the second case we have $\tau = \sigma$. It follows that $G(L/K) = \{\mathrm{id}, \sigma\}$ as claimed. ⊠

Proposition 10.2 Let p and q be distinct prime numbers, put

$$B = \{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\} \subset \mathbb{R},$$

and let L be the span of B over $\mathbb{Q}$.

(a) The set B is linearly independent over $\mathbb{Q}$, so is a basis for L, and $[L : \mathbb{Q}] = 4$.

(b) L is a splitting field for the polynomial $(t^2 - p)(t^2 - q) \in \mathbb{Q}[t]$.

(c) There are automorphisms σ and τ of L given by

$$\sigma(w + x\sqrt{p} + y\sqrt{q} + z\sqrt{pq}) = w - x\sqrt{p} + y\sqrt{q} - z\sqrt{pq}$$
$$\tau(w + x\sqrt{p} + y\sqrt{q} + z\sqrt{pq}) = w + x\sqrt{p} - y\sqrt{q} - z\sqrt{pq}.$$

(d) We have $\sigma^2 = \tau^2 = 1$ and $\sigma\tau = \tau\sigma$, and $G(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \simeq C_2 \times C_2$.

PROOF: For part (a), consider a nontrivial linear relation $w + x\sqrt{p} + y\sqrt{q} + z\sqrt{pq} = 0$. Here $w, x, y, z \in \mathbb{Q}$, but after multiplying through by a suitable integer we can clear the denominators and so assume that $w, x, y, z \in \mathbb{Z}$. We can then divide through by any common factor and thus assume that $\gcd(w, x, y, z) = 1$. Now rearrange the relation as $w + x\sqrt{p} = -(y + z\sqrt{p})\sqrt{q}$ and square both sides to get

$$(w^2 + px^2) + 2wx\sqrt{p} = (y^2 + pz^2)q + 2yzq\sqrt{p}.$$

We know that 1 and $\sqrt{p}$ are linearly independent over $\mathbb{Q}$, so we conclude that

$$wx = yzq,$$
$$w^2 + px^2 = (y^2 + pz^2)q.$$

From the first of these we see that either w or x is divisible by q. In either case we can feed this fact into the second equation to see that w^2 and x^2 are both divisible by q, so w and x are both divisible by q, say $w = qw'$ and $x = qx'$. We can substitute these in the previous equations and cancel common factors to get

$$yz = w'x'q$$
$$y^2 + pz^2 = (w'^2 + px'^2)q.$$

The same logic now tells us that y and z are both divisible by q, contradicting the assumption that $\gcd(w,x,y,z) = 1$. It follows that there can be no such linear relation, which proves (a).

For (b), the main point to check is that L is actually a subfield of $\mathbb{R}$. To see this, write $e_0 = 1$, $e_1 = \sqrt{p}$, $e_2 = \sqrt{q}$ and $e_3 = \sqrt{pq}$. By a straightforward check of the 16 possible cases, we see that $e_i e_j$ is always a rational multiple of e_k for some k (for example $e_1 e_3 = p e_2$). In particular, we have $e_i e_j \in L$. Now suppose we have two elements $x, y \in L$, say $x = \sum_{i=0}^3 x_i e_i$ and $y = \sum_{j=0}^3 y_j e_j$. Then $xy = \sum_{i,j} x_i y_j e_i e_j$ with $x_i y_j \in \mathbb{Q}$ and $e_i e_j \in L$, and L is a vector space over $\mathbb{Q}$, so $xy \in L$. We therefore see that L is a subring of $\mathbb{R}$. As L is finite-dimensional it follows that L is a subfield of $\mathbb{R}$. It is clearly generated by the roots of the polynomial

$$f(t) = (t^2 - p)(t^2 - q) = (t - \sqrt{p})(t + \sqrt{p})(t - \sqrt{q})(t + \sqrt{q}),$$

so it is a splitting field for $f(t)$.

Next, we can regard L as a degree two extension of $\mathbb{Q}(\sqrt{q})$ obtained by adjoining a square root of p. Proposition 10.1 therefore gives us an automorphism σ of L that acts as the identity on $\mathbb{Q}(\sqrt{q})$, and this is clearly described by the formula stated above. Similarly, we obtain the automorphism τ by regarding L as $\mathbb{Q}(\sqrt{p})(\sqrt{q})$ rather than $\mathbb{Q}(\sqrt{q})(\sqrt{p})$. This proves (c).

Now let θ be an arbitrary automorphism of L (which automatically acts as the identity on $\mathbb{Q}$). We must then have $\theta(\sqrt{p})^2 = \theta(\sqrt{p}^2) = \theta(p) = p$, so $\theta(\sqrt{p}) = \pm\sqrt{p}$. Similarly we have $\theta(\sqrt{q}) = \pm\sqrt{q}$, and it follows by inspection that there is a unique automorphism $\varphi \in \{1, \sigma, \tau, \sigma\tau\}$ that has the same effect on $\sqrt{p}$ and $\sqrt{q}$ as θ. This means that the automorphism $\psi = \varphi^{-1}\theta$ has $\psi(\sqrt{p}) = \sqrt{p}$ and $\psi(\sqrt{q}) = \sqrt{q}$, and therefore also $\psi(\sqrt{pq}) = \psi(\sqrt{p})\psi(\sqrt{q}) = \sqrt{pq}$. As B is a basis for L over $\mathbb{Q}$ and ψ acts as the identity on B, we see that $\psi = \mathrm{id}$, and so $\theta = \varphi$. This proves (d). ⊠

We next consider two different cubic equations for which the answers work out quite neatly. In a later section we will see that general cubics are conceptually not too different, although the formulae are typically less tidy.

Example 10.3 We will construct and study a splitting field for the polynomial $f(x) = x^3 - 3x - 3 \in \mathbb{Q}[x]$. This is an Eisenstein polynomial for the prime 3, so it is irreducible over $\mathbb{Q}$. We start by noting that $(3+\sqrt{5})/2$ is a positive real number, with inverse $(3-\sqrt{5})/2$. We let β denote the real cube root of $(3+\sqrt{5})/2$, so that β^{-1} is the real cube root of $(3-\sqrt{5})/2$. Then put $\omega = (\sqrt{-3} - 1)/2 \in \mathbb{C}$, so $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$. Finally, put $\alpha_i = \omega^i\beta + 1/(\omega^i\beta)$ for $i = 0, 1, 2$.

We claim that these are roots of $f(x)$. Indeed, we have

$$\begin{aligned}\alpha_i^3 &= (\omega^i\beta)^3 + 3(\omega^i\beta)^2/(\omega^i\beta) + 3\omega^i\beta/(\omega^i\beta)^2 + 1/(\omega^i\beta)^3 \\ &= \beta^3 + \beta^{-3} + 3(\omega^i\beta + \omega^{-i}\beta^{-1}) \\ &= (3+\sqrt{5})/2 + (3-\sqrt{5})/2 + 3\alpha_i = 3 + 3\alpha_i,\end{aligned}$$

which rearranges to give $f(\alpha_i) = 0$ as claimed. We also note that α_0 is real, whereas α_1 and α_2 are non-real and are complex conjugates of each other. It follows that we have three distinct roots of $f(x)$, and thus that $f(x) = (x - \alpha_0)(x-\alpha_1)(x-\alpha_2)$, so the splitting field is generated by α_0, α_1 and α_2. We write L for this splitting field.

Next, note that $\overline{\omega}$ (the complex conjugate of ω) is ω^{-1}, and so $\overline{\alpha_1} = \alpha_2$ and $\overline{\alpha_2} = \alpha_1$, whereas $\overline{\alpha_0} = \alpha_0$ because α_0 is real. This means that conjugation permutes the roots α_i and so preserves L. We thus have an automorphism $\sigma\colon\ L \to L$ given by $\sigma(a) = \overline{a}$ for all $a \in L$.

We also claim that there is an automorphism ρ of L with $\rho(\alpha_0) = \alpha_1$ and $\rho(\alpha_1) = \alpha_2$ and $\rho(\alpha_2) = \alpha_0$. Indeed, part (c) of Proposition **??** tells us that there is an automorphism λ such that $\lambda(\alpha_0) = \alpha_1$. We know that λ permutes the set $R = \{\alpha_0, \alpha_1, \alpha_2\}$ of roots of $f(x)$, so it must either be the three-cycle $(\alpha_0\ \alpha_1\ \alpha_2)$ or the transposition $(\alpha_0\ \alpha_1)$. In the first case, we can just take $\rho = \lambda$; in the second, we can take $\rho = \lambda\sigma$. It is now easy to check that the set $\{1, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$ gives all six permutations of R. It follows by Proposition **??** that the Galois group $G(L/\mathbb{Q})$ is the full group $\Sigma_R \simeq \Sigma_3$.

Example 10.4 Consider the polynomial $f(x) = x^3 + x^2 - 2x - 1$. We first claim that this is irreducible over $\mathbb{Q}$. Indeed, if it were reducible we would have $f(x) = g(x)h(x)$ for some monic polynomials $g(x), h(x) \in \mathbb{Q}[x]$ with $\deg(g(x)) = 1$ and $\deg(h(x)) = 2$. Gauss' Lemma would then tell us that $g(x), h(x) \in \mathbb{Z}[x]$. This would mean that $g(x) = x - a$ for some $a \in \mathbb{Z}$, and thus $f(a) = 0$. However, we have $f(2m) = 2(4m^3 + 2m^2 - m) - 1$ and $f(2m+1) = 2(4m^3 + 8m^2 + 3m) - 1$ so $f(a)$ is odd for all $a \in \mathbb{Z}$, which is a contradiction.

We now exhibit the roots of $f(x)$. Write

$$\begin{aligned}\zeta &= \exp(2\pi i/7) = \cos(2\pi/7) + i\sin(2\pi/7) \\ \alpha &= \zeta + \zeta^{-1} = 2\cos(2\pi/7) \\ \beta &= \zeta^2 + \zeta^{-2} = 2\cos(4\pi/7) \\ \gamma &= \zeta^4 + \zeta^{-4} = 2\cos(8\pi/7).\end{aligned}$$

(Remember that $\zeta^4 = \zeta^{-3}$.) We claim that α, β and γ are roots of $f(x)$. First

calculate $f(\alpha)$. We have:

$$\begin{aligned}\alpha^3 &= \zeta^{-3} + 3\zeta^{-1} + 3\zeta + \zeta^3\\ \alpha^2 &= \zeta^{-2} + 2 + \zeta^2\\ -2\alpha &= -2\zeta^{-1} - 2\zeta\\ -1 &= -1.\end{aligned}$$

If we add together the left hand sides we get $f(\alpha)$, and if we add together the right hand sides we get $\sum_{i=-3}^{3} \zeta^i$.

Now remember that $\zeta^7 = 1$ and $\zeta \neq 1$, so

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0.$$

Dividing by ζ^3 we get $\sum_{i=-3}^{3} \zeta^i = 0$, so $f(\alpha) = 0$.

By a modification of this calculation we also have $f(\beta) = f(\gamma) = 0$.

We now have three distinct roots for the cubic polynomial $f(x)$, so we have

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma).$$

We now claim that

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta, \gamma). \tag{1}$$

First, observe that

$$\begin{aligned}\alpha^2 - 2 &= (\zeta^{-2} + 2 + \zeta^2) - 2 = \zeta^{-2} + \zeta^2 = \beta\\ \beta^2 - 2 &= (\zeta^{-4} + 2 + \zeta^4) - 2 = \zeta^{-4} + \zeta^4 = \gamma\\ \gamma^2 - 2 &= (\zeta^{-8} + 2 + \zeta^8) - 2 = \zeta^{-8} + \zeta^8 = \zeta^{-1} + \zeta = \alpha.\end{aligned}$$

The first of these shows that $\beta \in Q(\alpha)$, and so $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$. From the other equations we see that $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma)$. Altogether we have $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, which implies (1).

So $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$.

Next, Proposition **??** tells us that there is an automorphism σ of $\mathbb{Q}(\alpha)$ with $\sigma(\alpha) = \beta$. Applying σ to $\beta = \alpha^2 - 2$ we get

$$\sigma(\beta) = \sigma(\alpha^2 - 2) = \sigma(\alpha)^2 - 2 = \beta^2 - 2 = \gamma.$$

By a similar argument we have $\sigma(\gamma) = \gamma^2 - 2 = \alpha$, so σ corresponds to the three-cycle $(\alpha\ \beta\ \gamma)$. We also know that $|G(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and it follows that $G(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma, \sigma^2\} \simeq C_3$.

Example 10.5 Consider the polynomial $f(x) = x^4 - 10x^2 + 20$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion at the prime 5. This is a quadratic function of x^2, so by the usual formula it vanishes when $x^2 = (10 \pm \sqrt{100 - 4 \times 20})/2 = 5 \pm \sqrt{5}$ (and both of these values are positive real numbers). The roots of $f(x)$ are therefore α, β, $-\alpha$ and $-\beta$ where $\alpha = \sqrt{5 + \sqrt{5}}$ and $\beta = \sqrt{5 - \sqrt{5}}$. It is a special feature of this example that β can be expressed in terms of α. To see this, note that $\alpha^2 = 5 + \sqrt{5}$ and so $\alpha^4 = 30 + 10\sqrt{5}$. Then put $\beta' = \frac{1}{2}\alpha^3 - 3\alpha$ and note that

$$\alpha\beta' = \tfrac{1}{2}\alpha^4 - 3\alpha^2 = 15 + 5\sqrt{5} - 15 - 3\sqrt{5} = -2\sqrt{5}$$
$$\alpha\beta = \sqrt{(5 + \sqrt{5})(5 - \sqrt{5})} = \sqrt{5^2 - \sqrt{5}^2} = \sqrt{25 - 5} = 2\sqrt{5}.$$

This shows that $\alpha\beta' = -\alpha\beta$, so $\beta = -\beta' = -(\frac{1}{2}\alpha^3 - \alpha) \in \mathbb{Q}(\alpha)$. This shows that all roots of $f(x)$ lie in $\mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$ over $\mathbb{Q}$. By Proposition **??** there is an automorphism σ of $\mathbb{Q}(\alpha)$ with $\sigma(\alpha) = \beta$. It follows that

$$\sigma(\sqrt{5}) = \sigma(\alpha^2 - 5) = \sigma(\alpha)^2 - 5 = \beta^2 - 5 = -\sqrt{5}.$$

We now apply σ to the equation $\alpha\beta = 2\sqrt{5}$ to get $\beta\sigma(\beta) = -2\sqrt{5}$. We can then divide this by the original equation $\alpha\beta = 2\sqrt{5}$ to get $\sigma(\beta)/\alpha = -1$, so $\sigma(\beta) = -\alpha$. Moreover, as σ is a homomorphism we have $\sigma(-a) = -\sigma(a)$ for all a, so $\sigma(-\alpha) = -\beta$ and $\sigma(-\beta) = \alpha$. This shows that σ corresponds to the four-cycle $(\alpha\ \beta\ -\alpha\ -\beta)$. It follows that the automorphisms $\{1, \sigma, \sigma^2, \sigma^3\}$ are all different, but $|G(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, so we have

$$G(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3\} \simeq C_4.$$

Example 10.6 Consider the polynomial $f(x) = x^4 - 6x^2 + 2 = (x^2 - 3 - \sqrt{7})(x^2 - 3 + \sqrt{7})$, which is irreducible over $\mathbb{Q}$, by Eisenstein's criterion at the prime 2. The roots are α, $-\alpha$, β and $-\beta$, where $\alpha = \sqrt{3 + \sqrt{7}}$ and $\beta = \sqrt{3 - \sqrt{7}}$. Let K be the splitting field, which is generated by α and β. Note that this contains the elements $\sqrt{7} = \alpha^2 - 3$ and $\sqrt{2} = \alpha\beta$. We can draw the set R of roots in a square as follows:

$$\begin{array}{cc} \alpha & \beta \\ \\ -\beta & -\alpha \end{array}$$

We claim that $G(L/\mathbb{Q})$ can be identified with the group D_8 of rotations and reflections of this square. Indeed, we can define a permutation $\mu = (\alpha\ -\alpha)(\beta\ -\beta) \in \Sigma_R$, and we put $H = \{\sigma \in \Sigma_R \mid \sigma\mu\sigma^{-1} = \mu\}$. One can see that H is a proper subgroup of Σ_R containing D_8, so $|H|$ is divisible by $|D_8| = 8$ and strictly less than $|\Sigma_R| = 24$, so $|H| = 8$ and $H = D_8$. Next, if $\sigma \in G(K/\mathbb{Q})$ then σ satisfies $\sigma(-a) = -\sigma(a)$ for all $a \in K$, so we have $\sigma\mu = \mu\sigma$, so $\sigma \in H = D_8$.

It follows that $G(K/\mathbb{Q})$ is a subgroup of D_8 of order equal to $[K:\mathbb{Q}]$, so it will suffice to check that $[K:\mathbb{Q}]=8$. As $f(x)$ is irreducible we certainly have $[\mathbb{Q}(\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg(f(x))=4$ and $K=\mathbb{Q}(\alpha)(\beta)$ with $\beta^2=3-\sqrt{7}\in\mathbb{Q}(\sqrt{7})\subseteq\mathbb{Q}(\alpha)$, so $[K:\mathbb{Q}(\alpha)]$ is either 1 (if $\beta\in\mathbb{Q}(\alpha)$) or 2 (if $\beta\notin\mathbb{Q}(\alpha)$). It would be an odd coincidence if β were already in $\mathbb{Q}(\alpha)$ and the reader may wish to take it on trust that this is not the case. However, for completeness we will give a proof below. Assuming this, we have $[K:\mathbb{Q}]=[K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=8$ as required.

For the proof that $\beta\notin\mathbb{Q}(\alpha)$, we first observe that $[\mathbb{Q}(\beta):\mathbb{Q}]=4>2=[\mathbb{Q}(\sqrt{7}):\mathbb{Q}]$, so $\beta\notin\mathbb{Q}(\sqrt{7})$. Similarly, we have $\alpha\notin\mathbb{Q}(\sqrt{7})$. We also claim that $\beta/\alpha\notin\mathbb{Q}(\sqrt{7})$. Indeed, if it were we could multiply by $\alpha^2=3+\sqrt{7}\in\mathbb{Q}(\sqrt{7})$ to see that $\sqrt{2}=\alpha\beta\in\mathbb{Q}(\sqrt{7})$, which would contradict the case $(p,q)=(2,7)$ of Proposition 10.2. Now suppose (for a contradiction) that $\beta\in\mathbb{Q}(\alpha)$. We can then write $\beta=u+v\alpha$ for some $u,v\in\mathbb{Q}(\sqrt{7})$. As $\beta\notin\mathbb{Q}(\sqrt{7})$ we must have $v\neq 0$, and as $\beta/\alpha\notin\mathbb{Q}(\sqrt{7})$ we must have $u\neq 0$. We can now square the relation $\beta=u+v\alpha$ and rearrange to get $\alpha=(\beta^2-u^2-v^2\alpha^2)/(2uv)$. As $u,v,\alpha^2,\beta^2\in\mathbb{Q}(\sqrt{7})$ this gives $\alpha\in\mathbb{Q}(\sqrt{7})$, which is the required contradiction.

§ 11 The discriminant

Note that the group S_n contains a normal subgroup of index 2, namely A_n, the group of even permutations. Let's compute the extension of K corresponding to this subgroup.

Suppose that a degree n polynomial $f(x)$ splits as $\prod_{i=1}^{n}(x-\alpha_i)$ in its splitting field. Suppose all α_i are distinct (true if f is irreducible). The group S_n acts by permuting the roots (and $\mathrm{Gal}(f/K)$ is a subgroup of S_n).

We define $\Delta(f) = \prod_{i>j}(\alpha_i - \alpha_j)$.

Lemma 11.1 Suppose $\theta \in \mathrm{Gal}(f/K) \subseteq S_n$. Then

$$\theta(\Delta(f)) = \begin{cases} \Delta(f) & \text{if } \theta \text{ is an even permutation} \\ -\Delta(f) & \text{if } \theta \text{ is an odd permutation} \end{cases}$$

PROOF. This is an equivalent definition of even/odd. ⊠

Define the *discriminant*, $D(f)$, to be $\Delta(f)^2$. Then note that $\theta(D(f)) = D(f)$ for all $\theta \in \mathrm{Gal}(f/K)$ by the lemma. It follows that $D(f)$ lies in K, as it is fixed by every element of the Galois group (using Theorem 12.3).

Corollary 11.2 Let $f \in K[x]$ have only simple roots, and let L denote a splitting field. Regard $G = \mathrm{Gal}(f/K)$ as a subgroup of S_n. Then the subfield of L corresponding to the subgroup $G \cap A_n$ is $K[\Delta(f)]$. In particular,

$$G \subseteq A_n \iff \Delta(f) \in K \iff D(f) \text{ is a square in } K.$$

PROOF. As f has distinct roots, $\Delta(f) \neq 0$, and so the lemma shows that $\theta(\Delta(f)) = \Delta(f)$ if and only if $\theta \in A_n$. Thus $G \cap A_n$ is the subgroup of G corresponding to $K[\Delta(f)]$, and so

$$G \subseteq A_n \iff K[\Delta(f)] = K \iff \Delta(f) \in K.$$

⊠

Thus the Galois group $\mathrm{Gal}(f/K)$ of a polynomial f of degree d is contained in A_d, not just S_d, if and only if its discriminant is a square in K.

Corollary 11.3 Suppose $f \in K[x]$ is an irreducible cubic equation. Then

$$\mathrm{Gal}(f/K) = \begin{cases} A_3 & \text{if } D(f) \text{ is a square} \\ S_3 & \text{if not} \end{cases}$$

PROOF. Let α be a root of f. As f is irreducible, it is the minimal polynomial of α. By Theorem 2.2, $[K(\alpha) : K] = 3$. But if L is the splitting field of f, $L \supseteq K(\alpha)$,

so we conclude that $3|[L:K]$ by Theorem 2.3. Also, L/K is Galois (it's a splitting field), so $|\mathrm{Gal}(L/K)| = [L:K]$. Finally, the Galois group may be regarded as a subgroup of S_3, a group of order 6. It follows that $\mathrm{Gal}(f/K)$ is either all of S_3, or it is a subgroup of order 3 – the only such subgroup is $A_3 = \langle(1\ 2\ 3)\rangle$. By Corollary 11.2, the Galois group is A_3 precisely when $D(f)$ is a square, and is S_3 if not. ⊠

By an Exercise, the cubic $f(x) = x^3 + ax + b$ has $D(f) = -(4a^3 + 27b^2)$.

Remark 11.4 An explicit computation (or use Maple!) shows that a quartic has the same discriminant as its resolvent cubic.

Remark 11.5 We can now classify Galois groups of irreducible quartics. As the quartic is irreducible, then its Galois group is a transitive subgroup of S_4. These subgroups are known; there are 5 possibilities, namely, S_4, A_4, D_4, V_4 and C_4.

We also know that if its discriminant is a square, then its Galois group is a transitive subgroup of A_4 and must therefore be either A_4 or V_4 (the other groups all contain 4-cycles, so cannot be contained in A_4). Otherwise, its Galois group is not contained in A_4, so is one of S_4, D_4 or C_4.

Also, if its resolvent cubic is irreducible, adjoining the roots of the resolvent cubic leads to an extension of degree divisible by 3. This was the first step in constructing the splitting field of the quartic. It follows that the Galois group of the quartic must be of order divisible by 3, so must be one of S_4 or A_4. Otherwise the Galois group will be one of D_4, V_4 or C_4.

We therefore have the following classification:

$D(f)$ square?	res. cubic irred.?	Galois group
Yes	Yes	A_4
No	Yes	S_4
Yes	No	V_4
No	No	D_4 or C_4

In fact, we can distinguish between these latter two possibilities – the Galois group is D_4 if the quartic remains irreducible over the splitting field of the cubic, and is C_4 if not. In general, however, it is usually easier to compute these by hand.

We have seen examples of all of these occurring earlier in the course, or on example sheets, for polynomials over $\mathbb{Q}$. In Exercise 25, we saw that $x^4 + 8x + 12$ has irreducible resolvent cubic, but its discriminant is 576^2. Thus its Galois group is A_4. However, $x^4 + 8x - 12$ has irreducible resolvent cubic and discriminant which is not a square, so its Galois group is S_4. We have just seen that $x^4 - 10x^2 + 1$ has splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, so has Galois group V_4. Another example is provided by $x^4 + 1$, which is the cyclotomic polynomial λ_8 – recall that the Galois group of λ_n over $\mathbb{Q}$ was $U(\mathbb{Z}_n)$. We see that $U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ and that this is a group isomorphic to V_4. In §6, we found that the Galois group of $x^4 - 2$ was D_4.

Finally, the fifth cyclotomic polynomial $\lambda_5 = x^4 + x^3 + x^2 + x + 1$ has Galois group $U(\mathbb{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, which is cyclic of order 4.

Thus all five possible transitive subgroups of S_4 can occur as Galois groups of polynomials over $\mathbb{Q}$. More generally, it is conjectured that any finite group may be realised as the Galois group of some polynomial over $\mathbb{Q}$. This question is known as the "Inverse Galois Problem", and is the subject of much current research.

List of groups

This is a list of groups which will be encountered in the course. Probably you will have met them already. There will be more detail when we come to make use of them.

Cyclic groups

The cyclic group of order n, denoted C_n, is often written as

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$$

under addition mod n.

Equally often, C_n is taken to be the set of nth roots of 1 in the complex plane, under multiplication.

Symmetric groups

The symmetric group on n symbols, denoted S_n, is the group of all permutations on $\{1, 2, \ldots, n\}$ or on any other convenient set of n symbols. Note: we compose permutations from right to left as with maps in general.

Alternating groups

The alternating group on n symbols, denoted A_n, is the group of all permutations on $\{1, 2, \ldots, n\}$ (or on any other convenient set of n symbols) which have even parity.

Remember that any permutation $\sigma \in S_n$ can be written as a product of transpositions, and that the parity (even/odd) of the number of transpositions is the same for all such products.

Dihedral groups

The dihedral groups are the isometry groups of regular polygons in the plane.

We will denote the dihedral group for the n-gon by D_n. It is also sometimes denoted D_{2n}, since it has $2n$ elements.

Denote rotation through $\frac{2\pi}{n}$ by R. Then R generates a cyclic subgroup, $\{I, R, R^2, \ldots, R^{n-1}\}$. Denote reflection by F; clearly $F^2 = I$. Lastly, $FRF = R^{-1}$.