MAS 442 GALOIS THEORY
MAS 6310 ALGEBRA I

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

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://kchmackenzie.staff.shef.ac.uk/MAS442/`

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 $\mathrm{Gal}(L/K) \longrightarrow \langle\zeta\rangle$. ⊠