MA3D5 Galois theory

Miles Reid

Jan–Mar 2004
printed Nov 2004

Contents

1 The theory of equations

Summary Polynomials and their roots. Elementary symmetric functions. Roots of unity. Cubic and quartic equations. Preliminary sketch of Galois theory. Prerequisites and books.

1.1 Primitive question

Given a polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \tag{1.1}$$

how do you find its roots? (We usually assume that $a_0 = 1$.) That is, how do you find *some* solution α with $f(\alpha) = 0$. How do you find *all* solutions? We see presently that the second question is equivalent to *splitting* f, or factoring it as a product of linear factors $f = a_0 \prod_{i=1}^{n}(x - \alpha_i)$.

1.2 Quadratic equations

Everyone knows that $f(x) = ax^2 + bx + c$ has two solutions

$$\alpha, \beta = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{1.2}$$

Set $a = 1$ for simplicity. You check that

$$\alpha + \beta = -b, \quad \text{and} \quad \alpha\beta = c, \tag{1.3}$$

which gives the polynomial identity $f(x) = x + bx + c \equiv (x - \alpha)(x - \beta)$. The relations (1.3) imply that

$$\Delta(f) = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = b^2 - 4c. \tag{1.4}$$

This gives the following *derivation* of the quadratic formula (1.2): first, the argument of §1.4 below (see Corollary 1.4) proves directly the polynomial identity $x^2 + bx + c \equiv (x - \alpha)(x - \beta)$, hence equations (1.3–1.4). Thus we have an equation for $\alpha + \beta$ and for $\delta = \alpha - \beta = \sqrt{\Delta}$, that yield (1.2).

The expression $\Delta(f)$ of (1.4) is called the *discriminant* of f. Clearly, it is a polynomial in the coefficients of f, and is zero if and only if f has a repeated root. Over $\mathbb{R}$, f has two distinct real roots if and only if $\Delta > 0$, and two conjugate complex roots if and only if $\Delta < 0$. Compare Ex. 15

1.3 The remainder theorem

Theorem 1.1 (Remainder Theorem) *Suppose that $f(x)$ is a polynomial of degree n and α a quantity.*[1] *Then there exists an expression*

$$f(x) = (x - \alpha)g(x) + c,$$

where $g(x)$ is a polynomial of degree $n - 1$ and c is a constant. Moreover, $c = f(\alpha)$. In particular, α is a root of f if and only if $x - \alpha$ divides $f(x)$.

Proof The "moreover" clause follows trivially from the first part on substituting $x = \alpha$. For the first part, we use induction on n. Suppose that $f(x)$ is given by (1.1). Subtracting $a_0x^{n-1}(x-\alpha)$ from $f(x)$ kills the leading term a_0x^n of $f(x)$, so that $f_1(x) := f(x) - a_0x^{n-1}(x - \alpha)$ has degree $\leq n - 1$. By induction, $f_1(x)$ is of the form $f_1(x) = (x - \alpha)g_1(x) + \text{const.}$, and the result for f follows at once. $\square$

Corollary 1.2 *(i) Let $\alpha_1, \ldots, \alpha_k$ be distinct quantities. They are roots of $f(x)$ if and only if $f(x) = \prod_{i=1}^{k}(x-\alpha_i)g(x)$, where $g(x)$ is a polynomial of degree $n - k$.*

(ii) The number of roots of $f(x)$ is $\leq n$.

(iii) If $f(x)$ is monic (meaning that $a_0 = 1$) of degree n and has n (distinct) roots then

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \equiv \prod_{i=1}^{n}(x - \alpha_i).$$

As discussed later in the course, we can always assume that $f(x)$ of degree n has n roots (not necessarily distinct). For example, if the coefficients a_i of $f(x)$ are rational numbers, then the "fundamental theorem of algebra" implies that $f(x)$ has n complex roots α_i. The proof of the fundamental theorem is analytic, and is given in topology (winding number) or in complex analysis (contour integral).

[1] "Quantity" is explained in Exercise 2.3 below. For the moment, bear in mind the important special case $a_i \in \mathbb{Q}$ and $\alpha \in \mathbb{C}$.

1.4 Relation between coefficients and roots

This section generalises the relations (1.3). Suppose given n quantities $\alpha_1, \ldots, \alpha_n$. We eventually intend them as the n roots of a polynomial $f(x)$, but in this section we only treat them in formal identities, so that we could also think of them as independent indeterminates.

Definition 1.3 The kth *elementary symmetric function* σ_k of the α_i is defined by

$$\sigma_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \prod_{j=1}^{k} \alpha_{i_j}.$$

In other words, take the sum of all products of k distinct choices of the α_i, starting with $\alpha_1 \alpha_2 \cdots \alpha_k$. Thus

$$\begin{aligned}
\sigma_1 &= \sum_{1 \le i \le n} \alpha_i = \alpha_1 + \alpha_2 + \cdots + \alpha_n; \\
\sigma_2 &= \sum_{1 \le i < j \le n} \alpha_i \alpha_j = \alpha_1 \alpha_2 + \cdots; \\
\sigma_n &= \prod_{i=1}^{n} \alpha_i.
\end{aligned}$$

These quantities are defined in order to provide the polynomial identity

$$\prod_{i=1}^{n} (x + \alpha_i) \equiv \sum_{i=0}^{n} \sigma_{n-i} x^i.$$

Or, more relevant to our context

$$f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^{n-1} \sigma_{n-1} x + (-1)^n \sigma_n \equiv \prod_{i=1}^{n} (x - \alpha_i).$$

We set $\sigma_0 = 1$ by convention (a single choice of the empty product, if you like that kind of thing).

Corollary 1.4 *Suppose that $f(x)$ is a monic polynomial of degree n, having n roots $\alpha_1, \ldots, \alpha_n$. Then the coefficient a_k of x^{n-k} in $f(x)$ is equal to $(-1)^k$ times σ_k, the kth elementary symmetric function of the α_i.*

Theorem 1.5 (Symmetric Polynomials) *Let $P(\alpha_1, \ldots, \alpha_n)$ be a polynomial expression that is symmetric in the α_i. Then $P(\alpha_1, \ldots, \alpha_n)$ can be written as a polynomial in $\sigma_1, \ldots, \sigma_n$.*

The elementary symmetric polynomials σ_i are an important ingredient in many different areas of math, and give rise to many useful calculations.

Example 1.6 What is $\sum \alpha_i^3$? Write

$$\begin{aligned}\sigma_1^3 &= (\alpha_1 + \alpha_2 + \cdots + \alpha_n)^3 \\ &= \alpha_1^3 + 3\alpha_1^2(\alpha_2 + \cdots + \alpha_n) + 3\alpha_1(\alpha_2 + \cdots + \alpha_n)^2 + (\alpha_2 + \cdots + \alpha_n)^3 \\ &= \sum \alpha_i^3 + 3\sum_{i \neq j} \alpha_i^2 \alpha_j + 6 \sum_{i<j<k} \alpha_i \alpha_j \alpha_k.\end{aligned}$$

So what is $\sum \alpha_i^2 \alpha_j$?

$$\sigma_1\sigma_2 = (\alpha_1 + \cdots + \alpha_n)(\alpha_1\alpha_2 + \cdots) = \sum \alpha_i^2\alpha_j + 3\sum_{i<j<k} \alpha_i\alpha_j\alpha_k;$$

note the coefficient 3: each term, say $\alpha_1\alpha_2\alpha_3$ occurs as $\alpha_1(\alpha_2\alpha_3)$, $\alpha_2(\alpha_1\alpha_3)$ and $\alpha_3(\alpha_1\alpha_2)$. Thus $\sum \alpha_i^2\alpha_j = \sigma_1\sigma_2 - 3\sigma_3$, and finally

$$\sum \alpha_i^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$$

These computations get moderately cumbersome to do by hand. They provide lots of fun exercises in computer algebra (see Ex. 5 and Ex. 14).

Proof of Theorem 1.5 A polynomial is a sum of monomials $\alpha^{\underline{b}} = \prod \alpha_i^{b_i}$; introduce the *lex order* (dictionary order) on these monomials, in which

$$1 < \alpha_1 < \alpha_1^2 < \alpha_1^3 < \alpha_1^2\alpha_2 < \alpha_1\alpha_2\alpha_3 < \text{etc.}$$

More formally, write each monomial $\alpha^{\underline{b}}$ as a word

$$\underbrace{\alpha_1 \cdots \alpha_1}_{b_1} \cdot \underbrace{\alpha_2 \cdots \alpha_2}_{b_2} \cdots \underbrace{\alpha_n \cdots \alpha_n}_{b_n} \cdot 1,$$

adding 1 as an end-of-word marker, with $1 < \alpha_1 < \alpha_2 \cdots$. A word beats another if and only if it beats it the first time they differ. The *leading term*

of $P(\alpha_1, \ldots, \alpha_n)$ is its first term in lex order. Obviously, the leading term $\alpha^{\underline{b}}$ of a symmetric polynomial P has $b_1 \geq b_2 \geq \cdots \geq b_n$.

Now consider the polynomial $\sigma_1^{c_1}\sigma_2^{c_2}\cdots\sigma_n^{c_n}$. Its leading term is the product of the leading terms in each factor, that is

$$\alpha_1^{c_1+c_2+\cdots+c_n}\alpha_2^{c_2+\cdots+c_n}\cdots\alpha_n^{c_n}.$$

Thus we can hit the leading term of P by choosing $c_i = b_i - b_{i-1}$. Then P minus a scalar multiple of $\sigma_1^{c_1}\sigma_2^{c_2}\cdots\sigma_n^{c_n}$ is a symmetric polynomial that is a sum of monomials that is later in the lex order. An induction completes the proof.

1.5 Complex roots of 1

The equation $x^n = 1$ and its roots are important for several reasons. As everyone knows, its complex roots are the nth roots of unity

$$\exp\frac{2\pi ai}{n} = \cos\frac{2\pi ai}{n} + i\sin\frac{2\pi ai}{n} \quad \text{for } a = 0, \ldots, n-1.$$

These form a subgroup of the multiplicative group of complex numbers $\mu_n \subset \mathbb{C}^\times$ that is cyclic of order n, generated by $\exp\frac{2\pi i}{n}$.

Example 1.7 (Cube roots of 1) Write

$$\omega = \exp\frac{2\pi i}{3} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1 \pm \sqrt{-3}}{2}.$$

Then $\omega^3 = 1$. In fact $x^3 - 1 = (x-1)(x^2+x+1)$, with ω satisfying $\omega^2 + \omega + 1 = 0$. There are 3 complex cube roots of 1, namely $1, \omega$ and $\omega^2 = \overline{\omega}$, and the equation $\omega^2 + \omega + 1 = 0$ says that these add to 0. You can think of this geometrically (see Figure 1.1): the 3 cube roots of 1 are the vertexes of a regular triangle centred at 0.

Clearly $x^n - 1$ factors as $(x-1)(x^{n-1} + \cdots + x + 1)$; if $n = p$ is prime, it is known (and proved in §2.4 below) that the polynomial $\Phi_p = x^{p-1} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$. It is called the pth *cyclotomic polynomial*.

Definition 1.8 If n is composite, the nth roots of 1 include the mth roots for different factors $m \mid n$, satisfying $x^m = 1$. We say that α is a *primitive* nth root of unity if $\alpha^n = 1$ but $\alpha^m \neq 1$ for any $m < n$, or equivalently, if it generates the cyclic group μ_n.

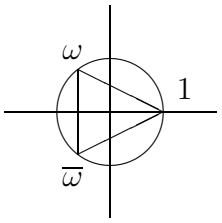


Figure 1.1: Three cube roots of 1

The primitive nth roots of 1 in $\mathbb{C}$ are $\exp \frac{2\pi a i}{n}$ with a coprime to n.

Remark 1.9 The *number* of primitive roots of 1 is given by the Euler phi function of elementary number theory:

$$\begin{aligned}\varphi(n) &= \left\{ a \in [0,n] \;\middle|\; a \text{ is coprime to } n \right\} \\ &= n \cdot \prod_{p|n} \frac{p-1}{p}.\end{aligned}$$

That is $n = \prod p_i^{a_i}$ has $\varphi(n) = \prod p_i^{a_i - 1}(p_i - 1)$.

The primitive nth roots of 1 are roots of a polynomial Φ_n, called the nth *cyclotomic polynomial* (see Ex. 4.11). It is determined by factorising $x^n - 1$ as a product of irreducible factors, then deleting any factors dividing $x^m - 1$ for some $m < n$. (See also Ex. 5.11.) We are mainly concerned with the case $n = p$ a prime, although other cases will occur as examples at several points. We finally prove that Φ_n is irreducible of degree $\varphi(n)$ in §5.7.

One reason for the importance of nth roots of 1 is as follows. Suppose that we already own a full set of nth roots of 1; equivalently, that our field contains a primitive root of unity ε, or that $x^n - 1$ splits into linear factors:

$$x^n - 1 = \prod_{a=0}^{n-1} (x - \varepsilon^a).$$

Then if we manage to find one nth root $\alpha = \sqrt[n]{a}$ of any quantity a, we automatically get all n of them without any further ado; in other words, $x^n - a$ also splits into linear factors

$$x^n - a = \prod_{a=0}^{n-1} (x - \varepsilon^a \alpha).$$

As we see many times later in the course, finding one root α of a polynomial $f(x)$ in general only allows us to pull one factor $x - \alpha$ out of f, giving $f(x) = (x - \alpha)g(x)$. It certainly happens sometimes that $g(x)$ is irreducible of degree $n - 1$ (see Example 3.23), and we have more work to do to find all the roots of f.

Example 1.10 Another reason nth roots of 1 are important is that they allow us to split an action of the cyclic group $\mathbb{Z}/n$ into eigenspaces; for simplicity consider only the case $n = 3$, which we use in our treatment of the cubic formula. (For general n, see Ex. 10.)

Consider 3 quantities α, β, γ, and the cyclic permutation $(\alpha\beta\gamma)$, that is,

$$\alpha \mapsto \beta \mapsto \gamma \mapsto \alpha. \tag{1.5}$$

Suppose that we own 3 cube roots of unity $1, \omega, \omega^2$. The trick is to shift from α, β, γ to new quantities

$$\begin{aligned} d_1 &= \alpha + \beta + \gamma, \\ d_\omega &= \alpha + \omega^2\beta + \omega\gamma, \\ d_{\omega^2} &= \alpha + \omega\beta + \omega^2\gamma \end{aligned} \tag{1.6}$$

Then the rotation $(\alpha\beta\gamma)$ leaves d_1 invariant, multiplies d_ω by ω, and d_{ω^2} by ω^2.

The quantities $d_1, d_\omega, d_{\omega^2}$ are analogues of the quantities $\alpha \pm \beta$ discussed in our treatment of the quadratic equation in §1.2: in deriving the quadratic formula (1.2) we recovered α, β by knowing $\alpha \pm \beta$ (and it is at this juncture that the denominator 2 arises). We can recover α, β, γ from $d_1, d_\omega, d_{\omega^2}$ in a similar way (see Ex. 9).

1.6 Cubic equations

A solution of certain types of general cubic equations was given by Cardano in the 16th century. The neatest way of presenting the formula is to reduce the general cubic to $x^3 + 3px + 2q$ (by a change of variable $x \mapsto x + \frac{1}{3}b$). Then the formula for the roots is

$$\sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}, \tag{1.7}$$

where the two cube roots are restricted by requiring their product to be $-p$. It works: try it and see.

For a derivation, we start by looking for 3 roots α, β, γ with

$$\left.\begin{aligned} \alpha+\beta+\gamma &= 0, \\ \alpha\beta+\alpha\gamma+\beta\gamma &= 3p, \\ \alpha\beta\gamma &= -2q. \end{aligned}\right\} \tag{1.8}$$

The trick of Example 1.10 (and its inverse Ex. 9) suggests asking for solutions in the form

$$\left.\begin{aligned} \alpha &= y+z, \\ \beta &= \omega y+\omega^2 z, \\ \gamma &= \omega^2 y+\omega z. \end{aligned}\right\} \tag{1.9}$$

If we substitute (1.9) in (1.8) and tidy up a bit, we get

$$yz=-p, \quad y^3+z^3=-2q.$$

It follows from this that y^3, z^3 are the two roots of the *auxiliary quadratic* equation

$$t^2+2qt-p^3=0.$$

Thus the quadratic formula gives

$$y^3, z^3 = -q \pm \sqrt{q^2+p^3};$$

and $yz=-p$ limits the choice of cube roots. This gives the solutions (1.7).

The quantity q^2+p^3 is (up to a factor of $2^2 3^3$) the *discriminant* of the cubic f. For its properties, see Exs. 13–15.

1.7 Quartic equations

The historical solution in this case is due to Ferrari in the 17th century. Consider the normalised equation

$$f(x)=x^4+rx^2+sx+t=0.$$

We expect 4 roots $\alpha_1, \ldots, \alpha_4$ satisfying

$$\left.\begin{aligned} \alpha_1+\alpha_2+\alpha_3+\alpha_4 &= 0, \\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4 &= r, \\ \alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4 &= -s, \\ \alpha_1\alpha_2\alpha_3\alpha_4 &= t. \end{aligned}\right\} \tag{1.10}$$

This time our gambit is to look for the 4 roots in the form

$$\left.\begin{aligned} 2\alpha_1 &= u+v+w, \\ 2\alpha_2 &= u-v-w, \\ 2\alpha_3 &= -u+v-w, \\ 2\alpha_4 &= -u-v+w. \end{aligned}\right\} \tag{1.11}$$

Substituting (1.11) in (1.10) and calculating for a while gives

$$\left.\begin{aligned} u^2+v^2+w^2 &= -2r, \\ uvw &= -s, \\ u^2v^2+u^2w^2+v^2w^2 &= r^2-4t. \end{aligned}\right\} \tag{1.12}$$

As a sample calculation, write

$$\begin{aligned} 16t = 16\alpha_1\alpha_2\alpha_3\alpha_4 &= (u+v+w)(u-v-w)(-u+v-w)(-u-v+w) \\ &= (u^2-(v+w)^2)(u^2-(v-w)^2) \\ &= (u^2-v^2-w^2)^2-4v^2w^2 \\ &= (u^2+v^2+w^2)^2-4(u^2v^2+u^2w^2+v^2w^2). \end{aligned}$$

Now the first line of (1.12) translates the first term into $4r^2$, and that proves the third line of (1.12).

The equations (1.12) say that u^2, v^2, w^2 are the roots of the *auxiliary cubic*

$$T^3+2rT^2+(r^2-4t)T-s^2=0. \tag{1.13}$$

Hence we can solve the quartic by first finding the 3 roots of the cubic (1.13), then taking their square roots, subject to $uvw=-s$, and finally combining u, v, w as in (1.11). We abstain from writing out the explicit formula for the roots.

Alternative derivations of Ferrari's solution are given in Ex. 17–20.

1.8 The quintic is insoluble

In a book published in 1799, Paolo Ruffini showed that there does not exist any method of expressing the roots of a general polynomial of degree ≥ 5 in terms of radicals; Niels Henrik Abel and Evariste Galois reproved this in the 1820s. This impossibility proof is one main aim of this course.

On the face of it, the solutions to the general cubic and quartic discussed in §§1.6–1.7 seem to involve ingenuity. How can this be accommodated into a math theory? The unifying feature of the quadratic, cubic and quartic cases is the idea of *symmetry*. Think of the symmetric group S_n acting on $\alpha_1, \dots, \alpha_n$ (with $n = 2, 3, 4$ in the three cases). The aim is to break up the passage from the coefficients $a_1, \dots, a_n$ to the roots $\alpha_1, \dots, \alpha_n$ into simpler steps. However, the mechanism for doing this involves (implicitly or explicitly) choosing elements invariant under a big subgroup of S_n.

When we put together combinations of the roots, such as

$$y = \frac{1}{3}(\alpha + \omega^2\beta + \omega\gamma) \quad \text{and} \quad z = \frac{1}{3}(\alpha + \omega\beta + \omega^2\gamma)$$

in the cubic case, we are choosing combinations that behave in a specially nice way under the rotation $(\alpha\beta\gamma)$. In fact, y^3, z^3 are invariant under this rotation, and are interchanged by the transposition $(\beta\gamma)$. We conclude from this that y^3, z^3 are roots of a quadratic. Then y, z are the cube roots of y^3, z^3, and we finally recover our roots as simple combinations of y, z.

In the quartic case, we chose

$$u = \alpha_1 + \alpha_2 = -(\alpha_3 + \alpha_4), \quad v = \alpha_1 + \alpha_3 = -(\alpha_2 + \alpha_4),$$
$$w = \alpha_1 + \alpha_4 = -(\alpha_2 + \alpha_3),$$

so that

$$u^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \quad v^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), \quad w^2 = \cdots$$

These quantities are clearly invariant under the subgroup

$$H = \langle (12)(34), (13)(24) \rangle \subset S_4 \quad (H \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2),$$

and the 3 quantities u^2, v^2, w^2 are permuted by S_4. Thus again, the intermediate quantities are obtained implicitly or explicitly by looking for invariants under a suitable subgroup $H \subset S_n$. The fact that the intermediate roots are permuted nicely by S_n is closely related to the fact that H is a normal subgroup of S_n.

Sketch of Galois theory

In a nutshell, Galois theory says that reducing the solution of polynomial equations to a simpler problem is equivalent to finding a normal subgroup

of a suitable permutation group. At the end of the course we will do some rather easy group theory to show that the symmetric group S_n for $n \geq 5$ does not have the right kind of normal subgroups, so that a polynomial equation cannot in general be solved by radicals.

To complete the proof, there are still two missing ingredients: we need to give intrinsic meaning to the groups of permutation of the roots $\alpha_1, \ldots, \alpha_n$ in terms of symmetries of the field extension $k \subset K = k(\alpha_1, \ldots, \alpha_n)$. And we need to get some practice at impossibility proofs.

Concrete algebra versus abstract algebra

Galois theory can be given as a self-contained course in abstract algebra: field extensions and their automorphisms (symmetries), group theory. I hope to be able to shake free of this tradition, which is distinctly old-fashioned. My aim in this section has been to show that much of the time, Galois theory is closely related to concrete calculations. Beyond that, Galois theory is an important component of many other areas of math beyond field theory, including topology, number theory, algebraic geometry, representation theory, differential equations, and much besides.

1.9 Prerequisites and books

Prerequisites This course makes use of most of the undergraduate algebra course. Linear algebra: vector spaces, dimension, basis. Permutation groups, abstract groups, normal subgroups, cosets. Rings and fields: ideals, quotient rings, prime and maximal ideals; division with remainder, principal ideal domains, unique factorisation. None of this should cause too much problem for 3rd or 4th year U. of W. students, and I will in any case go through most of the necessary stuff briefly.

Books These lecture notes are largely based on the course as I gave it in 1979, 1980, 1985 and 2003. Other sources

IT Adamson, Introduction to Field Theory, Oliver and Boyd
E Artin, Galois Theory, University of Notre Dame
DJH Garling, A course in Galois theory, CUP
IN Stewart, Galois Theory, Chapman and Hall
BL van der Waerden, Algebra (*or* Modern algebra), vol. 1
S Lang, Algebra, Springer

IR Shafarevich, Basic notions of algebra, Springer
J-P Tignol, Galois' theory of algebraic equations, World scientific

Exercises to Chapter 1

Exercises in elementary symmetric functions. Let σ_i be the elementary symmetric functions in quantities α_i as in §1.4.

1. Count the number of terms in σ_k, and use the formula

$$\prod(x+\alpha_i) = \sum \sigma_i x^{n-i}$$

to give a proof of the binomial theorem.

2. Express in terms of the σ_i each of the following: $\sum_i \alpha_i^2$, $\sum_{i,j} \alpha_i^2\alpha_j$, $\sum_{i<j} \alpha_i^2\alpha_j^2$.

3. If $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ has roots $\alpha_1, \ldots, \alpha_n$, use elementary symmetric functions to find the polynomial whose roots are $c\alpha_1, c\alpha_2, \ldots, c\alpha_n$. Say why the result is not surprising.

4. Use elementary symmetric polynomials to find the polynomial whose roots are $1/\alpha_1, \ldots, 1/\alpha_n$. Check against common sense.

5. Write $\Sigma_k = \sum \alpha_i^k$ for the power sum. Compute Σ_k for $k = 4, 5$. Do it for $k = 6, 7, \ldots$ if you know how to use Maple or Mathematica.

6. Prove Newton's rule

$$\Sigma_k - \sigma_1\Sigma_{k-1} + \sigma_2\Sigma_{k-2} - \cdots + (-1)^{k-1}\sigma_{k-1}\Sigma_1 + (-1)^k k\sigma_k = 0.$$

This can be viewed as a recursive formula, expressing the power sums Σ_i in terms of the elementary symmetric functions σ_i, or vice versa. Note that the resulting formula gives Σ_k as a combination of the σ_i with integer coefficients, whereas the inverse formula for σ_k in terms of the Σ_k has $k!$ as denominator.

Roots of 1

7. For p a prime, write down all the pth roots of 1 (see Definition 1.8), and calculate the elementary symmetric functions in these. Verify Corollary 1.4 in the special case $f(x) = x^p - 1$. [Hint: Start with $p = 3$ and $p = 5$ until you get the hang of it.]

8. As in Ex. 7, for p a prime, write down all the *primitive* pth roots of 1, and calculate the elementary symmetric functions in them. Verify Corollary 1.4 in the special case $f(x) = \Phi_p = x^{p-1} + \cdots + x + 1$.

9. If $d_1, d_\omega, d_{\omega^2}$ are defined as in (1.6), prove that

$$\alpha = \frac{1}{3}(d_1 + d_\omega + d_{\omega^2}), \quad \beta = \frac{1}{3}(d_1 + \omega d_\omega + \omega^2 d_{\omega^2}),$$

and similarly for γ.

10. Generalise the argument of Example 1.10 to the cyclic rotation of n objects $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ in the presence of a primitive nth root of 1.

Elementary symmetric functions and the cubic §§1.4–1.6

11. Suppose that $n = 3$; find the polynomial whose roots are $\alpha^2, \beta^2, \gamma^2$.

12. Let $n = 3$ and let ω be a primitive cube root of 1 as in §1.5. Study the effect of permuting α, β, γ on the quantities

$$\alpha + \omega\beta + \omega^2\gamma \quad \text{and} \quad \alpha + \omega^2\beta + \omega\gamma,$$

and deduce that their cubes are invariant under the 3-cycle $(\alpha\beta\gamma)$. Use elementary symmetric functions to find the quadratic polynomial whose two roots are

$$(\alpha + \omega\beta + \omega^2\gamma)^3 \quad \text{and} \quad (\alpha + \omega^2\beta + \omega\gamma)^3.$$

Use this to redo the solution of the cubic in §1.6.

13. Draw the graph $y = f(x) = x^3 + 3px + 2q$, identifying its max and min; show that y is a monotonic function of x if and only if $p \geq 0$, and that f has 3 distinct real roots if and only if $p < 0$, $f(-\sqrt{-p}) > 0$ and $f(\sqrt{-p}) < 0$. Use this to prove that the cubic f has 3 distinct real roots if and only if $\Delta = -2^2 3^3(p^3 + q^2) > 0$.

14. Study the effect of permuting the 3 quantities α, β, γ on the expression

$$\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha);$$

deduce that $\Delta = \delta^2$ is a symmetric function of the α_i. Its expression in terms of the elementary symmetric functions is

$$\Delta = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2.$$

(this computation is long, but rather easy in computer algebra – try it in Maple or Mathematica). In particular, deduce that if α, β, γ are the 3 roots of $x^3 + 3px + 2q$ then $\Delta = -2^2 3^3(p^3 + q^2)$.

15. A polynomial $f(x)$ of degree n has a repeated factor if and only if it f and $f' = \frac{\mathrm{d}f}{\mathrm{d}x}$ have a common factor, which happens if and only if the $2n - 1$ polynomials

$$f, xf, \ldots, x^{n-2}f, f', xf', \ldots, x^{n-1}f'$$

are linearly dependent in the vector space of polynomials of degree $2n - 2$. Calculate the determinants

$$\det \begin{vmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2 & b \end{vmatrix} \quad \text{and} \quad \det \begin{vmatrix} 1 & 0 & 3p & 2q & 0 \\ 0 & 1 & 0 & 3p & 2q \\ 3 & 0 & 3p & 0 & 0 \\ 0 & 3 & 0 & 3p & 0 \\ 0 & 0 & 3 & 0 & 3p \end{vmatrix}$$

to rediscover the discriminants of the quadratic $x^2 + bx + c$ of §1.2 and cubic $x^3 + 3px + q$ of §1.6.

16. Show that in the case that all 3 roots α, β, γ are real, the "solution by radicals" in §1.6 involves complex quantities.

17. Write a notional or actual computer program to compute all real roots of a cubic polynomial (by iteration of the Newton–Ralphson formula).

Elementary symmetric functions and the quartic §1.7

18. Suppose that $n = 4$ and that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$. Use symmetric functions to find the cubic equation whose 3 roots are

$$-(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \quad -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), \quad -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_4).$$

Redo the solution of the quartic in §1.7 using this.

19. Let $Q = y^2 + ry + sx + t$ and $Q_0 = y - x^2$; suppose that the two parabolas $(Q = 0)$ and $(Q_0 = 0)$ meet in the 4 points $P_i = (a_i, a_i^2)$ for $i = 1, \ldots, 4$ (see Figure 1.2) Show that the line $L_{ij} = P_iP_j$ is given by

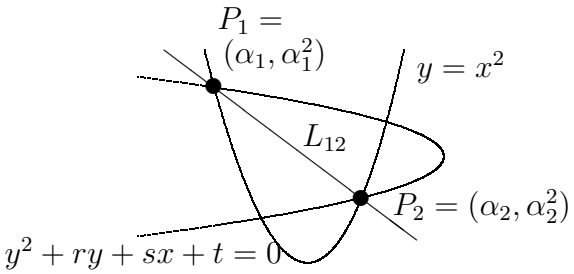


Figure 1.2: Intersection of two plane conics $Q \cap Q_0$ and reduction of the quartic

$$L_{ij} : y = (a_i + a_j)x - a_ia_j,$$

and that the reducible conic $L_{12} + L_{34}$ by

$$y^2 + (a_1a_2 + a_3a_4)y + (a_1 + a_2)(a_3 + a_4)x^2 + sx + t = 0,$$

that is, by $Q - (a_1 + a_2)(a_3 + a_4)Q_0 = 0$. Deduce that the 3 values of μ for which the conic $Q + \mu Q_0$ breaks up as a line pair are

$$-(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \quad -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), \quad -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_4).$$

20. It is known that

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$$

is a singular conic if and only if

$$\det \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} = 0$$

Use this to give a derivation of the auxiliary cubic that does not involve computing any symmetric functions.

2 Rings and fields

Summary Reminder of rings, fields, field of fractions, ideals and quotient rings. The standard map $\mathbb{Z} \to A$, characteristic and prime subfield of a field k. Polynomial ring $k[x]$, division with remainder; field extensions $k \subset K$, the minimal polynomial of $\alpha \in K$, primitive extensions. Factorisation in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$, Gauss' lemma. Eisenstein's irreducibility criterion; the cyclotomic polynomials Φ_p and Φ_{p^2} are irreducible.

2.1 Definitions and elementary properties

Some simple reminders and remarks on rings, fields, ideals, etc. You will not actually go far wrong if you assume throughout that every ring is a subring of the complex numbers, in which case many of the definitions are superfluous or simplify.

Definition 2.1 (Ring) In this course, *ring* always means "commutative ring with a 1". So a ring A is a set with two binary operations, addition $+$ and multiplication $\cdot$, with given neutral elements 0 and 1 (sometimes 0_A and 1_A to avoid ambiguity), satisfying

(i) Under addition, A an Abelian group with neutral element 0.

(ii) Multiplication has neutral element 1; is associative: $(ab)c = a(bc)$; and commutative: $ab = ba$.

(iii) Multiplication is distributive over addition: $a(b + c) = ab + ac$.

Definition 2.2 (Integral domain, field) A ring A is an *integral domain* if $0_A \neq 1_A$ and $a \neq 0, b \neq 0$ implies that $ab \neq 0$.

A ring A is a *field* if $A \setminus 0$ is a group under multiplication. This just means that any nonzero $a \in A$ has a multiplicative inverse a^{-1} with $aa^{-1} = 1_A$. (We usually write $k = A$ for a field.)

Clearly, a field is an integral domain.

Exercise 2.3 Analyse the proof of the Remainder Theorem 1.1 and Corollary 1.2 to check that they work provided that all the "quantities" involved are elements of an integral domain A. They fail over a noncommutative ring: for example, there are infinitely many roots of $x^2 = -1$ in the quaternions;

but where does the proof go wrong? They also fail over commutative rings with zerodivisors: find a counterexample.

Proposition 2.4 (Field of fractions) *Given an integral domain A, there exists a field $k = \operatorname{Frac} A$ and an embedding $A \hookrightarrow k$, with every element $c \in k$ a quotient $c = a/b$ of $a, b \in A$ and $b \neq 0$. The field k and the embedding $A \hookrightarrow k$ are essentially unique. $k = \operatorname{Frac} A$ is called the* field of fractions *of A.*

Proof You are supposed to know this; it is essentially the same as the construction of $\mathbb{Q}$ from $\mathbb{Z}$. We make $k = \operatorname{Frac} A$ as the set of expressions a/b with $a, b \in A$ and $b \neq 0$ up to the equivalence relation

$$\frac{a}{b} \sim \frac{a'}{b'} \iff ab' = a'b.$$

We define addition and multiplication on these fractions by the usual arithmetic formulas; we have to check that addition and multiplication respect the equivalence relation $\sim$, and that these then define operations on k that satisfy the ring axioms. k is a field, because the nonzero expression $a/b \in k$ has inverse b/a. $\square$

Definition 2.5 (Ring homomorphism) Let A and B be rings. A map $\varphi\colon A \to B$ is a *ring homomorphism* if

$$\varphi(a \pm b) = \varphi(a) \pm \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b) \quad \text{and} \quad \varphi(1_A) = 1_B.$$

Definition 2.6 (Ideal, kernel) A subset $I \subset A$ is an *ideal* of a ring A if

(i) $0 \in I$, and $a \pm b \in I$ for all $a, b \in I$;

(ii) $ab \in I$ for all $a \in A$ and $b \in I$.

Note that (i) ensures that I is a subgroup of the additive group of A, whereas (ii) means that I is closed under multiplication by any elements of A.

If $\varphi\colon A \to B$ is a ring homomorphism, its kernel $\ker \varphi$ is defined by

$$\ker \varphi = \varphi^{-1}(0) = \left\{ a \in A \;\middle|\; \varphi(a) = 0 \right\} \subset A.$$

Proposition 2.7 *(i) The kernel $\ker \varphi$ of a ring homomorphism $\varphi\colon A \to B$ is an ideal.*

(ii) Conversely, given an ideal $I \subset A$, there exists a surjective ring homomorphism $\varphi\colon A \to B$ such that $I = \ker \varphi$. The ring B and the quotient homomorphism φ are essentially unique, and we write $B = A/I$.

Proof You are again supposed to know this. The elements of B are elements of A considered modulo I, that is, modulo the equivalence relation $a \sim a' \iff a - a' \in I$. In practice this just means that you set all elements of I equal to zero. $\square$

Example 2.8 $\mathbb{Z}/n = \mathbb{Z}/(n) = \{0, 1, \dots, n-1\}$ with sum and product $i \pm j$, ij defined as operations in $\mathbb{Z}$, reduced modulo n.

Definition 2.9 (Prime and maximal ideals) An ideal $I \subset A$ is *prime* if $I \neq A$ and

$$a \notin I, b \notin I \implies ab \notin I.$$

An ideal $I \subset A$ is *maximal* if $I \neq A$, but there does not exist any intermediate ideal $I \subsetneq J \subsetneq A$.

Proposition 2.10 *Let A be a ring and $I \subset A$ an ideal.*

(i) I is prime if and only if A/I is an integral domain.

(ii) I is maximal if and only if A/I is a field.

In particular, I maximal implies that I is prime.

Proof Also supposed known. Let us do $\Rightarrow$ in (ii) as a sample. If I is maximal and $a \in A \setminus I$, it follows that the ideal (I, a) is the whole of A; in particular, it contains 1_A. This means that $1_A = f + ab$ for some $f \in I$ and some $b \in A$. Now go down to A/I, and write $\overline{a}, \overline{b}$ for the images of $a, b \in A$. Then $1_A = f + ab$ gives $\overline{a}\overline{b} = 1 \in A/I$. But $\overline{a}$ is an arbitrary element of A/I, so this proves that A/I is a field.

Example 2.11 Let $A = \mathbb{R}[x]$, $I = (x^2 + 1)$, and write $\overline{x}$ for the image of x in A/I. Then any element of A/I is of the form $a + bx$ with $a, b, \in \mathbb{R}$, and we calculate

$$(a + b\overline{x})(a - b\overline{x}) = a^2 - b^2\overline{x}^2 = (a^2 + b^2) - b^2(1 + \overline{x}^2) = (a^2 + b^2) \in A/I.$$

Therefore $(a + b\overline{x})^{-1} = \frac{a - b\overline{x}}{a^2 + b^2}$ in A/I for any nonzero $a + b\overline{x}$. (Of course, you know that $A/I = \mathbb{C}$, with $\overline{x} = i$.)

2.2 Factorisation in $\mathbb{Z}$

Proposition 2.12 (Division with remainder) *Given $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist a quotient and remainder $q, r \in \mathbb{Z}$ such that*

$$a = bq + r \quad \textit{with} \quad 0 \leq r < |b|.$$

Proof We only do the case $a, b > 0$. Consider $a, a-b, a-2b$, etc. At some point this becomes negative, so that $b > r = a - bq \geq 0$. $\square$

Corollary 2.13 *If $I \subset \mathbb{Z}$ is an ideal then $I = (a)$ for some $a \in \mathbb{Z}$ (and we can assume $a \geq 0$).*

Proof If $I = 0$ there is nothing to prove. Let $0 \neq b \in I$, and say $b > 0$. Pick the smallest element of $I \cap (0, b]$, say a. Then $a \in I$, and $|a|$ is the smallest for all $0 \neq a \in I$. Then for any element $c \in I$, division with remainder gives

$$c = aq + r \quad \text{with} \quad 0 \leq r < a.$$

But $r = c - aq \in I$, and by minimality of a, $r = 0$. Therefore $c \in (a)$. $\square$

Proposition 2.14 *Let $0 \neq p \in \mathbb{Z}$; then the three following conditions are equivalent:*

(i) $p \neq \pm 1$ and is irreducible (this just means that p is $\pm$ a prime number: $p = ab$ implies a or $b = \pm 1$).

(ii) The ideal (p) is prime.

(iii) The ideal (p) is maximal.

In particular, $\mathbb{F}_p = \mathbb{Z}/p$ is a field.

Proof (i) $\Rightarrow$ (iii). Suppose that p is irreducible and let I be an ideal with $(p) \subset I \subset \mathbb{Z}$. We know that $I = (a)$, so that $p = ab$. Therefore either $a = p$ and $(p) = I$, or $a = \pm 1$ and $I = \mathbb{Z}$. Therefore (p) is a maximal ideal. (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) are clear. $\square$

Proposition 2.15 *Given any ring A, there exists a unique ring homomorphism $\nu \colon \mathbb{Z} \to A$.*

Proof Included in the definition of homomorphism is the requirement that $\nu(1) = 1_A$. Thus ν is uniquely determined by

$$\nu(n) = \begin{cases} \underbrace{1+1+\cdots+1}_{n \text{ times}} & \text{if } n > 0, \\ -\nu(-n) & \text{if } n < 0. \end{cases}$$

One checks that ν so defined satisfies all the axioms for a ring homomorphism; for example, if $n, m > 0$ then

$$\nu(n)\nu(m) = \Big(\underbrace{1+1+\cdots+1}_{n \text{ times}}\Big)\Big(\underbrace{1+1+\cdots+1}_{m \text{ times}}\Big)$$

and by the distributive law in A this equals

$$\underbrace{\underbrace{1+1+\cdots+1}_{n \text{ times}} + \cdots + \underbrace{1+1+\cdots+1}_{n \text{ times}}}_{m \text{ times}} = \underbrace{1+1+\cdots+1}_{nm \text{ times}} = \nu(nm). \quad \square$$

Definition 2.16 (Characteristic, prime subfield) Let A be a ring and $\nu\colon \mathbb{Z} \to A$ the homomorphism of Proposition 2.15. The number $\operatorname{char} A = n \in \mathbb{Z}$ such that $\ker \nu = (n)$ and $n \geq 0$ is called the *characteristic* of A. We can spell this out as follows:

$$\operatorname{char} A = 0 \iff \nu \text{ is injective} \iff \mathbb{Z} \hookrightarrow A;$$

and

$$\operatorname{char} A = n > 0 \iff \underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$$

and n is minimal with this property.

Proposition 2.17 (Prime subfield) *An integral domain A either has* $\operatorname{char} A = 0$ *or* $\operatorname{char} A = p$ *a prime number (that is, $p = 2, 3, 5, 7, 11, \ldots$). Thus A contains either $\mathbb{Z}$ or $\mathbb{F}_p = \mathbb{Z}/p$ as a subring.*

A field k contains either $\mathbb{Q}$ or $\mathbb{F}_p$ as a subfield. Thus either $\operatorname{char} k = 0$ *and $\mathbb{Q} \subset k$, or* $\operatorname{char} k = p$ *and $\mathbb{F}_p \subset k$.*

Definition 2.18 The subfield $\mathbb{Q} \subset k$ or $\mathbb{F}_p \subset k$ of Proposition 2.17 is called the *prime subfield* of k. Any field can be viewed as an extension of its prime subfield.

2.3 Factorisation in $k[x]$

Definition 2.19 Let A be a ring and x an unknown (or "indeterminate", or "symbol"). A *polynomial* in x over A is a formal sum

$$f = a_m x^m + \cdots + a_1 x + a_0 \quad \text{with } a_i \in A.$$

The degree of f is defined by

$$\deg f = \begin{cases} m & \text{if } f \text{ is as above, with } a_m \neq 0; \\ 0 & \text{if } f = a_0 \neq 0, \text{ that is, } f \text{ is a nonzero constant;} \\ -\infty & \text{if } f = 0. \end{cases}$$

The set of all polynomials forms a ring, called the *polynomial ring* in x over A:

$$A[x] = \Big\{ f \;\Big|\; f \text{ is a polynomial in } x \text{ over } A \Big\}.$$

Here sum and product of $f = \sum a_i x^i$ and $g = \sum b_i x^i$ are defined by the usual rules:

$$f \pm g = \sum (a_i \pm b_i) x^i;$$
$$fg = \sum_{k=0}^{N} c_k x^k \quad \text{where } c_k = \textstyle\sum_{i+j=k} a_i b_j$$

(here $N = \deg f + \deg g$).

Proposition 2.20 *Assume that A is an integral domain; then*

(i) $\deg fg = \deg f + \deg g$*;*

(ii) $A[x]$ *is again an integral domain;*

(iii) f *is a unit of* $A[x]$ *if and only if* $\deg f = 0$ *and* a_0 *is a unit of* A*;*

(iv) There is an injective ring homomorphism $A \hookrightarrow A[x]$ *defined by* $a_0 \mapsto a_0$ *(the constant polynomial).*

Proof (i) If $f = a_m x^m + \cdots$ (lower order terms) and $g = b_n x^n + \cdots$ then $fg = a_m b_n x^{m+n} + \cdots$, and $a_m b_n \neq 0$.

(i) $\Rightarrow$ (ii) and (iii) are clear. (iv) is easy.

Proposition 2.21 (Division with remainder in $k[x]$) *Let k be a field and $f, g \in k[x]$ with $g \neq 0$. Then there exist polynomials $q, r \in k[x]$ such that*

$$f = gq + r \quad \textit{and} \quad \deg r < \deg g.$$

The Remainder Theorem 1.1 is the particular case with $g = x - \alpha$.

Proof Write $\deg f = m$, $\deg g = n$. If $m < n$ there is nothing to do: just set $q = 0$, $r = f$. So assume $m \geq n$, and prove the result by induction on m. Write

$$\begin{aligned} f &= a_m x^m + \cdots + a_1 x + a_0 \\ (a_m/b_n)x^{m-n} g &= a_m x^m + (a_m b_{n-1}/b_n)x^{m-1} + \cdots + (a_m b_0/b_n)x^{m-n}. \end{aligned}$$

Subtracting the second from the first gives

$$f_1 = f - (a_m/b_n)x^{m-n} g \quad \text{has } \deg f_1 \leq m - 1.$$

The statement holds for f_1 by induction, so that

$$f_1 = gq_1 + r \quad \text{with } \deg r < n.$$

Hence

$$f = g\big((a_m/b_n)x^{m-n} + q_1\big) + r. \quad \square$$

Definition 2.22 f is *irreducible* if f is not a unit, and $f = gh$ with $g, h \in k[x]$ implies that either g or h is a unit.

Remark 2.23 Thus $\deg f = 1$ implies that f is irreducible. For every $f \in k[x]$ there exists an expression $f = \prod g_i$ with g_i irreducible.

Corollary 2.24 *Every ideal $I \subset k[x]$ is principal, that is, $I = (f)$ for some $f \in I$.*

Proof If $I = 0$ there is nothing to prove: just set $f = 0$. If $I = 0$, let $0 \neq f \in I$ be an element of smallest degree. Then for $g \in I$, by division with remainder,

$$g = fq + r \quad \text{with } \deg r < \deg f.$$

But then $r = g - fq \in I$, so $r = 0$ by the assumption that $\deg f$ is minimal. Thus $I = (f)$. $\square$

Proposition 2.25 *Let $0 \neq f \in k[x]$; then the 3 following conditions are equivalent:*

(i) f is irreducible (that is, not a unit, and cannot be factored).

(ii) The ideal (f) is prime.

(iii) The ideal (f) is maximal.

In particular, $k[x]/(f)$ is a field.

Proof Suppose that f is irreducible and let I be an ideal with $(f) \subset I \subset k[x]$. We know that $I = (a)$ for some $a \in k[x]$, so that $f = ab$ for some $b \in k[x]$. Therefore either b is a unit and $I = (f)$, or a is a unit and $I = k[x]$. Therefore (f) is a maximal ideal. This proves (i) $\Rightarrow$ (iii).

(iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) are clear. $\square$

As usual, irreducible $\Rightarrow$ prime allows us to deduce that $k[x]$ is a UFD, so that the factorisation referred to in Remark 2.23 is unique up to units. Notice the analogy between 2.12–2.14 and 2.21–2.25, which are almost identical. The following result is an analogue of Proposition 2.15.

Theorem 2.26 *Let k be a field, $k \subset A$ a ring, and $a \in A$. Then there exists a unique homomorphism $\nu_a \colon k[x] \to A$ subject to the conditions*

(i) ν_a is the identity on k;

(ii) $\nu_a(x) = a$.

Note the difference with Proposition 2.15: because $k[x]$ contains a *variable* x, you have the freedom to specify where x is sent to. Theorem 2.26 is the basic result on which the whole of Galois theory is built. It leads at once to the key results on primitive extensions and minimal polynomials.

Proof ν is unique, because

$$\nu_a(b_m x^m + \cdots + b_1 x + b_0) = b_m a^m + \cdots + b_1 a + b_0$$

by the axioms for a ring homomorphism. In other words, this is the operation of substituting $x = a$ in a polynomial: $\nu_a(g(x)) = g(a)$. On the other hand, the same formula defines a map $\nu_a \colon k[x] \to A$ satisfying $\nu_a(b_0) = b_0$ and $\nu_a(x) = a$; you can check that ν is a ring homomorphism.

Notation

Given a subfield k of a ring A, we write $k[a]$ (note the square brackets) for the sub*ring* of A generated by k and a; in other words, $k[a]$ is the set of elements of A expressible by successively applying ring operations to a and elements of k. Clearly, $k[a] = \operatorname{im} \nu_a$, where $\nu_a \colon k[x] \to A$ is the homomorphism of Theorem 2.26. Similarly for $k[a_1, a_2]$ and so on.

Given a subfield k of a field K and $a \in K$, we write $k(a)$ (with round brackets) for the sub*field* of K generated by k and a; this is the set of elements of K expressible by successively applying ring operations to a and elements of k. The difference is that in $k(a)$ we are allowed to take quotients. Thus $k[a] \subset k(a) = \operatorname{Frac} k[a]$.

Definition 2.27 We say that a field extension $k \subset K$ is *primitive* if $K = k(a)$ for some a.

Corollary 2.28 *Suppose that k is a field, A an integral domain with $k \subset A$ and $a \in A$. Let $\nu_a \colon k[x] \to A$ be the homomorphism of Theorem 2.26.*

Then $\ker \nu_a \subset k[x]$ *is a prime ideal. There are just two cases:*

(i) *ν_a is injective; then $k[x] \cong k[a] \subset A$. If this happens, we say that a is* transcendental *over k.*

(ii) $\ker \nu_a = (f)$*, where f is an irreducible polynomial of degree ≥ 1. In this case $f(a) = 0$, and for $g \in k[x]$,*

$$\nu_a(g) = g(a) = 0 \iff f \mid g.$$

Then we say that a is algebraic *over k, and that f is the* minimal polynomial *of $a \in A$ over k.*

Note that in (ii), f is unique up to multiplication by a constant, and is actually unique if we assume that it is monic, that is, $f = x^m + \cdots + b_1 x + b_0$, with leading term 1.

Proposition 2.29 *If a is algebraic over k then $k[a] = k(a)$.*

Proof $k[a] \cong k[x]/(f)$; but $(f) \subset k[x]$ is a maximal ideal so that $k[a]$ is a field. $\square$

Example 2.30 Proposition 2.29 says that we can clear the denominator of any fraction in $k(a)$. A familiar example is operations on surds such as

$$\frac{1}{a + b\sqrt{c}} = \frac{a - b\sqrt{c}}{a^2 - b^2 c}.$$

Another example: $f = x^3 + 2x + 2$ is irreducible over $\mathbb{Q}$ and has a real root $a \in \mathbb{R}$. To express $(1 + a)^{-1}$ as an element of $\mathbb{Q}[a]$,

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

so that $(1 + a)^{-1} = a^2 - a + 3$.

In general, Proposition 2.29 means that every $0 \neq \gamma \in k[a]$ is invertible. In more detail, γ is of the form $\gamma = c_k a^k + \cdots + c_1 a + c = g(a)$, where $g(x) = c_k x^k + \cdots + c_1 x + c \in k[x]$. Then $g(a) \neq 0$ means that $g(x) \notin \ker \nu_a = (f)$; but (f) is a maximal ideal by Proposition 2.14, so that there exist $p, q \in k[x]$ such that

$$pf + qg = 1; \tag{2.1}$$

you find p, q by the Euclidean algorithm (see Ex. 12). Thus setting $\beta = \nu_a(q) = q(a) \in k[x]$ gives $\beta\gamma = p(a)f(a) + q(a)g(a) = 1$, so that $\gamma^{-1} \in k[a]$.

Remark 2.31 Theorem 2.26 is the main technical tool, and we return to it many times. We use it in the following ways:

(i) *Existence of field extension* If k is a field and $f \in k[x]$ an irreducible polynomial then there exists a field extension $k \subset K$ and $\alpha \in K$ such that $f(\alpha) = 0$. Just set $K = k[x]/(f)$ and $\alpha =$ image of x modulo (f).

(ii) *Uniqueness of field extension* If k is a field, $k \subset K$ and $k \subset L$ extension fields, with $\alpha \in K$ and $\beta \in L$ elements that are algebraic over k with the same minimal polynomial f. Then there is a unique isomorphism $k[\alpha] \cong k[\beta]$ that restricts to id_k taking $\alpha \mapsto \beta$.

(iii) *Finding all field homomorphisms* If $k \subset k[a]$ is a primitive field extension, where a is algebraic with minimal polynomial f, and $k \subset K$ is another field extension, then field homomorphisms $\varphi\colon k[a] \to K$ that restrict to id_k correspond one-to-one with roots of f in K.

Proof of (iii) If φ is a field homomorphism then

$$f(\varphi(a)) = (\varphi(a))^m + \cdots + b_1\varphi(a) + b_0 = \varphi(f(a)) = 0.$$

Thus $\varphi(a)$ is a root of f in K. Conversely, if $\beta \in K$ is a root of f in k then

$$k[a] \cong k[x]/(f) \cong k[\beta] \subset K.$$

2.4 Factorisation in $\mathbb{Z}[x]$, Eisenstein's criterion

Given $f \in k[x]$, how to determine if f is irreducible? The definition of irreducible polynomial was clear enough. However, it should be clear that we cannot expect an answer without knowing something about the field k. Here we look at $k = \mathbb{Q}$, using the fact that $\mathbb{Q} = \operatorname{Frac}\mathbb{Z}$ together with the fact that $\mathbb{Z}$ is a UFD. What we obtain is not a systematic method for studying irreducibility, rather ad hoc methods for exhibiting irreducible polynomials.

Definition 2.32 Let A be a UFD and $k = \operatorname{Frac} A$ its field of fractions (for example, $\mathbb{Z} \subset \mathbb{Q}$). A polynomial

$$g = b_n x^n + \cdots + b_1 x + b_0 \in A[x]$$

is *primitive* if $\operatorname{hcf}(b_0, \ldots, b_n) = 1$.

Proposition 2.33 *Suppose that k is the field of fractions of a UFD A. Every $f \in k[x]$ has a unique expression $f = (p/q) \cdot g$, where $g \in A[x]$ is primitive, and $p, q \in A$ have no common factor.*

Proof This is clear; multiply f through by a common numerator to obtain $Nf \in A[x]$, then divide through by the hcf of the coefficients of Nf.

Lemma 2.34 (Gauss' lemma) *Let A be a UFD and $k = \operatorname{Frac} A$.*

(i) $g, h \in A[x]$ primitive $\Rightarrow$ gh is primitive.

(ii) If $f \in A[x]$ is irreducible in $A[x]$, then it is also irreducible in $k[x]$.

Proof (i) Suppose that $p \in A$ is a prime element and set $g = b_n x^n + \cdots + b_1 x + b_0$, $h = c_m x^m + \cdots + c_1 x + c_0$. Then, since we assumed that g, h are primitive, there are $r, s \geq 0$ such that

$$\begin{aligned} p \mid b_0, b_1, \ldots, b_{r-1}, \quad p \nmid b_r, \\ p \mid c_0, c_1, \ldots, c_{s-1}, \quad p \nmid c_s, \end{aligned}$$

Therefore

$$p \nmid \text{coefft. of } x^{r+s} \text{ in } gh = \underbrace{b_{r+s}c_0 + \cdots + b_{r+1}c_{s-1}} + b_r c_s + \underbrace{b_{r-1}c_{s+1} + \cdots}$$

Thus no prime element of A divides all the coefficients of gh, so that gh is primitive.

(ii) If $f = gh$ with $g, h \in k[x]$ and $\deg g, h \geq 1$, then by the easy Proposition 2.33 applied to g and h, we get $f = (p/q)g_0 h_0$ with $g_0, h_0 \in A[x]$ primitive. Then by (i), $q = 1$, so that f is reducible in $A[x]$. $\square$

Theorem 2.35 *Let $f = a_m x^m + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Let p be a prime number and write*

$$\overline{f} = \overline{a}_m x^m + \cdots + \overline{a}_1 x + \overline{a}_0 \in \mathbb{F}_p[x]$$

for its reduction modulo p. Suppose that $\deg \overline{f} = \deg f$, or equivalently that $p \nmid a_m$. If $\overline{f}$ is irreducible over $\mathbb{F}_p$ then f is irreducible over $\mathbb{Q}$.

Proof If $f = gh$ then up to scalar multiples, we can assume that $f, g, h \in \mathbb{Z}[x]$ are all primitive. Then $\overline{f} = \overline{g}\overline{h}$, so that $\overline{f}$ is reducible over $\mathbb{F}_p$. $\square$

Theorem 2.36 (Eisenstein's irreducibility criterion) *Let A be a ring and P a prime ideal of A; write P^2 for the ideal of A generated by the products $\{pq \mid p, q \in P\}$. (In applications, $A = \mathbb{Z}$ and $P = (p)$, $P^2 = (p^2)$.) Suppose that a polynomial $f = a_m x^m + \cdots + a_1 x + a_0 \in A[x]$ satisfies*

(a) $a_m \notin P$;

(b) $a_i \in P$ for $i = 0, 1, \ldots, m-1$;

(c) $a_0 \notin P^2$.

(We call f an Eisenstein polynomial *for P.)*
Then f cannot be written $f = gh$ with $g, h \in A[x]$ with $\deg g, h \geq 1$.

Proof By contradiction, suppose that $f = gh$ with

$$g = b_r x^r + \cdots + b_1 x + b_0 \in A[x],$$
$$h = c_s x^s + \cdots + c_1 x + c_0 \in A[x].$$

Starting from the constant term, we have $a_0 = b_0 c_0 \in P \setminus P^2$, so that either $b_0 \in P$ or $c_0 \in P$, but not both. We suppose that $b_0 \in P$, and prove that by induction that $b_0, b_1, \ldots, b_r \in P$. For

$$a_k = \underbrace{b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1}_{\in P \text{ by induction}} + b_k c_0$$

Then $a_k \in P$ by the assumption on f (because $k < m$), so that $b_k c_0 \in P$; but $c_0 \notin P$, therefore $b_k \in P$. It follows that $b_0, \ldots, b_r \in P$, and therefore $a_m \in P$, contradicting (a). $\square$

Corollary 2.37 *Let $f = b_m x^m + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$ be an Eisenstein polynomial for p. Then f is irreducible in $\mathbb{Q}[x]$.*

Proof Theorem 2.36 says that f cannot be written $f = gh$ with $g, h \in \mathbb{Z}[x]$ and $\deg g, h \geq 1$. So $f = a f_0$ with f_0 irreducible and $a \in \mathbb{Z}$. Hence by Gauss' Lemma 2.34, (ii), $f \in \mathbb{Q}[x]$ is irreducible. $\square$

Example 2.38 The cyclotomic polynomial

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

is irreducible. For, set $y = x - 1$. Then

$$\Phi_p(y+1) = \frac{(y+1)^p - 1}{y} = y^{p-1} + py^{p-1} + \binom{p}{2} y^{p-3} + \cdots + \binom{p}{2} y + p$$

is an Eisenstein polynomial for p, hence is irreducible.

Example 2.39 We prove that the cyclotomic polynomial

$$\Phi_{p^2}(x) = \frac{x^{p^2} - 1}{x^p - 1}$$

is irreducible. This is the polynomial whose roots are all the primitive p^2th roots of 1. (See Definition 1.8.)

The trick is again to substitute $y = x - 1$. Then

$$(y+1)^{p^2} - 1 = \Phi_{p^2}(y+1) \cdot ((y+1)^p - 1). \tag{2.2}$$

The constant term of $\Phi_{p^2}(y+1)$ is determined by the terms in y in the two other factors: namely

$$\left.\begin{array}{l} (y+1)^{p^2} - 1 = p^2 y + \text{terms divisible by } y^2 \\ (y+1)^p - 1 = py + \text{terms divisible by } y^2 \end{array}\right\}$$
$$\Longrightarrow \Phi_{p^2}(y+1) = p + \text{terms divisible by } y.$$

Recall that $(a+b)^p \equiv a^p + b^p \mod p$ (see Ex. 1. Reducing (2.2) mod p gives

$$\text{l-h.s.} = \big((y+1)^p\big)^p - 1 \equiv (y^p + 1)^p - 1 \equiv y^{p^2},$$

and

$$\text{r-h.s.} \equiv \Phi_{p^2} \cdot y^p \mod p.$$

Hence $\Phi_{p^2} \equiv y^{p^2-p} \mod p$, so that $\Phi_{p^2}(y+1)$ is an Eisenstein polynomial, hence Φ_{p^2} is irreducible.

Exercises to Chapter 2

Exs. 1–13 are intended as revision exercises in the definitions of rings and fields.

1. Let G be a nonempty finite set having a composition law $*$ such that

   (a) $*$ is associative, and

   (b) left cancellation holds.

   Prove that G is a group. [Hint: Start by showing that $g, g^2, \ldots, g^n, \ldots$ cannot all be distinct; if $g^n = g^m$ you should be able to find an identity element in G and an inverse for g.]

2. Prove that a finite integral domain is necessarily a field.

3. Prove that an integral domain A that is a finite dimensional vector space over a subfield k is a field.

4. Let A be a ring. Show that the set A^* of 2×2 matrixes of the form

$$A^* = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in A \right\}$$

   is a ring under the ordinary matrix operations; show that A^* is isomorphic to $A[x]/(x^2 + 1)$.

5. More general, let M be any 2×2 matrix with coefficients in a ring A; show that the set of matrixes $aI + bM$ with $a, b \in A$ is a ring. [Hint: You will need to use the fact that M satisfies an equation of the form $M^2 + cM + dI = 0$ with $c, d \in A$ (an easy case of the Cayley–Hamilton theorem).]

6. Let A be a ring and $A[x]$ the polynomial ring (Definition 2.19); verify the distributive and associative laws:

$$f(g + h) = fg + fh \quad \text{and} f(gh) = (fg)h \quad \text{for all } f, g, h \in A[x].$$

7. Prove that a ring A is a field if and only if $A \neq 0$ and every ideal of A is either 0 or A.

8. Prove directly that a maximal ideal is prime. More generally, let A be a ring, $a \in A$, and set $S = \{1, a, a^2, \dots\}$. Show that if I is an ideal of A maximal among ideals disjoint from S, then I is prime. [Hint: Suppose that $b, c \in A \setminus I$; show that both (I, b) and (I, c) must intersect S, and, if $bc \in I$, derive a contradiction.]

9. Prove that if $A = \mathbb{Z}$ or $k[x]$, and f, g are coprime elements of A, then

$$A/(fg) = A/(f) \times A/(g).$$

   Now if b is an element of k, distinguish the 3 possible cases for the ring $k[x]/(x^2 - b)$.

10. Prove that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, and use this to prove that there exists a field $\mathbb{F}_4$ with 4 elements; write out its multiplication table. Similarly, show that $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$, and that there is a field $\mathbb{F}_9$ with 9 elements; show that you multiply elements of $\mathbb{F}_9$ by the familiar rule

$$(a + bi)(c + di) = ac - bd + (ad + bc)i.$$

11. Let $f, g \in k[x]$. By Corollary 2.24, the ideal (f, g) can be generated by a single element h, that we can define to be $\mathrm{hcf}(f, g)$. Verify that h has the usual properties of hcf in a unique factorisation domain.

12. Show how to obtain $h = \mathrm{hcf}(f, g)$ from f and g using the Euclidean algorithm. [Hint: Apply division with remainder $f = gq + r$ repeatedly, setting $f_1 = g$, $g_1 = r$, etc., until $r = 0$.]

13. Find the hcf of

    (a) $f = x^4 + 3x^2 + 2x + 1$ and $g = 4x^3 - 2x^2 + x + 1$;

    (b) $f = x^{2n} - 3x^2 + x + 1$ (for $n \geq 1$) and $g = x^3 - 2x^2 - x + 2$.

14. Prove that the polynomial ring $k[x]$ over any field k has infinitely many irreducible polynomials. [Hint: Imitate Euclid's proof that $\mathbb{Z}$ has infinitely many primes.]

15. Let a denote the image of x in $\mathbb{Q}[x]/(x^3 + 3x + 3)$; find each of $1/a$, $1/(1 + a)$ and $1/(1 + a^2)$ in the form $c_2a^2 + c_1a + c_0$ with $c_i \in \mathbb{Q}$.

16. Let K be a field of characteristic p. Prove that $\varphi\colon K \to K$ defined by $\varphi(a) = a^p$ is a field homomorphism. [Hint: The point to prove is that $(a+b)^p = a^p + b^p$; for this, you should prove that most of the coefficients in the binomial theorem are divisible by p.] Prove by induction that

$$(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p.$$

Deduce that $p \mid n^p - n$ for every integer n and prime p.

17. Prove that $f(x) = x^5 - x^2 + 1 \in \mathbb{F}_2[x]$ is irreducible. [Hint: if reducible, it must have a linear or quadratic factor; there are essentially only 3 or 4 possibilities; try them all.] Using Theorem 2.35, deduce that the lift $\widetilde{f} = x^5 - x^2 + 1 \in \mathbb{Q}[x]$ is also irreducible.

18. Use Eisenstein's criterion to prove that each of the following polynomials is irreducible in $\mathbb{Z}[x]$. (You will need to make a suitable change of variable of the form $y = ax + b$, then find a suitable prime p.)

    (a) $2x^4 + 15x^2 + 10$;

    (b) $x^3 - 3x^2 + 9x - 5$;

    (c) $x^5 - 5x^4 + 10x^3 - 7x^2 + 8x - 4$.

19. Prove that $x^m + 1$ is irreducible in $\mathbb{Q}[x]$ if and only if $m = 2^n$.

20. Let $A = \mathbb{Z}[i]$ be the ring of Gaussian integers, with $i^2 = -1$; let p be a prime number, and consider the ideal (p) of A. Prove that (p) is prime if and only if $p \equiv 3 \bmod 4$. [Hint: You know from number theory that if $p \equiv 1 \bmod 4$ then -1 is a quadratic residue mod p. Conversely, if $p \equiv 3 \bmod 4$, you need to show that $x^2 + 1$ is irreducible over $\mathbb{F}_p$.]

21. Let $k = \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$. Prove that there exists a homomorphism $\varphi\colon k \to k$ taking $\sqrt{2} \mapsto -\sqrt{2}$. Comment on the continuity of φ.

22. Prove that any homomorphism $\varphi\colon \mathbb{R} \to \mathbb{R}$ is the identity. [Hint: Since $\varphi(1) = 1$, you can see as in Proposition 2.15 that φ is the identity on $\mathbb{Q}$; now, how to see that φ is necessarily continuous? The trick is to find a purely algebraic property that distinguishes positive and negative real numbers, so that $a > 0$ implies that $\varphi(a) > 0$.] This result is quite curious, since there are uncountably many homomorphisms $\mathbb{C} \to \mathbb{C}$.

3 Basic properties of field extensions

Summary Definition of extension, degree $[K : k]$ of an extension, tower law for composite extensions $k \subset K \subset L$, algebraic and finite extensions. Ruler-and-compass constructions: the field $\mathbb{Q}(S)$ of a set $S \subset \mathbb{R}^2$; if S' is constructible from S by ruler-and-compass then $[\mathbb{Q}(S') : \mathbb{Q}(S)]$ is a power of 2. Impossibility of trisecting the angle, doubling the cube, squaring the circle by ruler-and-compass; regular polygons and Fermat primes. Normal extension, splitting field, existence and uniqueness of splitting field; $k \subset K$ is a splitting field of some polynomial if and only if it is finite and normal.

A finite subgroup of the multiplicative group of a field is cyclic. The finite fields (Galois fields) $\mathbb{F}_q$ for $q = p^a$. Separable polynomials; derived polynomial $f' = \frac{\mathrm{d}f}{\mathrm{d}x}$; f has a repeated root in an extension if and only if f and f' have a common factor; the discriminant $\Delta(f)$. Irreducible polynomial $f \in k[x]$ is inseparable if and only if $\operatorname{char} k = p$ and $f = g(x^p)$. The counterexample. Every extension of a finite field is separable.

3.1 Degree of extension

Any ring homomorphism $\varphi\colon k \to K$ between fields is injective:

$$0 \neq a \in k \implies \varphi(a) \cdot \varphi(a^{-1}) = \varphi(1_k) = 1_K, \quad \text{so that } \varphi(a) \neq 0.$$

Writing $\varphi(k) = k'$ gives an isomorphism $\varphi\colon k \xrightarrow{\simeq} k' \subset K$. We can for most purposes simplify the notation by identifying $k = k' \subset K$. (This assumes that we are only interested in the algebraic structure of k and K, and it may not apply if we have to worry about a priori coincidences in $k \cap K$, or about having several different $\varphi_i\colon k \to K$.)

Definition 3.1 A *field extension* is an inclusion $k \hookrightarrow K$ of k in a bigger field. Thus $k \subset K$ a field extension is synonymous with k a subfield of K. We often write K/k for a field extension. If K/k and L/k are two extensions, a field homomorphism $\varphi\colon K \to L$ is a *k-homomorphism* if $\varphi_{|k} = \mathrm{id}_k$, that is, $\varphi(a) = a$ for all $a \in k$.

Notation

If $k \subset L$ is a field extension and $S \subset L$ any subset, write $k[S]$ for the subring of L generated by k and S, and $k(S)$ for the subfield of L generated by k

and S; that is,

$$k(S) = \left\{ b \in L \;\middle|\; \begin{array}{l} b \text{ can be expressed in terms of the field oper-} \\ \text{ations } +, -, \times, \div \text{ applied to elements of } k \cup S \end{array} \right\}.$$

If $S = \{\alpha_1, \ldots, \alpha_r\}$ is a finite set, we write $k(S) = k(\alpha_1, \ldots, \alpha_r)$. In this case we can think of the extension $k \subset k(\alpha_1, \ldots, \alpha_r)$ as built up of

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_r). \tag{3.1}$$

Definition 3.2 A field extension $k \subset K$ is *finitely generated* (or f.g.) if $K = k(\alpha_1, \ldots, \alpha_r)$ for some finite set $\{\alpha_1, \ldots, \alpha_r\} \subset K$.

Recall that a field extension is *primitive* if $K = k(\alpha)$ for some $\alpha \in K$. Thus (3.1) breaks a f.g. extension up as a chain of primitive ones. Recall that we know all about primitive extensions by Proposition 2.28:

Proposition 3.3 *If $k \subset K = k(\alpha)$ is a primitive extension then* either

(a) α is transcendental over k; then $k[\alpha] \cong k[x]$, the polynomial ring in x, and $K = k(\alpha) \cong k(x)$, the field of rational functions $g(x)/h(x)$. Or

(b) α is algebraic over k with minimal polynomial $f \in k[x]$, and $K = k(\alpha) = k[\alpha] \cong k[x]/(f)$.

If $k \subset K$ is a field extension then K is a vector space over k. To spell this out, K is an Abelian group under $+$, and k acts on K by $(a, u) \mapsto au$ (for $a \in k$, $u \in K$, multiplication in K), and satisfies

$$\begin{aligned} a(b(u)) &= (ab)u \quad \text{by associativity in } K; \\ a(u+v) &= au + av \quad \text{by distributive law in } K; \\ (a+b)u &= au + bu \quad \text{ditto.} \end{aligned}$$

Definition 3.4 The *degree* $[K : k]$ of the extension $k \subset K$ is defined as $[K : k] = \dim_k K$, the dimension of K over k. This is either a natural number ≥ 1, or ∞. We say that $k \subset K$ is a *finite* extension if $[K : k] < \infty$.

Proposition 3.5 *If $k \subset K = k(\alpha)$ is a primitive extension,*

$$[K : k] = \begin{cases} \deg f & \text{if } \alpha \text{ is algebraic with minimal polynomial } f; \\ \infty & \text{if } \alpha \text{ is transcendental.} \end{cases}$$

Proof In the first case, $K \cong k[x]/(f)$, so that $1, \alpha, \ldots, \alpha^{n-1}$ base K, where $n = \deg f$. In the second case, $K \supset k[x]$, which is already infinite dimensional over k. $\square$

Theorem 3.6 (Tower law) *Let $k \subset K \subset L$ be field extensions (or we sometimes write $L/K/k$). Then*

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

(If one side is infinite then so is the other.)

Proof L is a k-vector space, and $K \subset L$ a subspace. So $\dim_k K = \infty \Rightarrow \dim_k L = \infty$. Also, if L is infinite over K, then it is certainly infinite over k. So we need only treat the case $[K : k] = m$, $[L : K] = n$. Suppose

$$u_1, \ldots, u_n \in L \text{ is a } K\text{-basis of } L; \qquad v_1, \ldots, v_m \in K \text{ is a } k\text{-basis of } K$$

I claim that $\{u_i v_j\}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ is a k-basis of L, hence $\dim_k L = mn$, as required.

They span L as k-vector space. For $x \in L$ is of the form $x = \sum_{i=1}^{n} b_i u_i$ with $b_i \in K$ (because the u_i span L over K). Next, each $b_i \in K$, so is of the form

$$b_i = \sum_{j=1}^{m} a_{ij} v_j \quad \text{with } a_{ij} \in k$$

(for a similar reason). Therefore $x = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} v_j u_i$.

Next, they are linearly independent over k by a similar argument: suppose that $\{a_{ij} \in k\}$ are coefficients of a linear relation

$$\sum_{i,j} a_{ij} u_i v_j = 0.$$

For each i, set $b_i = \sum_j a_{ij} v_j \in K$. Thus $\sum_i b_i u_i = 0$, and since $\{u_i\}$ is a K-basis of L, and $b_i \in K$, it follows that $b_i = 0$ for all i. Now $a_{ij} \in k$, and

$$\sum a_{ij} v_j = b_i = 0$$

is a linear relation between the v_j with coefficients in k. Since $\{v_j\}$ is a k-basis of K, it follows that $a_{ij} = 0$. $\square$

Definition 3.7 A field extension $k \subset K$ is *finite* if $[K : k] < \infty$. We say that K/k is finite, or K is finite over k.

$k \subset K$ is *algebraic* if every $\alpha \in K$ is algebraic over k.

A finite extension $k \subset K$ is automatically algebraic: if $\alpha \in K$ then there must be a linear dependence relation between $1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots$, so there exists $b_i \in k$ with

$$b_m \alpha^m + \cdots + b_1 \alpha + b_0 = 0.$$

Thus Theorem 3.6 has important consequences.

Corollary 3.8 *(a) Let $k \subset K$ be a field extension. If $a, b \in K$ are algebraic over k, so are $a \pm b, ab, ab^{-1}$. Therefore the subset*

$$\left\{ \alpha \in K \;\middle|\; \alpha \text{ is algebraic over } k \right\} \subset K$$

is a subfield.

(b) A field extension $k \subset K$ is finite if and only if it is algebraic and finitely generated.

Proof (a) consider the tower $k \subset k(a) \subset k(a, b)$. Then a is algebraic over k, so $k \subset k(a)$ is a finite extension. Also, b is algebraic over k, hence over $k(a)$, and so $k(a) \subset k(a, b)$ is a finite extension. By the Tower Law 3.6, $k \subset k(a, b)$ is a finite extension, so as remarked above, any $\alpha \in k(a, b)$ is algebraic over k, in particular $a \pm b, ab, ab^{-1}$.

Notice that although we have proved that $a \pm b$, etc., satisfy polynomial relations, it might be hard in practice to determine these. See Ex. 6.

(b) Assume $k \subset K$ is finite. Then it is algebraic (by the above), and f.g., because if $u_1, \ldots, u_n$ is a k-basis of K then certainly $K = k(u_1, \ldots, u_n)$. Conversely, suppose that $K = k(\alpha_1, \ldots, \alpha_n)$ is a finitely generated algebraic extension. For $i = 0, \ldots, n$, set $K_i = k(\alpha_1, \ldots, \alpha_i)$. Then

$$k = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset K_n = K.$$

Each step $K_{i-1} \subset K_i$ is a primitive extension, since $K_i = K_{i-1}(\alpha_i)$, and α_i is algebraic over K_{i-1} (because it is over k). Thus $[K_i : K_{i-1}] < \infty$. So by induction using the Tower Law 3.6, $K = K_n$ satisfies $[K : k] < \infty$. $\square$

Theorem 3.9 *Let $k \subset K \subset L$ be field extensions. If each step $k \subset K$ and $K \subset L$ are algebraic, so is $k \subset L$.*

Proof Let $\alpha \in L$. It is enough to prove that α is algebraic over k. Now since L/K is algebraic, α satisfies a polynomial equation over K

$$\alpha^n + \cdots + b_1\alpha + b_0 = 0 \quad \text{with } b_i \in K. \tag{3.2}$$

The proof takes place entirely within the f.g. extension

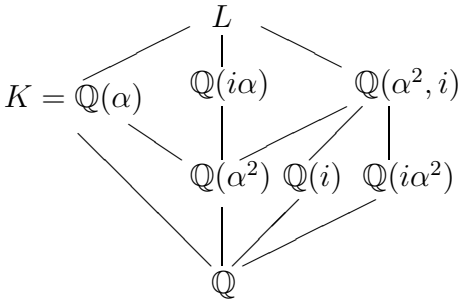
$$k \subset L_0 = k(b_0, b_1, \ldots, b_{n-1}, \alpha) \subset L,$$

and the point is that for a f.g. extension, algebraic $\Leftrightarrow$ finite. Set $K_0 = k(b_0, b_1, \ldots, b_{n-1})$, so that $L_0 = K_0(\alpha)$. Then $K_0 \subset K$, so it is algebraic over k. Also, it is f.g. over k, so by Corollary 3.8, $[K_0 : k] < \infty$. Now α satisfies the equation (3.2), which has coefficients in K_0 by construction of K_0. Hence α is algebraic over K_0, so that $[L_0 : K_0] < \infty$. Thus

$$[L_0 : k] = [L_0 : K_0][K_0 : k] < \infty.$$

Since $\alpha \in L_0$, it must be algebraic over k. $\square$

Example 3.10 $L = \mathbb{Q}(\sqrt[4]{2}, i) \subset \mathbb{C}$. Write $\alpha = \sqrt[4]{2} \in \mathbb{R}$ and $i = \sqrt{-1} \in \mathbb{C}$. Now $x^4 - 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion, hence $K = \mathbb{Q}(\alpha)$ has $[K : \mathbb{Q}] = 4$. Also $K \subset \mathbb{R}$, so that $x^2 + 1$ has no roots in K, and is hence irreducible over K. Therefore $[L : K] = [K(i) : K] = 2$. This proves $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 8$. We can write down lots of intermediate fields:



(3.3)

where each intermediate extension has degree 2 or 4. For example, in the tower

$$\mathbb{Q} \subset \mathbb{Q}(\alpha^2) \subset \mathbb{Q}(i\alpha) \subset L,$$

each step has degree ≤ 2 (because it is primitive, with generator satisfying a quadratic equation). And the product is 8, so all the degrees $= 2$.

If you write the 4 roots of $x^4 - 2$ as a regular 4-gon in $\mathbb{C}$, the set-up has symmetry the dihedral group D_8 (compare Example 4.22). We see later that D_8 is the Galois group of the extension $L/\mathbb{Q}$, and that intermediate fields $\mathbb{Q} \subset F \subset L$ are in one-to-one correspondence with subgroups of D_8. The two final subfields not given in (3.3) are $\mathbb{Q}(\frac{i\pm1}{\sqrt{2}}\alpha)$, which both have degree 4 over $\mathbb{Q}$. Note that $\pm\frac{i\pm1}{\sqrt{2}}$ are the roots of $x^4 = -1$, that is, the 4 primitive 8th roots of 1.

Example 3.11 Let $\varepsilon = \exp\frac{2\pi i}{5} \in \mathbb{C}$. Write $L = \mathbb{Q}(\varepsilon)$ and $K = \mathbb{R} \cap L$. We know by Example 2.38 that $\Phi_4 = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$, hence is the minimal polynomial of ε. Therefore $[L : \mathbb{Q}] = 4$. It looks plausible that $[L : K] = 2$ and $[K : \mathbb{Q}] = 2$. Let us prove this. First, $K \neq L$ since $K \subset \mathbb{R}$, $L \not\subset \mathbb{R}$. Thus $[L : K] \geq 2$.

Next, $\varepsilon + \varepsilon^{-1} = 2\sin\frac{2\pi}{5} \in \mathbb{R}$, hence in K so that ε satisfies the quadratic equation

$$x^2 + 1 = \alpha x, \quad \text{where } \alpha = 2\sin\tfrac{2\pi}{5} \in K.$$

Therefore $[L : K] = 2$. In fact $\alpha = \varepsilon + \varepsilon^4$ and $\varepsilon^2 + \varepsilon^3$ are the two roots of the quadratic $t^2 + t - 1 = 0$. Thus we can obtain $\sqrt[5]{1}$ by successively solving quadratics.

3.2 Applications to ruler-and-compass constructions

We show that irrational quantities obtained by ruler-and-compass constructions are contained in field extensions whose degree is a power of 2. This leads to proofs of impossibility of trisecting a general angle, or doubling the cube by ruler-and-compass, since these constructions certainly requires field extensions of degree divisible by 3. Thus the simple idea of the degree of a field extension has powerful consequence, and can solve problems that have been open since antiquity.

Definition 3.12 Let $S \subset \mathbb{R}^2$ be a finite set. We allow two constructions: given two points $P, Q \in S$,

"ruler": given two points $P, Q \in S$, join $P, Q \in S$ by a straight line PQ;

"compass": given points $P, Q_1, Q_2 \in S$, draw circle centre P, radius Q_1Q_2.

We say that a point $R \in \mathbb{R}^2$ is *1-step constructible* from S (by ruler-and-compass) if R is a point of intersection of 2 distinct curves (lines or circles) obtained from S by either of the above two constructions.

A point $R \in \mathbb{R}^2$ is *constructible* from S if there exist points $R_1, \ldots, R_n = R$ such that R_1 is 1-step constructible from S, and for each $0 \leq i \leq n-1$, R_{i+1} is 1-step constructible from $S \cup \{R_1, \ldots, R_i\}$.

Example 3.13 (a) If $S = \{P, Q, R\}$ with $R \notin PQ$. We can construct the parallelogram $QPRR'$, hence the line RR' parallel to PQ: indeed R' is the second point (other than P) such that $PQ = RR'$ and $PR = QR'$ (see Figure 3.1, (i)).

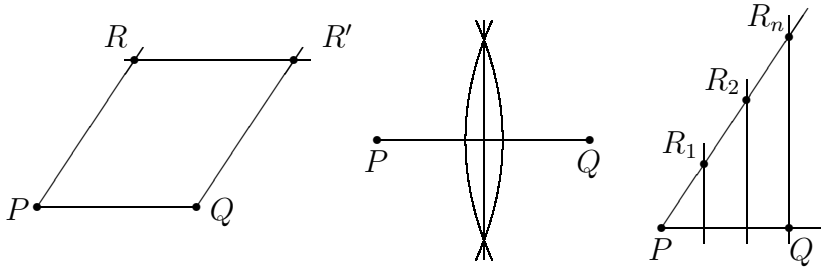


Figure 3.1: Ruler and compass constructions

(b) If $S = \{P, Q\}$, we can construct the perpendicular bisector of the line segment PQ.

(c) We can divide a line segment into n equal segments.

(d) We can bisect any angle (construct the line PR' in (i)).

Definition 3.14 Given a set of points $S \subset \mathbb{R}^2$, the *field* of S is defined to be the subfield of $\mathbb{R}$ generated by the x- and y-coordinates of all the points of S:

$$\mathbb{Q}(S) = \mathbb{Q}\Big(x_i, y_i \;\Big|\; (x_i, y_i) \in S\Big) \subset \mathbb{R}.$$

Proposition 3.15 *(i) If $R \in \mathbb{R}^2$ is 1-step constructible from S then*

$$\big[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)\big] = 1 \text{ or } 2.$$

(ii) If S' is constructible from S then $[\mathbb{Q}(S') : \mathbb{Q}(S)]$ is a power of 2.

Proof (i) R is a point of intersection of two locuses given by one of our two constructions, say

$$R = L_1 \cap L_2, \quad \text{where} \quad \begin{array}{ll} L_1: & a_1(x^2+y^2)+b_1x+c_1y+d_1=0; \\ L_2: & a_2(x^2+y^2)+b_2x+c_2y+d_2=0. \end{array}$$

with $a_1, \ldots, d_2 \in \mathbb{Q}(S)$. If $a_1 = a_2 = 0$ then R is the intersection of two lines, and the coordinates of R belong to $\mathbb{Q}(S)$, hence $\mathbb{Q}(S \cup \{R\}) = \mathbb{Q}(S)$. Otherwise $M = a_2L_1 - a_1L_2$ is a line of $\mathbb{R}^2$, given by $b_3x + c_3y + d_3 = 0$; if say $c_3 \neq 0$, substituting for y in L_1 gives a quadratic equation satisfied by the x-coordinate of R:

$$y = \frac{-d_3 + b_3x}{c_3}; \quad \lambda x^2 + \mu x + \nu \quad \text{with } \lambda, \mu, \nu \in \mathbb{Q}(S).$$

Therefore $\mathbb{Q}(S \cup \{R\}) = \mathbb{Q}(S)(x, y) = \mathbb{Q}(S)(x)$, and x satisfies a quadratic equation over $\mathbb{Q}(S)$, so that $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$ or 2, as claimed.

(ii) is clear, since if $S' = S \cup \{R_1, \ldots, R_n\}$,

$$\mathbb{Q}(S) \subset \cdots \subset \mathbb{Q}(S \cup \{R_1, \ldots, R_i\}) \subset \mathbb{Q}(S \cup \{R_1, \ldots, R_{i+1}\}) \subset \cdots \subset \mathbb{Q}(S'),$$

and by (i), each step has degree 1 or 2. Thus (ii) follows by the Tower Law 3.6 and induction. □

Corollary 3.16 *(i) Let $S = \mathbb{Q}^2 \subset \mathbb{R}^2$, so that $\mathbb{Q}(S) = \mathbb{Q}$. Then $R = (0, \sqrt[3]{2}) \in \mathbb{R}^2$ is not constructible from S. That is, the cube cannot be doubled by ruler and compass.*

(ii) Let $S = \mathbb{Q}^2 \subset \mathbb{R}^2$. Then $R = (\sin 10^\circ, \cos 10^\circ)$ is not constructible by ruler and compass from S. That is, the angle of 30° cannot be trisected by ruler and compass.

Proof (i) $Q(S \cup \{R\}) = \mathbb{Q}(\sqrt[3]{2})$. Since $x^3 - 2$ is irreducible over $\mathbb{Q}$ it follows that $[Q(S \cup \{R\}) : \mathbb{Q}] = 3$, which is not a power of 2. Thus R is not constructible.

(ii) The formula $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$ gives

$$4\sin^3 10^\circ - 3\sin 10^\circ = -\sin 30^\circ = -1/2,$$

so that $\alpha = 2\sin 10^\circ$ is a root of $f(x) = x^3 - 3x + 1$. Now f is irreducible over $\mathbb{Q}$: in fact substituting $y = x + 1$ gives

$$f(y-1) = (y-1)^3 - 3(y-1) + 1 = y^3 - 3y^2 + 3,$$

an Eisenstein polynomial for 3.

Now $\mathbb{Q}(R) \supset \mathbb{Q}(\alpha)$, and $[Q(\alpha) : \mathbb{Q}] = 3$, and thus $[\mathbb{Q}(R) : \mathbb{Q}]$ is not a power of 2. Hence R is not constructible. $\square$

Discussion $\mathbb{R}^2$ with its coordinate geometry is a model for Euclidean geometry. Two famous "unsolved problems" of Euclidean geometry were to construct a cube whose volume is twice that of a given cube: the side would have to be $\sqrt[3]{2}$ times as long, and if this could be constructed by ruler and compass then so could the point $R = (0, \sqrt[3]{2}) \in \mathbb{R}^2$, which we have proved is impossible. And to trisect any given angle; if you could trisect any angle, you must be able to trisect an angle of 30°, and we have seen this is impossible. Thus there does not exist a ruler and compass construction that trisects the angle.

Theorem 3.17 *If the regular N-gon is constructible from $\mathbb{Q}^2$ then $N = 2^a p_1 \cdots p_r$, where the p_i are distinct primes such that $p_i - 1$ is a power of 2.*

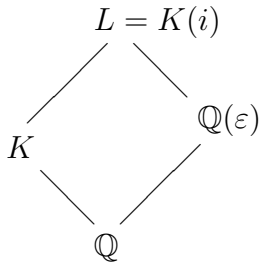
Primes of the form $p = 2^N + 1$ are called *Fermat primes*. It is known that then N itself is a power of 2, so that $p = 2^{2^n} + 1$; examples are $5, 17, 65537$. The theorem says that we can construct the regular N-gon only if any prime dividing N is either 2 or a Fermat prime p with $p^2 \nmid N$.

Proof If the regular N-gon is constructible, then so is the regular M-gon for any $M \mid N$, so I only need to prove that if p is an odd prime, and the regular p-gon is constructible, then $p - 1$ is a power of 2; and the regular p^2-gon is not constructible.

Write $P = (s, c) \in \mathbb{R}^2$ where $s = \sin \frac{2\pi}{p}$, $c = \cos \frac{2\pi i}{p}$. Let $K = \mathbb{Q}(s, c)$ and $L = K(i)$ and consider $\varepsilon = c + is \in L$. Then ε is a pth root of unity, $\varepsilon \neq 1$, and we know that ε is a root of the irreducible polynomial

$$\Phi_p = x^{p-1} + \cdots + x + 1 \in \mathbb{Q}[x].$$

Thus Φ_p is the minimal polynomial of ε over $\mathbb{Q}$. It follows that $[\mathbb{Q}(\varepsilon), \mathbb{Q}] = p - 1$. Consider the diagram of field extensions:

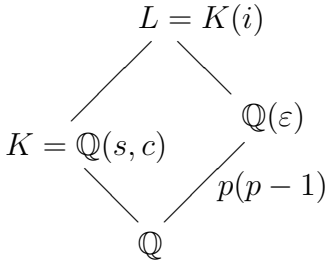


Under the assumption that P is constructible, $[K : \mathbb{Q}]$ is a power of 2. Also $L = K(i)$ is obtained by adjoining $i = \sqrt{-1}$, so that $[L : K] = 2$, and $[L : \mathbb{Q}]$ is also a power of 2. Finally, $[\mathbb{Q}(\varepsilon), \mathbb{Q}] = p - 1$ divides $[L : \mathbb{Q}]$, so that $p - 1$ is a power of 2.

The statement about p^2 is similar: let $(s, c) = \left(\sin \frac{2\pi i}{p^2}, \cos \frac{2\pi}{p^2}\right)$ and $\varepsilon = c + is$. Then ε is a p^2 root of 1, but not a pth root of 1, so is a root of the cyclotomic polynomial

$$\Phi_{p^2} = x^{p^2-p} + x^{p^2-2p} + \cdots + x^p + 1,$$

which is irreducible and of degree $p^2 - p = p(p - 1)$ (see Example 2.39). If $P = (s, c)$ is constructible, then as before, in the diagram



we have $[L : \mathbb{Q}]$ = power of 2 and $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = p(p - 1)$. Hence $p(p - 1)$ divides a power of 2, which implies $p = 2$. $\square$

Indications of converse The converse of Theorem 3.17 is true, and was proved by the teenage Gauss: for p a Fermat prime, the regular p-gon is constructible by ruler and compass. I indicate what is involved for $p = 5$ and $p = 17$.

We saw in Example 3.11 that the complex 5th roots of 1 can be constructed by successively solving two quadratic polynomials. If ε is the primitive 5th root of 1 then $\varepsilon + \varepsilon^4$ and $\varepsilon^2 + \varepsilon^3$ are the 2 roots of the quadratic $T^2 + T - 1$. From this we see that

$$P = \Big(\cos\frac{2\pi}{5}, \sin\frac{2\pi}{5}\Big) = \Big(\frac{1}{2}\cdot\frac{-1+\sqrt{5}}{2}, \frac{1}{2}\cdot\sqrt{\frac{1+\sqrt{5}}{2}}\Big).$$

You can devise a ruler and compass construction from this.

For $n = 17$, we need to understand the symmetry of the subgroup $\mu_{17} \subset \mathbb{C}^\times$. This is not the cyclic symmetry group $\mathbb{Z}/17$ of the regular 17-gon, but the algebraic symmetry of the field extension $\mathbb{Q} \subset \mathbb{Q}(\varepsilon)$; from this point of view, all the primitive roots of unity ε^i for $i = 1, \ldots, 16$ are equivalent: they all have the same minimal polynomial Φ_{17} over $\mathbb{Q}$. Thus for any $i = 1, \ldots, 16$ there is a field homomorphism $\varphi_i \colon \mathbb{Q}(\varepsilon) \to \mathbb{Q}(\varepsilon)$ taking $\varepsilon \mapsto \varepsilon^i$. We check that $\varphi_i \circ \varphi_j = \varphi_{ij}$ (because it does $\varepsilon^i \mapsto (\varepsilon^i)^j = \varepsilon^{ij}$). Thus the symmetry group is the multiplicative group $(\mathbb{Z}/17)^\times$, which is a group of order 16, and is cyclic, generated by 3:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^n	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Now write

$$\alpha_1 = \varepsilon + \varepsilon^9 + \varepsilon^{13} + \varepsilon^{15} + \varepsilon^{16} + \varepsilon^8 + \varepsilon^4 + \varepsilon^2;$$
$$\alpha_2 = \varepsilon^3 + \varepsilon^{10} + \varepsilon^5 + \varepsilon^{11} + \varepsilon^{14} + \varepsilon^7 + \varepsilon^{12} + \varepsilon^6.$$

These quantities are invariant under the subgroup of order 8 generated by 3^2, and are interchanged by 3. That is, $\varepsilon \mapsto \varepsilon^3$ moves the 16 roots around cyclically, and takes $\alpha_1 \mapsto \alpha_2$. We have

$$\alpha_1 + \alpha_2 = -1, \quad \alpha_1\alpha_2 = -4,$$

so that α_1, α_2 are the two roots of $T^2 + T - 4 = 0$; that is, $\alpha_1, \alpha_2 = \frac{-1\pm\sqrt{17}}{2}$. To prove this, note that $\alpha_1\alpha_2$ consists of 64 terms ε^k; we check that 1 does not occur, and symmetry considerations show that each of $k = 1, 2, \ldots, 16$ occurs the same number of times.

We deal likewise with the subgroups of order 4 and 2: set

$$\begin{aligned}\beta_1 &= \varepsilon + \varepsilon^{13} + \varepsilon^{16} + \varepsilon^4;\\ \beta_2 &= \varepsilon^9 + \varepsilon^{15} + \varepsilon^8 + \varepsilon^2;\\ \beta_3 &= \varepsilon^3 + \varepsilon^5 + \varepsilon^{14} + \varepsilon^{12};\\ \beta_4 &= \varepsilon^{10} + \varepsilon^{11} + \varepsilon^7 + \varepsilon^6.\end{aligned}$$

We see that $\beta_1+\beta_2 = \alpha_1$, $\beta_1\beta_2 = -1$, so that β_1, β_2 are roots of $T^2-\alpha_1 T-1$, and similarly β_3, β_4 are roots of $T^2 - \alpha_2 T - 1$.

Next, we can solve for

$$\gamma_1 = \varepsilon + \varepsilon^{16} = 2\cos\frac{2\pi}{17}, \quad \gamma_2 = \varepsilon^{13} + \varepsilon^4, \dots, \gamma_8$$

and finally for ε itself.

The main point here is that the group $\mu_{17} \cong \mathbb{Z}/17$ of 17th roots of 1 has symmetries $\mathrm{Aut}(\mathbb{Z}/17) = (\mathbb{Z}/17)^\times \cong \mathbb{Z}/16$. This is the group given by $\sigma_k \colon \varepsilon \mapsto \varepsilon^k$ for $k = 1, 2, \dots, 16$, and is cyclic with generator σ_3. To simplify the problem of finding roots ε, we looked at the subgroups

$$\{0\} \subset 8\mathbb{Z}/16 \subset 4\mathbb{Z}/16 \subset 2\mathbb{Z}/16 \subset \mathbb{Z}/16$$

(which are cyclic groups of order $1, 2, 4, 8, 16$). Then α_1, α_2 are invariant under the subgroup of order 8, $\beta_1, \dots, \beta_4$ under the subgroup of order 4, and $\gamma_1, \dots, \gamma_8$ under the subgroup of order 2. Gauss showed that the same argument works to construct the regular p-gon for any Fermat prime p.

3.3 Normal extensions

Definition 3.18 A field extension $k \subset K$ is *normal* if the following holds: every irreducible $f \in k[x]$ that has a root in K splits into linear factors over K. In other words,

$$f \text{ has one root in } K \implies \text{all roots of } f \text{ are in } K.$$

Example 3.19 (i) The extension $\mathbb{Q} \subset K = \mathbb{Q}(\varepsilon)$ where ε is a nontrivial (primitive) pth root of 1. The minimal polynomial of ε is Φ_p, and it has $p - 1 = \deg \Phi_p$ roots in $\mathbb{Q}(\varepsilon)$.

(ii) The extension $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[3]{2})$ is not normal. Because $X^3 - 2 \in \mathbb{Q}[x]$ is irreducible, and has 1 root in K, but not the other 2. In fact $K \subset \mathbb{R}$, and the other two cube roots $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2} \notin \mathbb{R}$.

Normal is a kind of symmetry condition, saying that the field extension $k \subset K$ does not discriminate between different roots of an irreducible polynomial $f \in k[x]$: either it contains none, or it contains them all.

Definition 3.20 Let $f \in k[x]$; a field extension $k \subset K$ is a *splitting field* for f over k if the following two conditions hold:

(i) f splits into linear factors over K, that is,

$$f = c \cdot \prod_{i=1}^{n} (x - \alpha_i) \quad \text{with } \alpha_i \in K;$$

(ii) $K = k(\alpha_1, \ldots, \alpha_n)$.

We allow f to be reducible. For example, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2-2)(x^2-3)$ over $\mathbb{Q}$. Also, the effect of (ii) is that f does not split over any strict subfield of K: it has n roots in K, and to get the splitting you need all of them, hence all of K.

Example 3.21 $x = \sqrt{a + \sqrt{b}}$ is a root of $f(x) = (x^2 - a)^2 - b$. Assuming $a, b \in \mathbb{Q}$ are "fairly general", the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{a + \sqrt{b}}, \sqrt{a - \sqrt{b}})$.

Consider the field extension $k \subset k_1 = k(\beta)$ with $\beta^2 = b$; and $k_1 \subset k_2 = k(\alpha, \beta)$ with $\alpha^2 = b + \beta$. Then $k \subset k_2$ is not in general a normal extension. The point is that α is a root of $f(x) = (x^2 - a)^2 - b$, which has the 4 roots

$$\pm\alpha, \pm\sqrt{a - \sqrt{b}},$$

and there is no particular reason why $\sqrt{a - \sqrt{b}}$ should exist in k_2 (for example, if $a = 6$, $b = 1$ over $\mathbb{Q}$; see Ex. 22 for when this happens).

Example 3.22 Suppose that k contains all pth roots of 1 and let $a \in k$ with a not a pth power. Then $x^p - a$ is irreducible (see Ex. 17); the extension

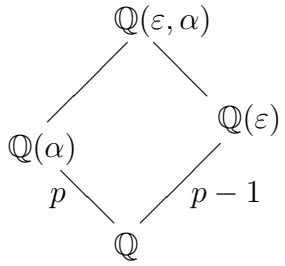
$$k \subset k(\alpha) \quad \text{with } \alpha^p = a$$

is already a splitting field of $x^p - a$ over k.

Example 3.23 Suppose on the contrary that $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ is irreducible over k (for example, $k = \mathbb{Q}$. Then $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ is not normal (compare the discussion after Remark 1.9). In fact

$$x^p - a = (x - \alpha)g, \quad \text{where} \quad g = x^{p-1} + \cdots + \alpha^{p-2}x + \alpha^{p-1},$$

and g is irreducible over $k(\alpha)$. The splitting field is $\mathbb{Q}(\varepsilon, \alpha)$, and arguing on degrees in the diagram



shows that $[\mathbb{Q}(\alpha, \varepsilon) : \mathbb{Q}] = p(p-1)$, and $g \in \mathbb{Q}(\alpha)[x]$ is irreducible, and is the minimal polynomial of $\varepsilon\alpha$.

Theorem 3.24 (Existence and uniqueness of K) *(a) Given any $f \in k[x]$, there exists a splitting field for f over k. In the "worst case", $[K : k] = n!$, where $n = \deg f$.*

(b) Let $f \in k[x]$, and suppose that K is a splitting field for f over k. Let L be any field, and $\sigma\colon k \to L$ a field homomorphism such that $\sigma(f) \in L[x]$ splits. Then σ extends to a homomorphism $\varphi\colon K \to L$:

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & L \\ \bigcup & \nearrow_{\sigma} & \\ k & & \end{array}$$

That is, there exists a field homomorphism φ such that $\varphi(a) = \sigma(a)$ for all $a \in k$.

Proof of (a) Write $f = l_1 \cdots l_a \cdot f'$ where $l_1, \ldots, l_a$ are linear factors and $f' \in k[x]$ has no linear factors. We work by induction of $\deg f'$. If $\deg f' = 0$ then f is already split over k, and the statement is trivial.

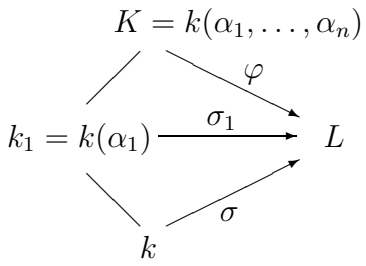
Let $g \in k[x]$ be an irreducible factor of f'. Then by Theorem 2.26 there exists a field extension $k \subset k_1$ in which g has a root α_1: set

$$k_1 = k[x]/(g) \quad \text{and } \alpha_1 = \text{class of } x \bmod g.$$

Then $(x - \alpha_1) \mid f'$ in $k_1[x]$, so that at least one more linear factor splits off f over k_1. That is, $f = l_1 \cdots l_b \cdot f''$ over k_1, where $\deg f'' < \deg f'$.

By induction, there exists a splitting field for f over k_1, say $k_1 \subset K$. Thus, f splits as $c \cdot \prod(x - \alpha_i)$, and $K = k_1(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_n)$, since $k_1 = k(\alpha_1)$. Therefore K is also a splitting field for f over k.

Proof of (b) We again work by induction, this time on $[K : k]$.



Suppose that K is a splitting field of f over K, and let $\alpha_1, \ldots, \alpha_n \in K$ be the roots of f. Assume without loss of generality that $\alpha_1 \notin k$, and define $k_1 = k(\alpha_1)$.

We first extend σ to $\sigma_1 \colon k_1 \to L$, using the idea of Theorem 2.26 again. Namely, $k_1 \cong k[x]/(g)$, where g is the minimal polynomial of α_1 over k. However, g is one irreducible factor of f, and $\sigma(f)$ splits in $L[x]$, so that $\sigma(g)$ has a root $\beta_1 \in L$. Now $\sigma(k) = k' \subset L$ is a subfield with $\sigma \colon k \xrightarrow{\simeq} k'$. Thus by Theorem 2.26, there is a unique extension σ_1 of σ to k_1 such that $\alpha_1 \mapsto \beta_1$.

Now the extension $k_1 \subset K$ and $\sigma_1 \colon k_1 \to L$ satisfies the assumptions of (b), with $[K : k_1] < [K : k]$. Indeed, K is a splitting field for f over k_1, and σ_1 is a homomorphism for which $\sigma_1(f) = \sigma(f)$ splits in $L[x]$. Thus by induction, σ_1 extends to $\varphi \colon K \to L$. $\square$

Corollary 3.25 *Given fields k, k' and polynomials $f \in k[x]$, $f' \in k[x']$, and an isomorphism $\sigma \colon k \to k'$ taking f to $\sigma(f) = f'$. If K is a splitting field for f over K and K' a splitting field for f' over k' then there exists an isomorphism $\varphi \colon K \to K'$ extending σ.*

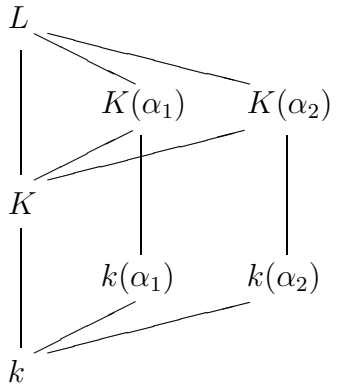
This is the particular case of (b) with $K' = L$. Roughly speaking, "the splitting field is unique up to k-isomorphism".

Theorem 3.26 *Let $k \subset K$ be a field extension. Then K is a splitting field over k for some polynomial $f \in k[x]$ if and only if $k \subset K$ is finite and normal.*

Proof We start with the easy "if" part. Suppose $[K : k] < \infty$ and let $\beta_1, \ldots, \beta_r \in K$ be such that $K = k(\beta_1, \ldots, \beta_r)$ (for example, take a basis). Now let $g_i \in k(x)$ be the minimal polynomial of β_i; each g_i is irreducible over k and has a root in K, so that if K is normal, it splits over K, so that K is the splitting field of $f = \prod g_i$.

The "only if" is harder in principle, since we have to prove splitting over K of any irreducible polynomial $g \in k[x]$ (not just some given g). We approach the problem somewhat obliquely. Suppose that K is a splitting field of f over k. For irreducible $g \in k[x]$, let L be any field containing K in which g splits, and let $\alpha_1, \alpha_2 \in L$ be any two roots of g.

We argue on the following diagram consisting of subfields of L:



Step 1 There exists a k-isomorphism $\sigma\colon k(\alpha_1) \xrightarrow{\simeq} k(\alpha_2)$. This follows from Theorem 2.26 since α_1, α_2 are both roots of the irreducible polynomial $g \in k[x]$.

Step 2 There exists a k-isomorphism $\varphi\colon K(\alpha_1) \xrightarrow{\simeq} K(\alpha_2)$ extending σ. This follows from Corollary 3.25, since $K(\alpha_1)$ is a splitting field for f over $k(\alpha_1)$, and ditto for α_2.

Step 3 It follows that $[K(\alpha_1) : k] = [K(\alpha_2) : k]$, hence

$$[K(\alpha_1) : K][K : k] = [K(\alpha_2) : K][K : k],$$

and cancelling gives $[K(\alpha_1) : K] = [K(\alpha_2) : K]$. In particular,

$$\alpha_1 \in K \iff \alpha_2 \in K$$

Step 4 Now if $g \in k[x]$ is irreducible and has one root in K, then it splits over some possibly bigger field L. But by Step 3, since $\alpha \in K$, all the other roots of g are also in K. Therefore, for any irreducible $g \in k[x]$,

$$g \text{ has a root in } K \implies g \text{ splits over } K. \quad \square$$

3.4 Application to finite fields

For the finite fields $\mathbb{F}_q$, compare van der Waerden, §60.

Theorem 3.27 *A finite field k has p^a elements for some prime power p^a.*

Proof $\mathbb{Z}$ is infinite, so that $\mathbb{Z} \subset k$ is impossible. Thus the prime subfield is $\mathbb{F}_p \subset k$ (see Definition 2.16). However, a finite field k must be finite dimensional over $\mathbb{F}_p$, say $[k : \mathbb{F}_p] = a$, and then $k \cong (\mathbb{F}_p)^a$ and $\#k = p^a$. $\square$

Example 3.28 $f = x^3 + x + 1 \in \mathbb{F}_2[x]$ is irreducible; for it has no root in $\mathbb{F}_2$, so no linear factor. Write $k = \mathbb{F}_2[x]/(f)$ and α for the class of x mod f. Then $1, \alpha, \alpha^2$ is a basis of k, and the multiplication table can be deduced from $\alpha^3 = \alpha + 1$:

$*$	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1

(and the other products by distributivity). This should persuade you that there exists a field $\mathbb{F}_8$ of order 8.

Proposition 3.29 *Let k be a field and $G \subset k^\times$ a finite subgroup of the multiplicative group. Then G is cyclic.*

Proof Write $N = |G|$. Then every element $\alpha \in G$ satisfies $\alpha^N = 1$. Thus G consists of all the N roots of $x^N - 1$.

For any divisor $m \mid N$ with $m < N$, since $x^m - 1$ has at most m roots in k, not all elements of G have $\alpha^m = 1$. Factor N as $N = p_1^{a_1} \cdots p_k^{n_k}$ with distinct primes p_i. Therefore for $i = 1, \ldots, k$, there exists $\alpha_i \in G$ so that $\alpha_i^{N/p_i} \neq 1$, and α_i has order divisible by $p_i^{a_i}$. Now set $\beta_i = \alpha_i^{N/p_i^{a_i}}$; its order is exactly $p_i^{a_i}$.

Hence $\beta = \prod \beta_i$ has order exactly N, and $G = \langle \beta \rangle$. $\square$

Theorem 3.30 *For any prime power $q = p^a$ there exists a field $\mathbb{F}_q$ of order q, and $\mathbb{F}_q$ is unique up to isomorphism.*

Proof The prime subfield must be $\mathbb{F}_p$. I make two claims:

(a) Any field of order q is a splitting field for $x^q - x$ over $\mathbb{F}_p$.

(b) Conversely, if K is a splitting field for $x^q - x$ over $\mathbb{F}_p$ then K is a field of order q.

The result follows from Theorem 3.24 and these claims: for the splitting field of $x^q - x$ exists and is unique up to isomorphism.

To prove (a), the multiplicative group $K^\times = K \setminus 0$ is a group of order $q - 1$, so every element $0 \neq \alpha \in K$ satisfies $\alpha^{q-1} = 1$. Thus the elements of K are exactly the roots in K of $x^q - x$. Therefore $K = \mathbb{F}_p(\text{roots of } x^q - x)$ is the splitting field of $x^q - x$.

For the converse (b), note first that in any field K of characteristic p, the set of roots of $x^q - x$ form a subfield: indeed

$$\alpha^q = \alpha \text{ and } \beta^q = \beta \implies \begin{cases} (\alpha\beta)^q = \alpha\beta, \text{ and} \\ (\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta. \end{cases}$$

(The last equation uses Ex. 1.16.) It follows that a splitting field K for $x^q - x$ over $\mathbb{F}_p$ consists entirely of roots of $x^q - x$. In particular $|K| \leq q$.

It remains to obtain a contradiction from the assumption that K has order $q' = p^{a'}$ with $a' < a$. In this case $K \setminus 0$ is a group of order $q' - 1$, and is cyclic by Proposition 3.29 so that K contains an element α of order $q' - 1$. By the above, $\alpha^{q-1} = 1$, so that $(q' - 1) \mid (q - 1)$. Write $b = q' - 1$ and

$q-1=bc$. Note that $c \equiv 1 \bmod p$. Then

$$x^{q-1}-1=(x^b-1)\Big(\underbrace{x^{b(c-1)}+x^{b(c-2)}+x^b+1}_{c \text{ terms}}\Big)=(x^{q'}-1)g.$$

Now g has no roots in K. In fact every nonzero $\alpha \in K$ satisfies $\alpha^b=1$, so that $g(\alpha)=1+\cdots+1=c=1 \in K$. Since K is a splitting field for x^q-x, it follows that $\deg g=1$, and $|K|=q$. $\square$

3.5 Separable extensions

This section addresses a certain pathology that only occurs for fields of characteristic p (so you can skip it for most purposes). Given a field k and an irreducible polynomial $f \in k[x]$, we know that f factorises as a product of linear factors $f=\prod_{i=1}^{n}(x-\alpha_i)$ over a splitting field $k \subset K$. Does it follow that the roots α_i are distinct? In this section, we see that the answer is yes if $\operatorname{char} k=0$, but not necessarily if $\operatorname{char} k=p$.

Definition 3.31 Let k be a field and $f \in k[x]$ an irreducible polynomial. Then f is *separable* if it has $n=\deg f$ distinct roots in some extension field. If it has multiple roots then f is *inseparable*.

Let $k \subset K$ be a field extension and $\alpha \in K$. We say that α is separable if its minimal polynomial $f \in k[x]$ is separable. The extension $k \subset K$ is separable if every $\alpha \in K$ is separable.

Example 3.32 Let k be a field of characteristic p containing an element t that is not a pth power. (For example, $k=\mathbb{F}_p(t)$, with t transcendental over $\mathbb{F}_p$.) Then $f=x^p-t$ is irreducible; consider the extension $k \subset K=k[x]/(f)$, with $\alpha \in K$ the class of x modulo f; in other words, $K=k(\alpha)$ with $\alpha=\sqrt[p]{t}$. Then f splits over K as $f=(x-\alpha)^p$, so is not separable.

Definition 3.33 (Derived polynomial) Define the map

$$\partial\colon k[x] \to k[x] \quad \text{by} \quad f=\sum a_n x^n \mapsto \partial(f)=\sum n a_n x^{n-1}.$$

In other words, $\partial f=\frac{\mathrm{d}f}{\mathrm{d}x}$, but treated as a formal operation. ∂f is called the *derived polynomial* of f. It obviously coincides with the usual derived polynomial $\partial f=\frac{\mathrm{d}f}{\mathrm{d}x}$ if k is a subfield of $\mathbb{C}$. (The definition of differentiation

by taking limits does not make sense over a general field. Compare Ex. 27 for an algebraic treatment in terms of a ring containing an element ε with $\varepsilon^2 = 0$. Note that ∂ is *not* a ring homomorphism.)

Proposition 3.34 *$\partial\colon k[x] \to k[x]$ is a k-linear derivation. That is,*

(i) $\partial(af + bg) = a\partial f + b\partial g$ *for* $a, b \in k$ *and* $f, g \in k[x]$.

(ii) $\partial(fg) = g\partial f + f\partial g$ *for all* $f, g \in k[x]$.

Proof Direct calculation. For (ii), suppose that $f = \sum a_n x^n$ and $g = \sum b_m x^m$; then $fg = \sum_n \sum_m a_n b_m x^{n+m}$, so that

$$g\partial f = \sum_n \sum_m n a_n b_m x^{n+m-1}, \quad f\partial g = \sum_n \sum_m m a_n b_m x^{n+m-1}.$$

These add to $\sum_n \sum_m (n+m) a_n b_m x^{n+m-1} = \partial(fg)$. $\square$

Proposition 3.35 *Let $f \in k[x]$ be a polynomial. Then f has a repeated root in some extension field $k \subset K$ if and only if $f, \partial f$ have a common factor $g(x) \in k[x]$ of degree ≥ 1.*

Proof Suppose that f has $n = \deg f$ distinct roots in its splitting field K. Then $f = \prod_{i=1}^{n} (x - \alpha_i)$. We extend ∂ to a derivation $\partial\colon K[x] \to K[x]$; then using Proposition 3.34, (ii), we get

$$\partial f = \sum_j \Big\{ \prod_{i \neq j} (x - \alpha_i) \Big\}.$$

Hence $(x - \alpha_i) \nmid \partial f$; in fact, it divides $n - 1$ of the summands, and not the nth. Thus $f, \partial f$ have no common factor in $K[x]$, hence no common factor in $k[x]$. This proves the "if".

Conversely, if f has a repeated root α in K then $(x - \alpha)^2 \mid f$, so Proposition 3.34, (ii) gives $(x - \alpha) \mid \partial f$, and so f and ∂f have the nontrivial common factor $x - \alpha$ in $K[x]$. It then follows that they have a nontrivial common factor in $k[x]$. For suppose by contradiction that f and ∂f have no common factor in $k[x]$. Then the ideal $(f, \partial f) \subset k[x]$ is principal, and therefore is the whole of $k[x]$. Therefore by the property of hcf (see Ex. 11)

$$pf + q\partial f = 1 \quad \text{for some } p, q \in k[x].$$

Then also $f, \partial f$ have no common factor in $K[x]$, which contradicts the above. $\square$

Proposition 3.36 (Discriminant) *Let $f = a_0 x^n + \cdots + a_{n-1}x + a_n \in k[x]$ be a polynomial of degree n. The following conditions are equivalent:*

(i) $h = \operatorname{hcf}(f, \partial f)$ *has degree* ≥ 1.

(ii) There exist polynomials $a, b \in k[x]$ of degrees $\deg a = d < n-1$, $\deg b = d+1$ satisfying $af + b\partial f \equiv 0$.

(iii) The $2n-1$ polynomials

$$f, xf, \ldots, x^{n-2}f, g, xg, \ldots, x^{n-1}g \tag{3.4}$$

are linearly dependent in the $2n-1$-dimensional vector space of polynomial of degree $\leq 2n-2$.

(iv) The discriminant $\Delta(f)$ *vanishes, where $\Delta(f)$ is defined as the determinant of the $(2n-1) \times (2n-1)$ matrix*

$$\begin{vmatrix}
a_0 & a_1 & \ldots & & a_{n-1} & a_n & 0 & \ldots & & \\
. & a_0 & a_1 & \ldots & & a_{n-1} & a_n & 0 & \ldots & \\
. & & \vdots & & & & & & & \vdots \\
. & . & . & \ldots & & a_0 & a_1 & \ldots & & a_n \\
na_0 & (n-1)a_1 & \ldots & & a_{n-1} & 0 & \ldots & & & \\
. & na_0 & (n-1)a_1 & \ldots & & a_{n-1} & 0 & \ldots & & \\
. & & \vdots & & & & & & & \vdots \\
. & . & . & \ldots & & & na_0 & (n-1)a_1 & \ldots & a_{n-1}
\end{vmatrix}$$

formed by the coefficients of the $2n-1$ polynomials (3.4).

Corollary 3.37 *Let $f \in k[x]$ be irreducible. Then f is inseparable if and only if $\partial f = 0$; this happens if and only if* $\operatorname{char} k = p$ *and $f = g(x^p)$.*

Proof Since f is irreducible, any nontrivial common factor of f and ∂f can only be f itself. However, ∂f has degree $\leq \deg f - 1$, so that $f \mid \partial f$ is only possible if $\partial f = 0$.

If $f = \sum a_n x^n$, then $\partial f = 0$ holds if and only if $na_n = 0$ for all n. In characteristic 0 this means that $f = \text{const}$. In characteristic p, it means that $a_n = 0$ unless $p \mid n$, that is, $f = \sum a_{mp} x^{mp}$ is a polynomial involving only x^p. $\square$

Proposition 3.38 *If k is a finite field with $|k| = q = p^a$ elements then every element of k is a pth power.*

If k is a field of characteristic p such that every element of k is a pth power, then every irreducible $f \in k[x]$ is separable, hence every algebraic extension $k \subset K$ is separable.

Proof The map $\varphi\colon k \setminus 0 \to k \setminus 0$ given by $a \mapsto a^p$ is injective, because $k^\times = k \setminus 0$ is a group of order $q - 1$ coprime to p. Therefore φ is also surjective.

We know that an irreducible polynomial f is inseparable if and only if

$$f = \sum a_{mp} x^{mp};$$

however, if the coefficients a_{mp} of f are all pth powers, say $a_{mp} = b_m^p$, then $f = g(x)^p$, where $g = \sum b_m x^m$. (Again, by repeated use of the formula $(a+b)^p = a^p + b^p$.) Therefore f is not irreducible, a contradiction. $\square$

Exercises to Chapter 3

1. If $a_1, \ldots, a_n \in K$ are algebraic over a subfield k, generalise Proposition 3.3 by proving that $k[a_1, \ldots, a_n] = k(a_1, \ldots, a_n)$.

2. Let $k \subset K$ be a field extension and $a \in K$. Show that if $g \in k[x]$ is any nonconstant polynomial and $b = g(a)$ then a is algebraic over $k(b)$. Note that g may be reducible, and b may be 0.

3. If $f \in k[x]$ is the minimal polynomial of $\alpha \in K$, show how to write down the minimal polynomial of $\alpha - b$ for $b \in k$.

4. If $\alpha \in K$ has minimal polynomial $f \in k[x]$ of odd degree, prove that $k(\alpha) = k(\alpha^2)$. Determine whether the condition is necessary.

5. Let $K = \mathbb{Q}(\sqrt{2} + \sqrt{5})$. Find the degree $[K : \mathbb{Q}]$ and show how to write down a basis of K over $\mathbb{Q}$.

6. Suppose that a quadratic $f(x) = x^2 + a_1x + a_2$ has roots α_1, α_2, and a cubic $g(y) = y^3 + b_1y^2 + b_2y + b_3$ has roots $\beta_1, \beta_2, \beta_3$. Use elementary symmetric functions to prove that the 6 quantities $\{\alpha_i + \beta_j\}$ for $i = 1, 2$ and $j = 1, 2, 3$ are roots of a sextic. [Hint: The elementary symmetric functions in the $\{\alpha_i + \beta_j\}$ are symmetric functions of α_i and β_j, so can be expressed in terms of the coefficients a_i, b_j. Calculating the sextic explicitly would be a huge task.]

7. Find the minimal polynomial of $\sqrt{2} + \sqrt[3]{5}$.

8. Let $\alpha \in \mathbb{C}$ be a root of $f = x^3 + 3x + 3$, and let $\beta \in \mathbb{C}$ be a root of $g = y^2 - \alpha y + 1$. Find an explicit polynomial equation for β over $\mathbb{Q}$.

9. $k \subset K$ is a field extension and $\alpha, \beta \in K$; suppose that $[k(\alpha) : k] = n$ and $[k(\beta) : k] = m$. Prove that

$$[k(\alpha, \beta) : k(\alpha)] = m \iff [k(\alpha, \beta) : k(\beta)] = n.$$

   Express this condition in terms of the minimal polynomial of β over k and over $k(\alpha)$.

10. Let $\alpha = \sqrt[3]{2}$ and $\beta = \omega\sqrt[3]{2}$; calculate the degrees, and find out whether the condition in Ex. 9 holds.

11. Suppose that $a, b \in k$ are such that a is a square in $k(\sqrt{b})$; prove that either a or ab is a square in k. [Hint: Write out $(c + d\sqrt{b})^2$.]

12. Let $a, b \in k$, and suppose that b is not a square in k; let $K = k(\beta)$ with $\beta^2 = b$. Prove that if one of $a + \beta$ or $a - \beta$ is a square in K, then so is the other, and deduce that then $c = a^2 - b$ is a square in k.

13. Say why the following question is nonsense, and try to form a sensible question along the same lines. Let $\alpha \in \mathbb{C} \setminus \mathbb{R}$, and suppose that α is algebraic over $\mathbb{Q}$. Set $K = \mathbb{Q}(\alpha)$ and $K_0 = K \cap \mathbb{R}$. Prove that $[K : K_0] = 2$, and deduce that $[K : \mathbb{Q}]$ is even.

14. Let p be an odd prime and write

$$c = \cos\frac{2\pi}{p}, \quad s = \sin\frac{2\pi}{p}, \quad \varepsilon = c + is = \exp\frac{2\pi i}{p};$$

set $K = \mathbb{Q}(s, c)$. Prove that $[K : \mathbb{Q}] = (p-1)/2$. It is clear in view of $c^2 + s^2 = 1$ that s is quadratic over $\mathbb{Q}(c)$ and vice versa, so that $[K : \mathbb{Q}(s)]$ and $K : \mathbb{Q}(c)] = 1$ or 2; which cases occur for different p?

15. Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Calculate $[K : \mathbb{Q}]$ and find a nice basis.

16. Let K be the splitting field of $x^{12} - 1$ over $\mathbb{Q}$; calculate $[K : \mathbb{Q}]$ and find a nice basis. Prove that K is also the splitting field of $(x^4 - 1)(x^3 - 1)$ over $\mathbb{Q}$.

17. Let p be a prime number. Prove that for any field k and any $a \in k$, the polynomial $x^p - a$ is either irreducible, or has a root. [Hint: If $f = f_1 f_2$, factorise f_1, f_2 into linear factors over a bigger field, and consider their constant terms.]

18. Let $k \subset K$ be an extension having degree $[K : k] = n$ coprime to p. Prove that a is a pth power in k if and only if it is in K.

19. Let p be a prime and k a field such that $x^p - 1$ splits into linear factors. Now suppose that $k \subset K$ is a field extension, and that $\alpha \in K$ has minimal polynomial $f \in k[x]$ of degree n coprime to p. Prove that $k(\alpha) = k(\alpha^p)$; find a counterexample if k does not contain all the pth roots of 1. [Hint: Argue on the degree $[k(\alpha) : k(\alpha^p)]$ and use the result of Ex. 17.]

20. Let k be a field of characteristic $\neq 2$, $a, b \in k$, and let $K = k(\alpha, \beta)$ where $\alpha^2 = a$ and $\beta^2 = b$. Set $\gamma = \alpha(\beta + 1)$; prove that $K = k(\gamma)$. [Hint: Express α and β in terms of γ.] Ex. 11 tells you when $[K : k] = 4, 2$ or 1. Find the minimal polynomial of γ over k in each case.

21. Suppose that $\operatorname{char} k \neq 2$, and let $k \subset L$ be a field extension of degree 4. Prove that the following two conditions are equivalent:

    (a) there exists an intermediate field $k \subset K \subset L$;

(b) $L = k(\alpha)$ for some α having minimal polynomial over k of the form $f = x^4 + ax^2 + b$.

22. Let $a, b \in k$ and set $c = a^2 - b$; suppose that none of b, c or bc is a square in k. If L is a splitting field of $f = (x^2 - a)^2 - b$, prove that $[L : k] = 8$. [Hint: Use Exs. 11–12 repeatedly.]

23. Let $a, b \in k$, and suppose that $f = x^4 - 2ax^2 + b^2$ is irreducible in $k(x)$. Show that if $\alpha \in L$ is a root of f in some extension field L, then so is b/α, and deduce that $K = k(\alpha)$ is already a splitting field of f.

24. Let $k \subset K$ be a finite normal extension, and suppose that $f \in k[x]$ is irreducible. Suppose that f factors in $K[x]$ as $f = g_1 \cdots g_r$ with irreducible $g_i \in K[x]$; prove that all the g_i have the same degree. [Hint: K is a splitting field of some $h \in k[x]$; if α is a root of g_i, show that $K(\alpha)$ is a splitting field for h over $k(\alpha)$.]

25. Show how to construct 7th and 13th roots of 1 by solving quadratics and a single cubic.

26. Prove that there exists an inclusion $\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}$ if and only $a \mid b$. [Hint: Reread the proof of Theorem 3.30.]

27. Let A be a ring, and define $B = A[\varepsilon]$ as follows: B is the set of pairs (a, b) with $a, b \in B$, and multiplication given by $(a, b)(c, d) = (ac, ad + bc)$. Show that B is a ring containing an element ε such that $\varepsilon^2 = 0$, and every element of B has a unique expression $a + b\varepsilon$ with $a, b \in A$.

28. Now let $A = k[x]$, and B as in Ex. 27; for $f \in k[x]$, write $f(x + \varepsilon) = f + \partial(f) \cdot \varepsilon \in B$. Verify that this defines a map $\partial\colon k[x] \to k[x]$ that satisfies $\partial(fg) = f\partial g + g\partial f$ and $\partial a = 0$ for $a \in k$. Check that $\partial f = \frac{\mathrm{d}f}{\mathrm{d}x}$ as in Definition 3.33.

4 Galois theory

Introduction

In this chapter we study a field extension $k \subset K$ by means of the group

$$\mathrm{Gal}(K/k) = \{k\text{-automorphisms } \varphi\colon K \to K\};$$

we will see that *under certain conditions*, this group provides detailed information about the structure of the field extension, and in particular allows us to find all the intermediate fields $k \subset F \subset K$. In Section 3.1 we talked about the degree $[K : k]$ of an extension; in the good cases, $\mathrm{Gal}(K/k)$ is a group of order $[K : k]$, and one should think of it as an invariant of the extension contained more detailed and more precise information than just the degree.

Summary Definition of $\mathrm{Gal}(K/k)$, $\#\{k\text{-homomorphisms } \tau\colon K \to L\}$ and relation with normal and separable extensions. Definition of fixed subfield K^G; Galois extensions; Galois if and only if finite, normal and separable; normal closure of an extension; how to construct elements of K^G. Galois extensions with cyclic group $\mathbb{Z}/n$.

The Galois correspondences

$$H \mapsto H^* = K^H \quad \text{and} \quad F \mapsto F^\dagger = \mathrm{Gal}(K/F)$$

define a bijection between subgroups $H \subset G = \mathrm{Gal}(K/k)$ and intermediate fields $k \subset F \subset K$; normal subgroups and normal field extensions; the example of a biquadratic polynomial

Recall basic group theory; definition of soluble group; compatibilities; S_n is not soluble for $n \geq 5$; criterion for subgroup $H \subset S_5$ to be the whole of S_5. Radical extension; given enough roots of 1, a Galois extension is radical if and only if its Galois group is soluble; radical extensions and normal closure; adjoining nth roots of 1; an extension is soluble in characteristic 0 if and only if the group is soluble. Impossibility of solving the quintic. The cubic and quartic revisited.

4.1 Counting field homomorphisms

Definition 4.1 (i) Let $k \subset K$ be a field extension and $\sigma\colon k \to L$ a given homomorphism. A *k-homomorphism* $\tau\colon K \to L$ is a field homomorphism

such that $\tau(a) = \sigma(a)$ for all $a \in k$:

$$\begin{array}{ccc} K & \xrightarrow{\tau} & L \\ \bigcup & \nearrow_{\sigma} & \\ k & & \end{array}$$

(ii) In the particular case $K = L$ and σ is the inclusion $k \subset K$, we say τ is a *k-automorphism* of K, or an automorphism of K/k. The set of all such,

$$\mathrm{Gal}(K/k) = \{k\text{-automorphisms of } K\}$$

is naturally a group under composition of maps, and is called the *Galois group* of the extension $k \subset K$.

Example 4.2 (Compare Remark 2.31) Let $K = k(\alpha)$ be a primitive extension, where α has minimal polynomial $f \in k[x]$; and let $\sigma\colon k \to L$ be a given homomorphism. Then the set of k-homomorphisms $\tau\colon K \to L$ is in bijection with the set of roots of $\sigma(f)$ in L.

This is essentially contained in Remark 2.31: if τ is a k-homomorphism then $\tau(\alpha)$ must be a root of $\sigma(f)$, since $0 = \tau(f(\alpha)) = \sigma(f)(\tau(\alpha))$; conversely, for any root β of $\sigma(f)$ in L, $K = k[\alpha] \cong k[x]/(f) \cong k[\beta] \subset L$ (k-isomorphisms), so that the composite defines a k-homomorphism $K \to L$ taking α to β.

Theorem 4.3 *Consider the diagram*

$$\begin{array}{ccc} K & \xrightarrow{\tau} & L \\ \bigcup & \nearrow_{\sigma} & \\ k & & \end{array}$$

where $k \subset K$ is a finite extension and $\sigma\colon k \to L$ a given homomorphism. Then

$$\#\{k\text{-homomorphisms } \tau\colon K \to L\} \leq [K : k],$$

and equality holds if and only if

(i) $k \subset K$ is separable, and

(ii) if $f \in k[x]$ is the minimal polynomial of some $\alpha \in K$ then $\sigma(f)$ splits in $L[x]$.

Note that (i) and (ii) together are just the condition that $\sigma(f)$ splits into distinct linear factors over L. The proof is in 4 steps.

Step 1 Let $\alpha \in K$, and consider the primitive extension $k_1 = k(\alpha) \subset K$; let f be the minimal polynomial of α, and $\deg f = n$. Then finding all the k-homomorphisms $\sigma_1 \colon k_1 \to L$ is solved by Example 4.2. Thus

$$\#\{k\text{-homomorphisms } \sigma_1\} = \#\{\text{roots of } \sigma(f) \text{ in } L\} \leq \deg f = [k_1 : k]$$

(and equality if we assume separability). Hence the theorem is true for the extension $k \subset k_1$: we have just proved the inequality, and equality holds if and only if $\sigma(f)$ has n distinct roots in L. This can be expressed as the two conditions

(i) f has distinct roots in a splitting field, that is, f is separable; and

(ii) $\sigma(f)$ splits over L.

Step 2 Fix $k_1 = k(\alpha)$ as in Step 1, and consider diagrams of the form

$$\begin{array}{ccc} K & \xrightarrow{\tau} & L \\ \bigcup & \nearrow_{\sigma_1} & \\ k_1 & & \end{array}$$

where τ and σ_1 are k-homomorphisms. Now any k-homomorphism $\tau \colon K \to L$ extends some well-defined k-homomorphism $\sigma_1 \colon k_1 \to L$ (with $\sigma_1 = \tau|k_1$), so that we can list the set $\{k\text{-homomorphisms } \tau \colon K \to L\}$ by listing

(a) all k-homomorphisms $\sigma_1 \colon k_1 \to L$, and

(b) for given σ_1, all k_1-homomorphisms $\tau \colon K \to L$.

Now we carried out (a) in Step 1, and (b) can be done by induction, since $[K : k_1] < [K : k]$. Thus for the inequality,

(a) $\#\{\sigma_1\} = [k_1 : k]$; and

(b) for any fixed σ_1, by induction,

$$\#\{k_1\text{-homomorphisms } \tau\} = [K : k_1].$$

Therefore $\#\{\tau\} \leq [K : k_1][k_1 : k] = [K : k]$, proving the inequality. Moreover, if equality holds, then necessarily

$$\#\{\sigma_1\} = [k_1 : k],$$

so that as we saw in Step 1, the two conditions of the theorem hold for this choice of α. However, this works for any $\alpha \in K$.

Step 3 I prove that (i) and (ii) imply $\#\{\tau\} = [K : k]$ using the same strategy. Assuming (i) and (ii), we know by Step 1 that

$$\#\{k\text{-homomorphisms } \sigma_1 \colon k_1 \to L\} = [k_1 : k].$$

Fix any σ_1, and consider diagrams of the form

$$\begin{array}{ccc} K & \xrightarrow{\tau} & L \\ \bigcup & \nearrow_{\sigma_1} & \\ k_1 & & \end{array}$$

If I can prove that the extensions $k_1 \subset K$ and $\sigma_1 \colon k_1 \to L$ satisfies (i) and (ii), then it follows by induction that $\#\{k_1\text{-homomorphisms } \tau\} = [K : k_1]$, so that by considering all the choices of σ_1, I get $\#\{\tau\} = [K : k_1][k_1 : k]$.

Step 4 k_1 and σ_1 satisfy (i) and (ii). For any $\alpha \in K$, write $f \in k[x]$ for its minimal polynomial over k, and $f_1 \in k_1[x]$ for its minimal polynomial over $k_1[x]$. Then f_1 divides f, because $f(\alpha) = 0$, and $f_1 \in k_1[x]$ generates $\ker\{k_1[x] \to K\}$ by $g \mapsto g(\alpha)$. Now the assumption (i) and (ii) is that $\sigma(f)$ splits over L into distinct linear factors; therefore, so does $\sigma_1(f_1)$. $\square$

Corollary 4.4 *Suppose that $k \subset K$ is finite. Then*

$$\mathrm{Gal}(K/k) \text{ has order } [K : k] \iff k \subset K \text{ is separable and normal.}$$

Proof Apply the Theorem to the special case $L = K$ and $\sigma \colon k \to K$ the inclusion map. Then (ii) in the theorem is exactly the condition that $k \subset K$ is normal.

Example 4.5 (i) Let $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{C}$; then as we have known for a long time, $\#\{k\text{-homomorphisms } K \to L\} = 3 = [K : k]$, (since $\mathbb{C}$ has 3 cube roots of 2).

(ii) k, K the same, but $L = \mathbb{R}$; then $[K : k]$=3, but there is only one k-homomorphism $K \to \mathbb{R}$, namely the identity. By the same argument $\mathrm{Gal}(K/k) = \{1\}$, the trivial group.

(iii) Let k be a field of characteristic p, and $t \in k$ an element that is not a pth power (as in Example 3.32). Let $K = k(\alpha)$, with $\alpha^p = t$; then $\mathrm{Gal}(K/k) = \{1\}$. The point is that any k-homomorphism $\tau \colon K \to K$ must take α to a root of $x^p - t$, and $x^p - t = (x - \alpha)^p$ has only one root, so there is no choice, $\tau = \mathrm{id}_K$.

4.2 Fixed subfields, Galois extensions

Write $\operatorname{Aut} K$ for the set of field automorphisms of K; this is clearly a group under composition.

Definition 4.6 (i) For $G \subset \operatorname{Aut} K$, write

$$K^G = \big\{a \in K \;\big|\; g(a) = a \text{ for all } g \in G\big\}.$$

Then $K^G \subset K$ is clearly a subfield (if $a, b \in K$ are fixed by all $g \in G$ then so are $a \pm b$, ab and a/b), called the *fixed subfield* of G. This construction is the main method for constructing intermediate fields in an extension.

(ii) An extension $k \subset K$ is *Galois* if there is a finite subgroup $G \subset \operatorname{Aut} K$ such that $k = K^G$.

This is a "top-down" definition, where k is considered as constructed from the extension field K, the opposite of what we have had so far.

Theorem 4.7 *Let $k \subset K$ be a field extension; then $k \subset K$ is Galois if and only if it is finite, separable and normal; moreover, then $G = \operatorname{Gal}(K/k)$.*

Proof of "if" This follows without much trouble from Theorem 4.3. Let $k \subset K$ be a finite, separable and normal extension. Then as we saw in 4.4, the group $\Gamma = \operatorname{Gal}(K/k)$ has order $[K : k]$. Consider the subfield $K^\Gamma \subset K$; then by definition of $\operatorname{Gal}(K/k)$, every element $g \in \Gamma$ is a k-homomorphism, so fixes every $a \in k$, so that $k \subset K^\Gamma \subset K$. On the other hand, by definition of K^Γ, every element of Γ is a K^Γ-homomorphism of K, so that by Theorem 4.3 applied to the extension $K^\Gamma \subset K$,

$$[K : k] = |\Gamma| = \#\{K^\Gamma\text{-automorphisms of } K\} = [K : K^\Gamma].$$

Hence $k = K^\Gamma$, which proves that $k \subset K$ is Galois.

First proof of "only if" We assume that $k \subset K$ is finite. (This argument proves directly that a Galois extension is normal and separable, but not that $k \subset K$ is finite.) Let $G \subset \operatorname{Aut} K$ be a finite group, and $k = K^G$. Let $\alpha \in K$ be any element, and consider the G-orbit of α, that is, the finite set $G \cdot \alpha = \{g(\alpha) \mid |g \in G\} = \{\alpha_1, \dots, \alpha_s\}$, say with $\alpha_1 = \alpha$; then the action

of G on K permutes $\alpha_1, \ldots, \alpha_s$: any α_i is of the form $\alpha_i = h(\alpha)$ for some $h \in G$, and if $g \in G$ is any element, then $g(\alpha_i) = g(h(\alpha_i)) = (gh)(\alpha) \in G \cdot \alpha$. It follows from this that the polynomial

$$f = \prod_i (x - \alpha_i) = x^s + \cdots + b_1 x + b_0 \in K[x]$$

is fixed by the action of G, and so has coefficients $b_i \in k = K^G$; if you prefer, the coefficients b_i are given by $b_{s-i} = (-1)^i \sigma_i$, where the σ_i are the elementary symmetric functions in $\alpha_1, \ldots, \alpha_s$ (as in Section 1.4), and so are fixed by any permutation of the α_i.

Now $k \subset K$ is normal and separable, since any $\alpha \in K$ is a root of a polynomial $f \in k[x]$ that splits into distinct factors over K.

Proposition 4.8 *Let $G \subset \operatorname{Aut} K$ be a finite group, and $k = K^G$; then*

$$[K : k] = |G|.$$

Proof First, $|G| \leq [K : k]$: if $[K : k] = \infty$ there is nothing to prove, and otherwise the result follows from Theorem 4.3.

Next, I suppose that $|G| = n$, and prove that $n \geq [K : k]$. So let $x_1, \ldots, x_{n+1} \in K$ be any elements; it is enough to construct a nontrivial linear dependence relation $\sum u_j x_j = 0$ between the x_j with coefficients $u_j \in k$.

To do this, suppose that $G = \{g_1, \ldots, g_n\}$, and consider the $n \times (n+1)$ matrix $\big(g_i(x_j)\big)_{i,j}$, where $i = 1, \ldots, n$ and $j = 1, \ldots, n+1$. By easy linear algebra over the field K, the n linear equations in $n+1$ variables u_j

$$\sum_j g_i(x_j) u_j = 0 \quad \text{for } i = 1, \ldots, n \tag{4.1}$$

certainly have nontrivial solutions $u_1, \ldots, u_{n+1}$. Hence there exists a nontrivial solution $u_1, \ldots, u_{n+1}$ for which the minimal number of u_i are nonzero. By permuting the indices j, I can assume that

$$u_1, \ldots, u_r \neq 0, \quad u_{r+1} = \cdots = u_{n+1} = 0;$$

also, by multiplying through by a constant in K, I can assume that $u_1 = 1$.

Claim 4.9 *Let $u_1, \ldots, u_r$ be a solution of (4.1) satisfying the above assumptions. Then $h(u_j) = u_j$ for all $h \in G$ and for $j = 1, \ldots, r$, that is, $u_1, \ldots, u_r \in K^G = k$.*

Proof of the claim Applying $h \in G$ to (4.1) gives

$$0 = h\Big(\sum_j g_i(x_j)u_j\Big) = \sum_j hg_i(x_j)h(u_j) \quad \text{for } i = 1, \dots, n.$$

However, since $G = \{g_1, \dots, g_n\}$, the set $\{hg_1, \dots, hg_n\}$ is just a permutation of G, so that n equations here are the same as the n equations in (4.1), just written in a different order. Therefore $h(u_1), \dots, h(u_r)$ is another solution of (4.1). Now $h(u_1) = h(1) = 1$; so the difference $u_j - h(u_j)$ for $j = 2, \dots, r$ is a solution of (4.1), with $< r$ nonzero terms. By the minimality assumption on the solution $u_1, \dots, u_r$, it follows that $u_j = h(u_j)$ for each j and each $h \in G$. This proves the claim.

Now id_K is one of the g_i, so (4.1) includes the condition that $\sum_j u_j x_j = 0$; this shows that any $n+1$ elements $x_j \in K$ are linearly dependent over k, so that $[K : k] = |G|$. This proves Proposition 4.8. □

Second proof of "only if" in Theorem 4.7 Assume $k \subset K$ is a Galois extension, so $k = K^G$, where $G \subset \operatorname{Aut} K$ a group of order $n = |G|$. Then we have seen in Proposition 4.8 that $[K : k] = n$. On the other hand G is a group of order n of k-automorphisms of K, so that by Theorem 4.3, G is the whole of $\mathrm{Gal}(K/k)$, and $k \subset K$ is normal and separable. □

Proposition 4.10 *Let $k \subset K$ be a finite normal extension, and $k \subset F \subset K$ an intermediate field; then any k-homomorphism $\tau\colon F \to K$ extends to a k-automorphism $\sigma\colon K \to K$.*

Proof By the easy implication of Theorem 3.26, we know that K is a splitting field over k for some polynomial $f \in k[x]$. Hence K is a splitting field for f both over F and over $\tau(F)$; now we can use Corollary 3.25 (uniqueness of splitting field): $\tau(f) = f$, because τ is a k-automorphism and $f \in k[x]$, hence there exists an isomorphism extending τ:

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K \\ \bigcup & & \bigcup \\ F & \xrightarrow{\tau} & \tau(F) \end{array}$$

Corollary 4.11 *Let $k \subset K$ be finite and normal, $\alpha \in K$, and let f be the minimal polynomial of α over k; if $\beta \in K$ is any other root of f then there exists $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha) = \beta$.*

Proof Apply Proposition 4.10 to $F = k(\alpha)$ and $\tau\colon k(\alpha) \xrightarrow{\simeq} k(\beta)$. $\square$

Remark 4.12 This gives another proof of the "if" part of Theorem 4.7: if $k \subset K$ is finite, separable and normal and $\alpha \in K \setminus k$, the minimal polynomial f of α over k has at least one other root $\beta \neq \alpha$, and there exists $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha) = \beta$. Therefore $\alpha \notin k$ implies that $\alpha \notin K^G$; hence $k = K^G$.

Definition 4.13 Let $k \subset K$ be an extension; a *normal closure* of K over k is an extension L of K such that

(i) $k \subset L$ is normal; and

(ii) no smaller subfield of L containing K is normal over k. That is,

$$K \subset L' \subset L \text{ with } k \subset L' \text{ normal } \implies L' = L.$$

Proposition 4.14 *For a given f.g. field extension $k \subset K$, there exists a normal closure L of K over k, and it is unique up to K-isomorphism.*

Proof Suppose that $K = k(\alpha_1, \ldots, \alpha_r)$, and let $f_i \in k[x]$ be the minimal polynomial of α_i; set $g = \prod_i f_i$. Then it is not hard to see that a normal closure of K over k is exactly the same thing as a splitting field for g over K. Therefore the proposition follows from Corollary 3.25.

How to find elements of K^G

Given a field K and a finite subgroup $G \subset \mathrm{Aut}\, K$, we have seen in Theorem 4.7 and Proposition 4.8 that K^G is "big enough". One method of finding elements of K^G was given in the proof of Theorem 4.7: take any $\alpha \in K$, consider the orbit $G \cdot \alpha = \big\{ g(\alpha) \;\big|\; g \in G \big\}$, and take the elementary symmetric functions of these.

Another method is contained in the proof of Proposition 4.8. Suppose that $|G| = n$, and take $n+1$ elements $x_1, \ldots, x_{n+1}$; consider the $n \times (n+1)$ matrix $M = \big(g_i(x_j)\big)_{i,j}$. Usually, this will have rank n; write A_j for the jth

minor of M (that is, the determinant obtained by deleting the jth column). Then by Cramer's rule for solving linear equations, $\sum A_j x_j = 0$. If M has rank n, wlog $A_1 \neq 0$, so that $u_i = A_i/A_1$ give $\sum u_j x_j = 0$. Moreover, since the action of $g \in G$ on K just permutes the rows of M, it clearly multiplies each A_i by ± 1, and fixes the u_i. Hence $u_i \in K^G$.

The following result shows another method of finding invariant elements in the special case of a cyclic group, and this will be an important step in our study of solubility by radicals. Compare Example 1.10 and Ex. 1.10.

Theorem 4.15 *Let k be a field containing n distinct nth roots of unity $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$; suppose that $k \subset K$ is a Galois field extension with cyclic Galois group $\mathrm{Gal}(K/k) \cong \mathbb{Z}/n$. Write σ for a generator of $\mathrm{Gal}(K/k)$. Then there exists $y \in K$ such that $\sigma(y) = \varepsilon y$, so that $y^n = a \in k$ and $K = k(y)$. That is, the extension $k \subset K$ is obtained by adjoining $\sqrt[n]{a}$ to k.*

Proof We are given a k-automorphism σ of K of order n. For $x \in K$, set

$$y = x + \varepsilon^{n-1}\sigma(x) + \varepsilon^{n-2}\sigma^2(x) + \cdots + \varepsilon\sigma^{n-1}(x) = \sum_{i=0}^{n-1} \varepsilon^{n-i}\sigma^i(x).$$

Then since $\varepsilon \in k$, $\sigma(\varepsilon) = \varepsilon$, and the action of $\sigma \in \mathrm{Gal}(K/k)$ on y is given by

$$\sigma(y) = \sigma(x) + \varepsilon^{n-1}\sigma^2(x) + \cdots + \varepsilon x = \sum_{i=0}^{n-1} \varepsilon^i \sigma^{n-i+1}(x) = \varepsilon y.$$

Thus $\sigma(y^n) = y^n$, so that $y^n = a \in K^G = k$. We[2] have thus found $y \in K \setminus k$ such that $y^n \in k$, and since $[K : k(y)] = n$, and $x^n - a \in k[x]$ is irreducible, $K = k(y)$ is clear. (Note that we find y by looking for an eigenvector of the action of σ on the k-vector space K, as in Example 1.10.) $\square$

4.3 The Galois correspondences and the Main Theorem

Fix a field extension $k \subset K$ and write $G = \mathrm{Gal}(K/k)$. Introduce the notation

$$\mathcal{F} = \big\{\text{intermediate fields } F \;\big|\; k \subset F \subset K\big\}$$

[2]There is a small gap here: I still need to prove that $y \neq 0$. The proof is based on the same linear independence of k-homomorphisms as in Prop. 4.8 and Claim 4.9, and I will tidy it up in a handout later.

and

$$\mathcal{G} = \big\{\text{subgroups} \;\big|\; H \subset G\big\}.$$

$\mathcal{F}$ and $\mathcal{G}$ are sets, with partial orders defined by inclusion.

Construction of $^*\colon \mathcal{F} \to \mathcal{G}$

For $F \in \mathcal{F}$, write

$$F^* = \big\{g \in G \;\big|\; g(x) = x \text{ for all } x \in F\big\} = \mathrm{Gal}(K/F).$$

The difference between G and F^* is that the elements g of G fix k, whereas to be in F^* they must fix the bigger field F. Now F^* is obviously a subgroup of G, so that * defines a map $\mathcal{F} \to \mathcal{G}$. Notice that for obvious reasons, if $F_1 \subset F_2$ then $F_1^* \supset F_2^*$: fixing all the elements of F_2 is a stronger condition than fixing all the elements of F_1.

Construction of $^\dagger\colon \mathcal{G} \to \mathcal{F}$

For $H \in \mathcal{G}$, write

$$H^\dagger = K^H = \big\{x \in K \;\big|\; g(x) = x \text{ for all } g \in H\big\}$$

$H^\dagger$ is the fixed field of H, so is a subfield of K, and in fact K is Galois over $H^\dagger$. Clearly if $H_1 \subset H_2$ then $H_1^\dagger \supset H_2^\dagger$, since the condition on $x \in K$ to be fixed under H_2 is a stronger condition than for it to be fixed under H_1.

Tautologies 4.16 *(a)* $F_1 \subset F_2 \implies F_1^* \supset F_2^*$*;*

(b) $H_1 \subset H_2 \implies H_1^\dagger \supset H_2^\dagger$*;*

(c) for all $F \in \mathcal{F}$*,* $F \subset (F^*)^\dagger$*;*

(d) for all $H \in G$*,* $H \subset (H^\dagger)^*$*.*

We have already discussed (a) and (b); (c) say that if $H = F^* =$ set of $g \in G$ fixing F, then F is contained in the set of things fixed by H. (d) is a similar sentiment.

Proposition 4.17 *Suppose that* $k \subset K$ *is a finite Galois extension with group* $G = \mathrm{Gal}(K/k)$*. Then for all* $F \in \mathcal{F}$*, the extension* $F \subset K$ *is Galois with group* F^**; the degrees are given by*

$$[K : F] = |F^*| \quad \textit{and} \quad [F : k] = |G|/|F^*| = \#\{\textit{cosets of } F^* \textit{ in } G\}.$$

Proof $F \subset K$ is finite, normal and separable, so by Theorem 4.7, it is Galois. Also by definition, $\mathrm{Gal}(K/F) = \{F\text{-automorphisms of } K\} = F^*$.

Theorem 4.18 (Main Theorem of Galois theory) *Let $k \subset K$ be a finite Galois extension with group $G = \mathrm{Gal}(K/k)$. Then * and † are inverse bijections, that is*

$$F = F^{*\dagger} \quad \textit{and} \quad H = H^{\dagger *} \quad \textit{for all } F \in \mathcal{F} \textit{ and } H \in \mathcal{G}.$$

Proof For $F \in \mathcal{F}$, we prove that $F = F^{*\dagger}$: the extension $F \subset K$ is Galois, with $\mathrm{Gal}(K/F) = F^*$; this is exactly what we want, since it says that

$$F = K^{F^*} = (F^*)^\dagger.$$

We now prove that $H = H^{\dagger *}$ for any $H \in \mathcal{G}$: if H is a finite subgroup of $\mathrm{Aut}\, K$, then $K^H \subset K$ is a Galois extension, and by Theorem 4.7, $\mathrm{Gal}(K/K^H) = H$; thus $K^H = H^\dagger$, and then $\mathrm{Gal}(K/K^H) = H^{\dagger *}$. $\square$

The action of G on $\mathcal{F}$ and $\mathcal{G}$

The group G acts on K fixing k, so that it acts on any invariant of the extension $k \subset K$, in particular the sets $\mathcal{F}$ and $\mathcal{G}$. In more detail, $g \in G$ acts on $\mathcal{F}$ by moving the fields F around: $g(F)$ is another subfield of K. Also, g acts on $\mathcal{G}$ by conjugacy, taking a subgroup $H \subset G$ to gHg^{-1}. So we can ask if the bijections * and † are compatible with these two actions.

Claim 4.19 $(g(F))^* = gF^*g^{-1}$ *for any $F \in \mathcal{F}$ and $g \in G$.*

Proof of claim The usual:

$$\begin{aligned} h \text{ fixes every element of } g(F) &\iff hg(a) = g(a) \text{ for all } a \in F \\ &\iff g^{-1}hg(a) = a \text{ for all } a \in F \\ &\iff g^{-1}hg \in F^* \iff h \in gF^*g^{-1}. \end{aligned}$$

Proposition 4.20 *Let $k \subset K$ be as in Main Theorem 4.18. Then for $F \in \mathcal{F}$,*

(i) $k \subset F$ is a normal extension

$$\iff g(F) = F \text{ for all } g \in G \iff F^* \subset G \text{ is a normal subgroup;}$$

(ii) if this holds, the Galois group $\mathrm{Gal}(F/k)$ *= the quotient group* G/F^*.

Proof Write $H = F^*$. By definition,

$$H \subset G \text{ is a normal subgroup} \iff gHg^{-1} = H \text{ for all } g \in G;$$

now using Claim 4.19, this happens if and only if $g(F) = F$ for all $g \in G$.

Now suppose that $k \subset F$ is a normal extension; if $\alpha \in F$ and $g \in G$, I prove that $g(\alpha) \in F$. Let f be the minimal polynomial of α over k. Then since g is a k-isomorphism, $g(\alpha)$ is a root of f in K, hence is in F, using the normality of F/k. Hence $k \subset F$ normal implies $g(F) = F$ for all $g \in G$.

Conversely, suppose $g(F) = F$ for all $g \in G$; then the minimal polynomial f of $\alpha \in F$ splits over K, by normality of $k \subset K$. If $\beta \in K$ is any root of f then by Corollary 4.11, there exists $g \in \mathrm{Gal}(K/k)$ such that $g(\alpha) = \beta$. So if we assume that $g(F) = F$ for all $g \in \mathrm{Gal}(K/k)$, it follows that all the roots of f are already in F, so that F is normal over k. This proves (i).

(ii) is easy: assuming $F \in \mathcal{F}$ is such that $k \subset F$ is normal. Then for all $g \in G$, $g(F) = F$, so that $g_{|F} \colon F \to F$ is a k-homomorphism of F; hence there is a restriction map $r = \mathrm{res}_F \colon G = \mathrm{Gal}(K/k) \to \mathrm{Gal}(F/k)$, given by $g \mapsto g_{|F}$. By definition,

$$F^* = \big\{ g \in G \;\big|\; g \text{ fixes } F \text{ elementwise} \big\} = r^{-1}(\mathrm{id}_F) = \ker r.$$

Also, r is surjective: this is exactly the statement of Proposition 4.10. Hence r induces an isomorphism $G/F^* \xrightarrow{\simeq} \mathrm{Gal}(F/k)$. $\square$

Example 4.21 Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$, that is, $K = \mathbb{Q}(i, \alpha)$, with $i^2 = -1$, $\alpha^4 = 2$. We have seen in Example 3.10 that $[K : \mathbb{Q}] = 8$. Then it is easily seen that the Galois group of K over $\mathbb{Q}$ is generated by

$$\sigma \colon \begin{cases} i \mapsto i, \\ \alpha \mapsto i\alpha \end{cases} \quad \text{and} \quad \tau \colon \begin{cases} i \mapsto -i, \\ \alpha \mapsto \alpha. \end{cases}$$

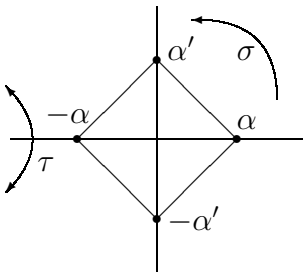
Since $\sigma^4 = 1 = \tau^2$ and $\tau\sigma = \sigma^3\tau$, we see that $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$, the dihedral group of order 8; the intermediate subfields $\mathbb{Q} \subset F \subset K$ were listed in Example 3.10. You know how to write down the subgroups of D_8, and it is an easy exercise to work out the correspondance in detail in this case.

Example 4.22 (Biquadratic equations) Let k be a field, $a, b \in k$, and let K be the splitting field of $f = (x^2-a)^2-b$ over k; we get $k \subset k_1 = k(\beta)$, where $\beta^2 = b$, then $k_1 \subset k_2 = k_1(\alpha)$ where $\alpha^2 = a+\beta$ and finally $K = k_2(\alpha')$, where $(\alpha')^2 = a-\beta$. Now in general, $[K : k]$ is a divisor of 8, since $k \subset k_1 \subset k_2 \subset K$ and each step has degree 1 or 2. Ex. 3.22 explains how to prove that $[K : k]$=8 provided that none of b, $a^2 - b$ and $b(a^2 - b)$ are squares in k. Clearly, any element $g \in \mathrm{Gal}(K/k)$ must take $\beta \mapsto \pm\beta$. There are two cases: either

(i) $g(\beta) = \beta$, then $g(\alpha) = \pm\alpha$, $g(\alpha') = \pm\alpha'$, giving at most 4 possibilities; or

(ii) $g(\beta) = -\beta$, then $g(\alpha) = \pm\alpha'$, $g(\alpha') = \pm\alpha$, again giving 4 possibilities.

Now K/k is a Galois extension, and hence if $[K : k] = 8$, all 8 of these possibilities must occur. Suppose that this happens. Then $\mathrm{Gal}(K/k)$ contains elements $\sigma\colon \beta \mapsto -\beta, \alpha \mapsto \alpha' \mapsto -\alpha$ and $\tau\colon \beta \mapsto \beta, \alpha \mapsto \alpha$, $\alpha' \mapsto -\alpha'$; it is again not hard to see that $\sigma^4 = \tau^2 = 1$ and $\tau\sigma = \sigma^3\tau$ (they both do $\beta \mapsto -\beta, \alpha \mapsto -\alpha' \mapsto -\alpha$), so that here again we have a dihedral group D_8:



(4.2)

The subgroups of D_8 are as follows:

- 4 generated by reflections: $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, $\langle\sigma^2\tau\rangle$, $\langle\sigma^3\tau\rangle$;
- the other subgroup of order 2 $\langle\sigma^2\rangle$;
- the cyclic subgroup $\langle\sigma\rangle$ of order 4;
- two 4-groups $\langle\sigma^2, \tau\rangle$ and $\langle\sigma^2, \sigma\tau\rangle$.

It is not hard to see that

- $k_1 = k(\beta)$ is the fixed field of $\langle\sigma^2, \tau\rangle$;
- $k_2 = k(\beta, \alpha)$ is the fixed subfield of $\langle\tau\rangle$; and

- $k(\beta, \alpha')$ is the fixed subfield of $\langle \sigma^2\tau \rangle$.

To find the other subfields, consider $\gamma = \alpha\alpha'$ and $\delta = \alpha + \alpha'$, $\delta' = \alpha - \alpha'$; by considering $\alpha = \sqrt{a+\beta}$, $\alpha' = \sqrt{a-\beta}$, we get

$$\gamma^2 = a^2 - b \quad \text{and} \quad \delta^2 = 2(\gamma + a).$$

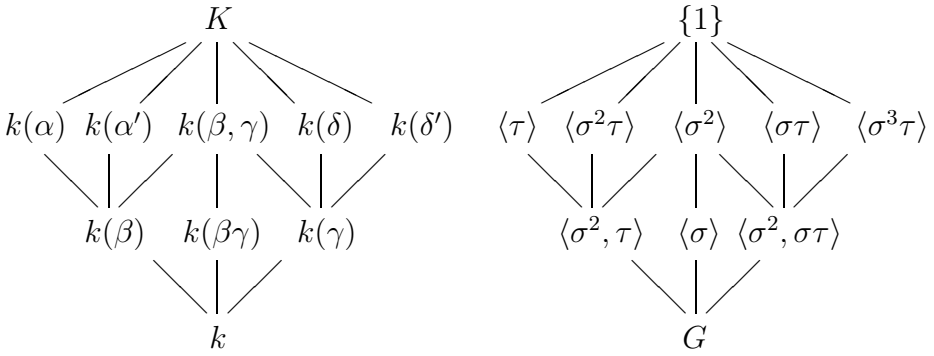
Then $k \subset k(\gamma) \subset k(\delta) \subset K$ is a tower of three extensions of degree $= 2$, so that each step is in fact quadratic. Then

- $k(\delta)$ is the fixed field of $\langle \sigma\tau \rangle$ (since $\sigma\tau \colon \alpha \mapsto \alpha'$);
- $k(\delta')$ is the fixed field of $\langle \sigma^3\tau \rangle$;
- $k(\gamma)$ is the fixed field of $\langle \sigma^2, \sigma\tau \rangle$;

  now by taking unions, we get

- $k(\beta, \gamma)$ is the fixed field of $\langle \sigma^2 \rangle$;
- $k(\beta\gamma)$ is the fixed field of $\langle \sigma \rangle$.

Thus the final picture of all the intermediate subfields $k \subset F \subset K$ and all the subgroups $H \subset \mathrm{Gal}(K/k)$ is as follows:



4.4 Soluble groups

Definition 4.23 A finite group G is *soluble* if there exists a chain

$$G = A_0 \supset A_1 \supset \cdots \supset A_r = \{e\}$$

of subgroups of G such that for $i = 0, \ldots, r-1$, $A_{i+1} \subset A_i$ is normal and $A_i/A_{i+1} \cong \mathbb{Z}/p_i$ for some prime p_i.

Theorem 4.24 (Isomorphism theorems) *(I) If $A \subset G$ is a normal subgroup and $H \subset G$ a subgroup, let HA be the subgroup of G generated by A and H; then A is normal in HA, $A \cap H$ is normal in H, and*

$$H/A \cap H \;\cong\; HA/A.$$

(II) If $H_1 \subset H_2$ are two normal subgroups of G, then H_1 is normal in H_2, H_2/H_1 is normal in G/H_1, and

$$(G/H_1)/(G/H_2) \;\cong\; G/H_2.$$

Proof This is elementary and supposed to be known. The normality statements are easy; to prove the isomorphisms, there are natural maps $H \to HA/A$ and $G/H_1 \to G/H_2$, and it is not hard to see that these are surjective, and to find their kernels.

Proposition 4.25 *(i) G soluble and $H \subset G$ implies that H is soluble;*

(ii) G soluble and H normal in G implies that G/H is soluble;

(iii) conversely to (i) and (ii), if H is normal in G then H and G/H soluble implies that G is soluble.

(iv) a finite Abelian group is soluble.

Proof (i) Given the chain $G = A_0 \supset A_1 \supset \cdots \supset A_r = \{e\}$ and the subgroup $H \subset G$, set $B_i = H \cap A_i$. Then $H = B_0 \supset B_1 \supset \cdots \supset B_r = \{e\}$, and I claim that for $i = 0, \ldots, r-1$, B_{i+1} is normal in B_i and $B_i/B_{i+1} \cong$ either 0 or $\mathbb{Z}/p_i$. This is because the Isomorphism Theorem 4.24, (I) applied to $A_i \supset A_{i+1}$ and B_i gives

$$B_i/B_{i+1} \cong A_{i+1}B_i/A_{i+1} \subset A_i/A_{i+1} \cong \mathbb{Z}/p_i.$$

(ii) is similar, and (iii) is easy. (iv) If A is Abelian and $e \neq a \in A$ is any element, let N be the order of a, and $p \mid N$ any prime factor. Set $b = a^{N/p}$. Then b is of order p, so generates a subgroup $A_1 \cong \mathbb{Z}/p \subset A$; since A is Abelian, A_1 is automatically normal, and the quotient A/A_1 is soluble by induction. Then we are home using (iii). $\square$

Theorem 4.26 *The alternating group A_5 is not soluble. Therefore, for $n \geq 5$, the symmetric group S_n on n elements is not soluble.*

Proof Write A_5 for the alternating group on 5 elements. $A_5 \subset S_5 \subset S_n$, so that by Proposition 4.25, (i), it is enough to show that A_5 is not soluble. There are lots of ways of doing this. Here is one: for any group G and $g, h \in G$, the *commutator* of g and h is the element $[g, h] = ghg^{-1}h^{-1} \in G$; obviously if $\varphi\colon G \to M$ is any homomorphism to an Abelian group M,

$$\varphi([g, h]) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = e_M.$$

Claim 4.27 *Every element of A_5 is a commutator; hence A_5 has no non-trivial homomorphism to an Abelian group.*

Proof Every element of A_5 is one of (ijk), or $(ij)(kl)$ or $(ijklm)$ where i, j, k, l, m are distinct choices of elements $1, 2, 3, 4, 5$. One can see by a direct computation that each of these is a commutator:

$$[(ijl), (ikm)] = (ijl)(ikm)(ilj)(imk) = (ijk),$$
$$[(ijk), (ijl)] = (ijk)(ijl)(ikj)(ilj) = (ij)(kl),$$
$$[(ij)(km), (iml)] = (ij)(km)(iml)(ij)(km)(ilm) = (ijklm). \quad \square$$

Ex. 8 gives an alternative proof of Claim 4.27. In fact A_5 is a simple group, that is, it has no nontrivial normal subgroup, or equivalently no nontrivial quotient homomorphism $A_5 \to G$.

Proposition 4.28 *Let $H \subset S_5$ be a subgroup containing at least one transposition (ij), and acting transitively on $\{1, 2, 3, 4, 5\}$. Then $H = S_5$.*

Proof We build up the group step by step, starting from the given flip (transposition); suppose $(12) \in H$.

Step 1 Every $k \in \{1, 2, 3, 4, 5\}$ is involved in a flip $(jk) \in H$.

Since H acts transitively on the 5 elements, there exists $\sigma \in H$ such that $\sigma(1) = k$; then $\sigma \cdot (12) \cdot \sigma^{-1} = (jk)$ where $j = \sigma(2)$.

Step 2 At least one $k \in \{1, 2, 3, 4, 5\}$ is involved in 2 or more flips of H. Hence H contains the full S_3 of permutations on some 3 elements $\{i, j, k\}$.

Indeed, there must be at least 3 flips in H in order to satisfy Step 1. But then they must overlap at least once. By renumbering, I can suppose that $H \supset S_3$ on $\{1, 2, 3\}$.

Step 3 Assume $H \supset S_3$ on $\{1,2,3\}$; then 4 is involved in at least 2 flips.

As in Step 1, suppose $\sigma \in H$ with $\sigma(1) = 4$; then $\sigma' = \sigma \cdot (23) \in H$ and has the same property. So as in Step 1, $\sigma \cdot (12)\sigma^{-1} = (k\sigma(2))$, and $\sigma' \cdot (12) \cdot \sigma^{-1} = (k\sigma'(2)) = (k\sigma(3))$.

Step 4 Therefore there is a flip $(j4)$ with $j = 1, 2$ or 3. But S_3 together with any one of these generates the whole of S_4 on $\{1,2,3,4\}$.

Step 5 S_4 and any of the flips $(j5)$ for $j = 1,2,3,4$ generate S_5. $\square$

4.5 Solving equations by radicals

Radical and soluble extensions

A field extension $k \subset K$ is *radical* if there exists a chain

$$k = k_0 \subset k_1 \subset \cdots \subset k_r = K$$

such that for each i, $k_{i+1} = k_i(\alpha_i)$ with $\alpha_i^{p_i} \in k_i$ for some prime p_i; that is, each step consists of adjoining a pth root. Note that in this, we allow a_i to be a p_ith power in k, so that $x^{p_i} - a_i$ may be reducible; for example, the chain of a radical extension may include some steps that adjoin pth roots of 1.

$k \subset K$ is *soluble* if there exists an extension $K \subset L$ such that $k \subset L$ is radical. For example, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$ is radical (since $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ both have cubes in $\mathbb{Q}$); the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+\sqrt[3]{5})$ is soluble (since $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ is radical), but is not obviously radical itself. If $f \in k[x]$ is an irreducible polynomial, and $K = k(\alpha)$ is an extension in which f has a root, then $k \subset K$ is soluble if and only if a root of f can be got by successively applying field operations and taking roots; that is, we are asking if f can be solved by radicals.

Proposition 4.29 *Let $k \subset K$ be a Galois extension with Galois group $G = \mathrm{Gal}(K/k)$.*

(i) G is soluble if and only if there exists a chain of intermediate fields $k = k_0 \subset k_1 \subset \cdots \subset k_r = K$ such that each $k_i \subset k_{i+1}$ is Galois with group $\mathbb{Z}/p_i$.

(ii) Suppose in addition that k contains p distinct pth roots of 1 for every prime p dividing $|G|$. Then G is soluble if and only if $k \subset K$ is radical.

Proof (i) The Main Theorem shows at once that there exists a chain of intermediate fields if and only if there exists a chain of subgroups of G; moreover, given the chain, Proposition 4.20 says that $k_i \subset k_{i+1}$ is normal if and only if $G_{i+1} \subset G_i$ is.

(ii) We have seen in Theorem 4.15 that in the presence of roots of 1, a Galois extension with group $\mathbb{Z}/p$ is exactly the same thing as an extension obtained by adjoining a pth root.

We are not quite home for two rather technical reasons:

(a) as it stands, Proposition 4.29 only applies to Galois extensions, so maybe not to $k \subset k(\alpha)$; to get round this we have to discuss the relation of soluble to normal closure.

(b) There may not be enough roots of 1 around, so we have to discuss adding roots of 1.

Proposition 4.30 *Let $k \subset K$ be a radical extension and L its normal closure; then $k \subset L$ is also radical.*

Proof Suppose that $K = k(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i^{p_i} \in k(\alpha_1, \ldots, \alpha_{i-1})$ for each i. Let f_i be the minimal polynomial of α_i over k. Then we know L is the splitting field of $f = \prod_{i=1}^r f_i$, that is $L = k(\{\beta_{ij}\})$ where $i = 1, \ldots, r$, and $\beta_{i1}, \ldots, \beta_{id_i}$ are the roots of f_i (including α_i).

Let $K_i = k(\{\beta_{\iota j}\}_{\iota \le i})$; this obviously contains $k(\alpha_1, \ldots, \alpha_i)$, so that $\alpha_i^{p_i} \in K_{i-1}$. Now β_{ij} and α_i have the same minimal polynomial over k, so that by Corollary 4.11, there exists a k-homomorphism $\tau\colon L \to L$ taking $\alpha_i \mapsto \beta_{ij}$. Hence $\beta_{ij}^{p_i} = \tau(\alpha_i^{p_i}) \in \tau(K_{i-1})$; on the other hand, K_{i-1} is also a splitting field, so is normal, so $\tau(K_{i-1}) = K_{i-1}$. Hence $K_{i-1} \subset K_i$ is radical, since it is made by successively adjoining the β_{ij}, each of which has p_ith power in K_{i-1}. $\square$

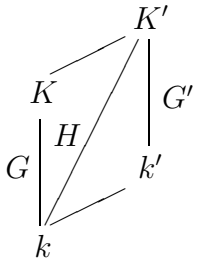
Adjoining roots of 1

Assume from now on that our fields are of characteristic 0. It is not hard to see that adjoining nth roots of 1 to a field k leads to a Galois extension with Abelian group: let k be a field, n a given integer, and K the splitting field of $x^n - 1$ over k. Then K has n roots of 1, forming a cyclic group (by Proposition 3.29), so generated by ε, a primitive nth root of 1. Then any

k-automorphism of K takes $\varepsilon \mapsto \varepsilon^i$ for some i, and composition is given by multiplication; that is, if $\tau_i(\varepsilon) = \varepsilon^i$ and $\tau_j(\varepsilon) = \varepsilon^j$ then

$$\tau_i\tau_j(\varepsilon) = \tau_i(\varepsilon^j) = \varepsilon^{ij}, \quad \text{so that} \quad \tau_i\tau_j = \tau_j\tau_i.$$

Proposition 4.31 *Let $k \subset K$ be a Galois extension, and n a given integer. Write K' for the splitting field of $x^n - 1$ over K, and $k' \subset K'$ for the splitting field over k:*



(4.3)

Then

(i) $[K' : k']$ *divides* $[K : k]$*;*

(ii) K'/k *is Galois. Moreover, if we set* $H = \mathrm{Gal}(K'/k)$, $G = \mathrm{Gal}(K/k)$ *and* $G' = \mathrm{Gal}(K'/k')$, *then*

$$H \text{ is soluble} \iff G \text{ is soluble} \iff G' \text{ is soluble.}$$

Proof If K is the splitting field of f, then K' is the splitting field of $(x^n - 1)f$, so K'/k is Galois. Consider the diagram (4.3).

Since K and k' are normal extensions of k, each of $A = \mathrm{Gal}(K'/K)$ and G' are normal subgroups of H and by Proposition 4.20, $G = H/A$; since by what we have said, A is a finite Abelian group, H soluble if and only if G soluble follows from Proposition 4.25. Similarly, since $\mathrm{Gal}(k'/k)$ is Abelian, H is soluble if and only if G' is soluble.

For (i), $\tau \in A$ is determined by its action on ε, so that the restriction map $A \to \mathrm{Gal}(k'/k) = H/G'$ is injective, hence $|A|$ divides $|\mathrm{Gal}(k'/k)|$. $\square$

Theorem 4.32 *Let $k \subset K$ be a field extension in characteristic 0. Then $k \subset K$ is soluble if and only if its Galois closure L has soluble Galois group.*

Proof Suppose first that $\mathrm{Gal}(L/k)$ is soluble. Introduce the nth roots of 1 as in Proposition 4.31, where $n = [L : k]$. Then by Proposition 4.25, L'/k' is Galois with soluble Galois group, and k' contains all roots of 1 of order dividing $[L : k]$, therefore all of order dividing $[L' : k']$. So by Proposition 4.30, $k' \subset L'$ is radical. Hence $k \subset L'$ is radical, so $k \subset K$ is soluble.

Conversely, if $k \subset K$ is soluble, it is contained in a radical extension, then by Proposition 4.31 in a Galois radical extension, say $k \subset M$. Introducing nth roots of 1, where $n = [M : k]$ as before, we see that $\mathrm{Gal}(M/k)$ is soluble, hence also $\mathrm{Gal}(L/k)$. $\square$

Impossibility of solving the quintic

If $f \in k[x]$, the Galois group of f is defined to be the Galois group of the splitting field of f over k. It can be viewed as a group of permutations of the roots of f; which particular subgroup of S_n depends on the particular k and f. It is quite tempting to think that for "fairly general" f, it should be the whole of S_n. Since S_n is not soluble (Theorem 4.26), it would then follow from Theorem 4.32 that the "general" equation of degree n is not soluble.

It can be seen (with more work), that there exist polynomials f of degree n over $\mathbb{Q}$ for which the Galois group is the whole of S_n. Here is a particular example of a quintic over $\mathbb{Q}$ whose Galois group is the whole of S_5: write $f = x^5 - 6x + 3$. Then f is irreducible by Eisenstein's criterion; hence if $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$ is the splitting field of f, $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $\alpha_1, \ldots, \alpha_5$. Also, by looking at the graph, it is clear that f has 3 real roots (approximately $-1.7, 0.5, 1.4$); and 2 complex conjugate roots: f increases from $-\infty$ to a maximum at $x_0 = -\sqrt[4]{\frac{6}{5}} \approx -1.05$ at which $f(x_0) \approx 8.02 > 0$, then goes down to a minimum at $x_1 = \sqrt[4]{\frac{6}{5}} \approx 1.05$ at which $f(x_1) \approx -2.02 < 0$. More simply, $f(-2) < 0$, $f(-1) > 0$, and $f(1) < 0$. Therefore complex conjugation $\mathbb{C} \to \mathbb{C}$ restricts to K to give a flip of these two roots, so that by Proposition 4.28, $\mathrm{Gal}(K/\mathbb{Q}) = S_5$.

Cubic and quartic revisited

Let $f \in k[x]$ be a cubic; if K is the splitting field, f has roots $\alpha_1, \alpha_2, \alpha_3 \in K$. The Galois group will be a subgroup $G \subset S_3$; if f is irreducible, G must act transitively on $\alpha_1, \alpha_2, \alpha_3$, so must have order 3 or 6. It is easy to deal with

the cyclic alternating group $A_3 = \langle(123)\rangle$, as in Theorem 4.15: write

$$y = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \quad \text{and} \quad z = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3.$$

Then y^3 and z^3 are invariant under A_3. So either y^3 and $z^3 \in k$ (if $G = A_3$), or they are interchanged by any element of $S_3 \setminus A_3$, in which case they are the two roots of a quadratic over k. See Section 1.6 for explicit formulas.

Now to deal with quartics. S_4 is soluble: indeed there is a natural surjective homomorphism $\pi\colon S_4 \to S_3$ defined as follows. Given $\{1,2,3,4\}$, there are 3 different ways of pairing them off into teams of 2 (well-known to bridge players): $A = [12:34]$, $B = [13:24]$, $C = [14:23]$. As you permute $\{1,2,3,4\}$, you permute $\{A,B,C\}$, for example (12) acts as (BC); (123) acts as (ACB). It is easy to see that $\ker\pi$ is the 4-group $V_4 = \langle(12)(34),(13)(24)\rangle$. Suppose that $f \in k[x]$ has Galois group S_4; then to solve f by radicals, you need first to find invariants of V_4. It is easy to see that $(\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$ and the 2 other such expressions are fixed by V_4, and are permuted as $\{A,B,C\}$ by S_4. So these 3 quantities are roots of a cubic equation with coefficients in k. See Section 1.7 for formulas.

Exercises to Chapter 4

1. Prove that if $[K:k] = 2$ then $k \subset K$ is a normal extension. Construct a tower $k \subset K \subset L$ such that $k \subset K$ and $K \subset L$ are both normal, but $k \subset L$ is not.

2. Let k be a field over which $f(x) = x^3 - 3x + 1 \in k[x]$ is irreducible, and $\operatorname{char} k \neq 3$. Let $K = k(\alpha)$ where $f(\alpha) = 0$. Prove that f splits over K, and deduce that $k \subset K$ is Galois with group $\mathbb{Z}/3$. [Hint: Factor f over $k(\alpha)$ as $f = (x-\alpha)g$, and solve the quadratic factor g by the usual formula, observing that $12 - 3\alpha^2$ is a perfect square in $k(\alpha)$:

$$12 - 3\alpha^2 = (-4 + \alpha + 2\alpha^2)^2.]$$

3. In Ex. 2, suppose in addition that k contains 3 cube roots of unity, $1, \omega, \omega^2$; find a radical expression for α.

4. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{5})$. Prove that $\mathbb{Q} \subset K$ is a Galois extension with group $\operatorname{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2 \times S_3$, and find some nice intermediate fields.

5. Suppose that k is a field containing a primitive nth root of unity ε (Definition 1.8). Let $K = k(t)$ with t transcendental over K. Show that there are k-automorphisms σ, τ of L given by

$$\sigma\colon t \mapsto \varepsilon t, \quad \tau\colon t \mapsto t^{-1},$$

and that these two generate a group G of automorphisms of L isomorphic to the dihedral group D_{2n}. Find the fixed subfields of the subgroups $\langle\sigma\rangle$, $\langle\tau\rangle$ and $\langle\sigma\tau\rangle$, and prove that the fixed subfield of G is $K = k(y)$, where $y = t^n + t^{-n}$.

6. Let k be any field, and $L = k(t)$. Let G be the group of k-automorphisms of L generated by $\sigma\colon t \mapsto 1 - t$ and $\tau\colon t \mapsto 1/t$; prove that $\sigma^2 = \tau^2 = \mathrm{id}$ and $(\sigma\tau)^3 = \mathrm{id}$, and deduce that $G \cong S_3$. Find the subfields of L fixed by σ and by τ respectively, and prove that $L^{\langle\sigma\tau\rangle} = k(y)$, where $y = \frac{t^3-3t+1}{t(t-1)}$; show that $y + \sigma(y) = 3$, and conclude that $K = L^G = k(z)$, where $z = y\sigma(y)$. Use Main Theorem 4.18 to find all the fields F intermediate between K and L.

7. Find all Galois extensions of degree 4; in more detail, prove that a Galois extension with group $\mathbb{Z}/2 \times \mathbb{Z}/2$ is of the form $k(\alpha, \beta)$, with $\alpha^2, \beta^2 \in k$ but $\alpha\beta \notin k$, whereas a Galois extension with group $\mathbb{Z}/4$ comes from a biquadratic equation $(x^2 - a)^2 - b = 0$ with $a \neq 0$, $\sqrt{b} \notin k$, but $\sqrt{a^2 - b} \in k$. [Hint: Refer back to Exs. 3.11–12 and 3.21 and Example 4.22.]

8. Prove that the alternating group A_n is generated by 3-cycles (ijk). Everyone knows that $(ijk) = (ij)(jk)$, so that (ijk) can be written as a product of two elements of order 2 in S_n, for any $n \geq 3$. By using two more letters l, m, show that (ijk) can also be written as a product of two elements of A_5 of order 2. Deduce that A_5 is not soluble. Find out why this proof (and that in 4.26) fails for $n \leq 4$.

9. Find your own proof of Proposition 4.28; prove also that a subgroup $H \subset A_5$ that contains (123) and acts transitively on $\{1, 2, 3, 4, 5\}$ is the whole of A_5.

10. Let $\varepsilon = \exp\frac{2\pi i}{n}$ be the usual nth root of 1 in $\mathbb{C}$. Prove that for any subfield $k \subset \mathbb{C}$, the extension $k \subset k(\varepsilon)$ is Galois, and that its Galois group is some subgroup of the multiplicative group $(\mathbb{Z}/n)^\times$ of the ring

$\mathbb{Z}/n$. (In other words, the group of integers $0 < a < n$ coprime to n, with multiplication mod n.)

11. Let ε be an nth root of 1; say that ε is a *primitive* nth root of 1 if its multiplicative order is exactly n (that is, $\varepsilon^m \neq 1$ for $m < n$). The primitive nth roots of 1 in $\mathbb{C}$ are $\varepsilon^a = \exp \frac{2\pi a i}{n}$ for a coprime to n, and the number of these is the Euler function

$$\varphi(n) = \{a \mid 1 < a < n \text{ and } \mathrm{hcf}(a, n) = 1\}.$$

Let $\Phi_n(x)$ be the monic polynomial with roots all the primitive nth roots of 1. It is easy to see that $x^n - 1 = \prod_{d|n} \Phi_d(x)$ (product over all d dividing n). Prove by induction that $\Phi_n \in \mathbb{Q}[x]$; then use the results of 2.4 to show that in fact $\Phi_n \in \mathbb{Z}[x]$.

12. The order of every element of the cyclic group $\mathbb{Z}/n$ is some factor $d \mid n$. The number of elements of order exactly d is given by the Euler phi function $\varphi(d)$. Thus $\sum_{d|n} \varphi(d) = n$. There is a famous inverse relation between n and $\varphi(d)$ called *Frobenius inversion*: namely

$$\varphi(n) = \sum_{d|n} \mu(d)\varphi(d), \tag{4.4}$$

where

$$\mu(d) = \begin{cases} 1 & \text{if } d = \prod p_i \text{ is a product of evenly many distinct primes,} \\ 1 & \text{if } d = \prod p_i \text{ is a product of oddly many distinct primes,} \\ 0 & \text{if } d \text{ has a square factor } p^2. \end{cases}$$

Prove (4.4). Or find a proof in a number theory textbook. [Hint: The set of elements of $[1, \ldots, n]$ coprime to n is the whole set minus the elements whose order divides n/p for each $p \mid n$, which gives $n - \sum_{p|n} \frac{n}{p}$ to first approximation. But those elements divisible by $p_1 p_2$ have been eliminated twice, so we have to add back in $\sum_{p_1 p_2 | n} \frac{n}{p_1 p_2}$.]

13. Prove the following Frobenius inversion formula for Φ_n:

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

[Hint: That is, start from $x^n - 1$, then for each $p_i \mid n$ divide out by $x^{n/p_i} - 1$. This gets rid of all roots of order $\frac{n}{p_i}$, hence all roots of order strictly dividing n, but unfortunately, roots of order $\frac{n}{p_1 p_2}$ now appear twice in the denominator, so we have to multiply again by $x^{n/p_1 p_2} - 1$, etc.]

14. Let ε be primitive nth root of 1 and let a be coprime to n. There exists a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\varepsilon)$ taking ε to ε^a if and only if ε and ε^a have the same minimal polynomial over $\mathbb{Q}$. Hence $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$ is the whole of $(\mathbb{Z}/n)^\times$ if and only if the cyclotomic polynomial Φ_n is irreducible over $\mathbb{Q}$. (Compare 2.38–2.39 for $n = p$ or p^2.)

15. Prove that for any prime p not dividing n, ε and ε^p have the same minimal polynomial over $\mathbb{Q}$. Proceed as follows: let f and g be the minimal polynomials of ε and ε^p respectively. By unique factoristion in $\mathbb{Z}[x]$, if f and g are coprime then fg divides $x^n - 1$. Now by considering $(f(\varepsilon))^p \bmod p$, prove that f and g reduced mod p have a common factor, and get a contradiction, by proving that $x^n - 1 \in \mathbb{F}_p$ does not have a repeated factor.

16. Prove that $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = (Z/n)^\times$. [Hint: Show that there exists a $\mathbb{Q}$-homomorphism taking $\varepsilon \mapsto \varepsilon^p$ for any prime p not dividing n; then show that these generate $(Z/n)^\times$.]

5 Additional material

This is stuff I don't have enough time to write out in this edition of the notes. Some of these ideas could serve as project material for 3rd or 4th year students.

5.1 Substantial examples with complicated $\mathrm{Gal}(L/k)$

It would be nice to have more explicit computations on the model of Example 4.22. Given your favourite finite group G, does there exist an extension $\mathbb{Q} \subset K$ with $\mathrm{Gal}(K/k) = G$? For $k = \mathbb{Q}$, this is a famous problem, called the *inverse Galois problem*. See for example, [Helmut Völklein, Groups as Galois groups: an introduction, Cambridge University Press, 1996].

5.2 The primitive element theorem

Every finite separable extension $k \subset K$ can be written as $K = k(\alpha)$ for some $\alpha \in K$. If k is an infinite field, this follows from the Main Theorem 4.18, since there are only finitely many intermediate fields $k \subset F \subset K$, and the vector space K is not the union of finitely many strict subspaces. So just take $\alpha \in K \setminus \bigcup F$.

5.3 The regular element theorem

If K/k is Galois with group $G = \mathrm{Gal}(K/k)$ then there exists an element $\alpha \in K$ such that $\{g(\alpha)\}_{g \in G}$ forms a basis of K. This means that K has a basis that is permuted simply transitively by the action of G, or in other words, that K is isomorphic to the regular representation of G over k.

5.4 Artin–Schreier extensions

For fields of characteristic p, a cyclic extension $k \subset K$ with group $\mathbb{Z}/p$ is an exotic object. Theorem 4.15 was based on the $x_0 + \varepsilon x_1 + \cdots + \varepsilon^{p-1} x_{p-1}$ trick described in Example 1.10 that turns a permutation representation of the cyclic group $\mathbb{Z}/p$ into an eigenvalue decomposition. This fails comprehensively to describe cyclic extensions in characteristic p, since there are no nontrivial roots ε of unity to play with.

Instead the typical extension is of the form $k \subset K = k(\alpha)$ with α a root of the *Artin–Schreier* equation $x^p - x = a$ for some $a \in k$. Notice that if α is a root, then so is $\alpha + 1$, and $\alpha + i$ for i in the prime subfield $\mathbb{F}_p \subset k$, so that $k(\alpha)$ is the splitting field over k of the separable polynomial $x^p - x - a$, so that $k \subset k(\alpha)$ is Galois of degree p.

To find α, start with some general orbit $u_0, u_1, \ldots, u_{p-1}$ in K permuted cyclically by the generator σ of $\mathbb{Z}/p$, and take the product

$$\alpha = u_0(u_1 + 1)(u_2 + 2) \cdots (u_{p-1} + p - 1). \tag{5.1}$$

In other words, we use the cyclic additive group of $\mathbb{F}_p$ in place of the cyclic multiplicative group of pth roots of unity in k. It's an exercise in the spirit of the proof of Theorem 4.15 to show that this product is a root of an Artin–Schreier equation $x^p + x = a$.

5.5 Algebraic closure

A field K is algebraically closed if every polynomial with coefficients in K has a root in K. For example, the complex field $\mathbb{C}$ is algebraically closed. For any field k, there exists an algebraic extension $k \subset \overline{k}$ with $\overline{k}$ algebraically closed. For example, if $k = \mathbb{Q}$ then $\overline{k}$ is the set $\{\alpha \in k \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$. For most purposes, the existence of $\overline{k}$ is unnecessary, and we haven't used it in this course; instead, we have used the notion of splitting field of a polynomial and its existence (Theorem 3.24), or simply assumed that k is contained in $\mathbb{C}$. We should give a proof in the next edition of the notes.

5.6 Transcendence degree

In Corollary 2.28 and Definition 3.7, we made the distinction of whether a field extension $k \subset K$ is algebraic or transcendental. We can take this further, and discuss how many independent transcendental elements K has over k. For example, if $t_1, \ldots, t_n$ are independent indeterminates, the function field $k(t_1, \ldots, t_n)$ has transcendence degree n over k. In general, a finite generated field extension $k \subset K$ can be obtained by choosing a *transcendence basis* $y_1, \ldots, y_n \in K$ over k, that is, a maximal set of elements of K that are algebraically independent over k. Then the remainder of the extension

$$k(y_1, \ldots, y_n) \subset K$$

is algebraic. One checks that the number n depends only on the extension $k \subset K$, and not on the choice of the y_i, then defines $n = \operatorname{tr\,deg}_k K$.

5.7 Rings of invariants and quotients in algebraic geometry

Galois theory has many applications in topology and algebraic geometry. In topology, the theory of covering spaces and the fundamental group. In algebraic and complex analytic geometry, the structure of quotients X/G of a group G acting on a variety X. The quotient variety is constructed as the topological space X/G, and functions on X/G are functions on X invariant under G. Thus $X \to X/G$ corresponds to fields and rings of invariants $k[X/G] = k[X]^G \subset k[X]$, etc. (Get on with it!)

5.8 Thorough treatment of inseparability

There are 3 or 4 equivalent characterisation of separability of a finite extension $k \subset K$ (compare Section 3.5).

(i) The minimal polynomial of any $\alpha \in K$ has distinct roots in a bigger extension L.

(ii) The number of k-homomorphisms $K \to L$ equals degree $[K : k]$.

(iii) $K \otimes_k K$ has no nilpotents.

(iv) The trace map $\mathrm{Tr}_{K/k} \colon K \to k$ defines a nondegenerate pairing $K \times K \to k$ by $(x, y) \mapsto \mathrm{Tr}_{K/k}(xy)$.

5.9 AOB

5.10 The irreducibility of the cyclotomic equation

(Taken from E. Landau, Math. Zeitschrift 1929, p. 462; communicated to me by Alan Robinson.)

Theorem 5.1 *Let $P(x) \in \mathbb{Z}[x]$ be an irreducible factor of $x^n - 1$. If $P(\xi) = 0$ then $P(\xi^r) = 0$ whenever n and r are coprime.*

Therefore the minimal polynomial of any primitive nth root of 1 has all of them as roots, so has degree $\varphi(n)$.

Proof Let η be any root of P. For any k, we have $P(\eta^k) = R(\eta)$, where $R \in \mathbb{Z}[x]$ is a well defined element, of degree $< \deg P$: only finitely many such R occur. Set

$$A = \sup\{\text{coefficients of all the } R\}.$$

For p a prime, each coefficient of the R corresponding to $P(\eta^p) = P(\eta^p) - (P(\eta))^p$ is divisible by p. If $p > A$ then $P(\eta^p) = 0$. Hence $P(\xi^m) = 0$ whenever m is not divisible by any prime $< A$. But $m = r + n \cdot \prod_{p \le A, p \nmid r} p$ satisfies the condition and is congruent to r mod n. Therefore $P(\xi^r) = 0$. $\square$

Exercises to Chapter 5

1. The final Exercises from Chapter 4 on the cyclotomic polynomial really belong here.

2. Write out an examples sheet working out all that stuff about Artin–Schreir extensions step-by-step. Work out in detail the cases $p = 2$ and $p = 3$, when the calculations are easily manageable, then find some slick way of doing the proofs in general.

Galois Theory. Sample exam

As usual, $\mathbb{Z}$ denotes the ring of integers, and $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ the fields of rational, real and complex numbers.

Q.1 Prove that a polynomial $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ which is irreducible in $\mathbb{Z}[x]$ is also irreducible in $\mathbb{Q}[x]$. [You may use the fact that if $g, h \in \mathbb{Z}[x]$ are two polynomials whose coefficients have no common factors then the product gh has the same property.]

Prove Eisenstein's criterion, that f is irreducible over $\mathbb{Z}$ if there exists a prime number p such that

(i) $p \nmid a_n$; (ii) $p \mid a_k$ for $k = 0, 1, \ldots, n-1$; and (iii) $p^2 \nmid a_0$.

Determine whether the following two polynomials are irreducible over $\mathbb{Q}$: (a) $(1/3)x^4 + 2x^3 + x + 2$; (b) $x^4 + 1$.

Q.2 Define the degree of a field extension, and state the Tower Law for field extensions. Define the notions of finite and algebraic extensions, and explain without detailed proof the relation between these; prove that given field extensions $k \subset K \subset L$, the composite extension $k \subset K$ is algebraic provided that $k \subset K$ and $K \subset L$ are both algebraic.

Let $k = \mathbb{Q}$ and $\alpha = \sqrt{2}$, and suppose that $\beta \in \mathbb{R}$ is a root of $f = x^3 - \alpha x + 1 - \alpha$; find a polynomial $g \in \mathbb{Q}[x]$ of degree 6 such that $g(\beta) = 0$.

Q.3 Let k be a field and $f \in k[x]$; explain the notion of a splitting field $k \subset K$ for f over k. Prove that a splitting field for f over k exists. Define a normal extension and explain without proof the relation between the two notions.

Suppose that $f = x^4 - 2ax^2 + b \in k[x]$ is irreducible, and let K be a splitting field for f over K; prove that the degree $[K : k]$ is either 4 or 8.

Q.4 Let $k \subset K$ be a finite field extension; define the Galois group of K over k, and say what it means for K to be a Galois extension of k. State the fundamental theorem of Galois theory.

Let K be the splitting field of $f = x^4 - 3$ over $\mathbb{Q}$. Describe the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ and its action on the 4 roots of f. List all the subgroups of G and use this to write down all the intermediate fields between $\mathbb{Q}$ and K.

References

[1] IT Adamson, Introduction to Field Theory, Oliver and Boyd.

[2] E Artin, Galois Theory, University of Notre Dame.

[3] DJH Garling, A course in Galois theory, CUP.

[4] IN Stewart, Galois Theory, Chapman and Hall.

[5] BL van der Waerden, Algebra (*or* Modern algebra), vol. 1

[6] S Lang, Algebra, Springer

[7] IR Shafarevich, Basic notions of algebra, Springer (strongly recommended as an extended essay in philosophical terms on the meaning of algebra – but it won't help much for the exam)

[8] J-P Tignol, Galois' theory of algebraic equations, World scientific (historically aware treatment of all the main issues)