FIELDS AND GALOIS THEORY

N. P. STRICKLAND

1. Fields: definitions and examples

Definition 1.1. [`defn-field`]
A *commutative ring* is a set K together with elements $0, 1 \in K$ and a definition of what it means to add or multiply two elements of K, such that:

(a) If $a, b \in K$ then $a + b \in K$ and $ab \in K$.
(b) The usual rules of algebra are valid. More explicitly, for all $a, b, c \in K$ the following equations hold:
  (1) $0 + a = a$
  (2) $a + (b + c) = (a + b) + c$
  (3) $a + b = b + a$
  (4) $0.a = 0$
  (5) $1.a = a$
  (6) $a(bc) = (ab)c$
  (7) $ab = ba$
  (8) $a(b + c) = ab + ac$
(c) For every $a \in K$ there is an element $-a$ with $a + (-a) = 0$.

A *field* is a commutative ring that satisfies the following two additional axioms:

(d) For every $a \in K$ with $a \neq 0$ there is an element $a^{-1} \in K$ with $aa^{-1} = 1$.
(e) $1 \neq 0$.

Remark 1.2. [`rem-axioms`]
The field axioms are equivalent to the following:

(a) The set K is a commutative group under addition, with 0 as the neutral element.
(b) The set $K^\times = K \setminus \{0\}$ is a commutative group under multiplication, with 1 as the neutral element.
(c) The distributivity law $a(b + c) = ab + ac$ holds for all $a, b, c \in K$.

Example 1.3. [`eg-fields-numbers`]
Recall that

$$\begin{aligned}
\mathbb{N} &= \{ \text{ natural numbers } \} = \{0, 1, 2, 3, 4, \dots\} \\
\mathbb{Z} &= \{ \text{ integers } \} = \{\dots, -2, -1, 0, 1, 2, 3, 4, \dots\} \\
\mathbb{Q} &= \{ \text{ rational numbers } \} = \{a/b \mid a, b \in \mathbb{Z}\ ,\ b \neq 0\} \\
\mathbb{R} &= \{ \text{ real numbers } \} \\
\mathbb{C} &= \{ \text{ complex numbers } \} = \{x + iy \mid x, y \in \mathbb{R}\},
\end{aligned}$$

so $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Then $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}$ are fields. The set $\mathbb{Z}$ is a ring but not a field, because axiom (d) is not satisfied: there is no element 2^{-1} *in the set* $\mathbb{Z}$ for which $2.2^{-1} = 1$. Similarly $\mathbb{N}$ is not a ring, because axiom (c) is not satisfied: there is no element -1 in the set $\mathbb{N}$ with $1 + (-1) = 0$.

Date: February 7, 2020.

Example 1.4. [eg-fields-rational]
Let K be any field, and let $K[x]$ denote the set of polynomials with coefficients in K. This is a ring but not a field (because the nonzero element $1+x \in K[x]$ does not have an inverse in $K[x]$, for example). A *rational function over K* is an expression of the form $p(x)/q(x)$, where $p(x), q(x) \in K[x]$ and $q(x) \neq 0$. These can be manipulated in an obvious way: in particular, expressions $p(x)/q(x)$ and $r(x)/s(x)$ are considered to be the same if and only if $p(x)s(x) = r(x)q(x)$. We write $K(x)$ for the set of all rational functions; this is again a field.

Lemma 1.5. [lem-domain]
Let K be a field, and let a and b be nonzero elements of K. Then $ab \neq 0$.

Proof. Suppose for a contradiction that $ab = 0$. Then we have

$$abb^{-1}a^{-1} = 0.b^{-1}a^{-1} = 0,$$

but also $abb^{-1}a^{-1} = a.1.a^{-1} = aa^{-1} = 1$. This means that $0 = 1$, which contradicts axiom (e). □

Next recall that $\mathbb{Z}/n\mathbb{Z}$ is the set of congruence classes modulo n. For each $a \in \mathbb{Z}$ we have a congruence class $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, with $\overline{a} = \overline{b}$ if and only if $a - b$ is divisible by n, so

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

There are well-defined operations of addition and multiplication, given by $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a}\,\overline{b} = \overline{ab}$.

Proposition 1.6. [prop-Zn-field]
The set $\mathbb{Z}/n\mathbb{Z}$ is always a commutative ring (under the operations mentioned above). It is a field if and only if n is prime.

Proof. The commutative ring axioms for $\mathbb{Z}/n\mathbb{Z}$ follow directly from those for $\mathbb{Z}$. Next, note that

$$\begin{aligned}
&\overline{a} \text{ has an inverse in } \mathbb{Z}/n\mathbb{Z} \\
\Leftrightarrow\ &\text{There exists } \overline{b} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \overline{a}\,\overline{b} = \overline{1} \\
\Leftrightarrow\ &\text{There exists } b \in \mathbb{Z} \text{ with } ab = 1 \pmod{n} \\
\Leftrightarrow\ &\text{There exists } b, c \in \mathbb{Z} \text{ with } ab + nc = 1 \\
\Leftrightarrow\ &a \text{ and } n \text{ are coprime.}
\end{aligned}$$

On the other hand, $\overline{a}$ is nonzero in $\mathbb{Z}/n\mathbb{Z}$ if and only if a is not divisible by n. If n is prime then any number that is not divisible by n is coprime to n, so whenever $\overline{a}$ is nonzero, it is invertible. This shows that $\mathbb{Z}/n\mathbb{Z}$ is a field. On the other hand, if n is not prime then we can write $n = ab$ for some integers $a, b > 1$. We find that a is not divisible by n but it is also not coprime with n, so $\overline{a}$ is a nonzero element of $\mathbb{Z}/n\mathbb{Z}$ that is not invertible, so $\mathbb{Z}/n\mathbb{Z}$ is not a field. □

Remark 1.7. [rem-Z-pid]
Here we have used various standard facts about divisibility and factorisation of integers. We will not review these facts in detail or prove them, but we will remark that the proofs are similar to those for divisibility and factoriasation of polynomials, which are covered in Section 4.

Definition 1.8. [defn-Fp]
If p is prime we write $\mathbb{F}_p$ as another notation for $\mathbb{Z}/p\mathbb{Z}$. We will omit the bars on elements of $\mathbb{F}_p$ unless necessary for emphasis. For example, the elements of $\mathbb{F}_5$ will usually be called $0, 1, 2, 3, 4$ rather than $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$.

The ideas in Proposition 1.6 can be generalised slightly as follows.

Definition 1.9. [defn-char]
Let K be a field. For any integer $n \geq 0$ we write $n.1$ for the sum $1 + \cdots + 1 \in K$ (with n terms). If for all $n > 0$ we have $n.1 \neq 0$ in K, we say that K has *characteristic zero*. Otherwise, the *characteristic* of K is the smallest $n > 0$ such that $n.1 = 0$ in K.

Proposition 1.10. [prop-char]
Let K be a field. Then the characteristic of K is either zero or a prime number.

Proof. If K has characteristic zero then there is nothing more to say, so we may assume that K has characteristic $p > 0$. If p is not prime then we can write $p = nm$ for some n, m with $1 < n, m < p$. Put $a = n.1$ and $b = m.1$. By definition p is the smallest positive integer with $p.1 = 0$, so we have $a \neq 0$ and $b \neq 0$. It follows by Lemma 1.5 that $ab \neq 0$, but $ab = p.1 = 0$ so this is a contradiction. It follows that p must be prime after all. □

Example 1.11. [`eg-F-four`]
Let $\mathbb{F}_4$ denote the following set of matrices over $\mathbb{F}_2$:

$$\mathbb{F}_4 = \{\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right], \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right], \left[\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right], \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]\}.$$

We will allow ourselves to write 0 for the zero matrix $\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right]$ and 1 for the identity matrix $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$. We also write $\alpha = \left[\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right]$. Note that $\alpha^2 = \left[\begin{smallmatrix}1&1\\1&2\end{smallmatrix}\right]$, which is the same as $\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]$ because we are working with matrices over $\mathbb{F}_2$. We thus have $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. One can check that $\alpha^3 = 1$ and thus $\alpha^4 = \alpha$, and also that $1 + \alpha + \alpha^2 = 0$. From this it follows that $\mathbb{F}_4$ is closed under the operations of addition and multiplication, which can be tabulated as follows:

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

From this we read off that every nonzero element of $\mathbb{F}_4$ has an inverse, namely $1^{-1} = 1$ and $\alpha^{-1} = \alpha^2$ and $(\alpha^2)^{-1} = \alpha$. This means that $\mathbb{F}_4$ is a field.

Remark 1.12. [`rem-F-q`]
Let p be a prime and n a positive integer. We will see in Section 9 that there is an an essentially unique finite field with precisely p^n different elements; this will be called $\mathbb{F}_{p^n}$. Example 1.11 is of course the case where $p = n = 2$ so $p^n = 4$.

Definition 1.13. [`defn-subfield`]
Let L be a field, and let K be a subset of L. We say that K is a *subfield* of L if

(a) 0 and 1 are elements of K.
(b) If $a, b \in K$ then $a + b \in K$ and $-a \in K$ and $ab \in K$.
(c) If $a \in K$ and $a \neq 0$ (so that there exists an inverse $a^{-1} \in L$) then $a^{-1} \in K$.

If this holds, it is clear that K is itself a field. We also say that L is an *extension* of K.

Example 1.14. [`eg-QRC`]
$\mathbb{Q}$ is a subfield of $\mathbb{R}$, which is a subfield of $\mathbb{C}$, which is a subfield of $\mathbb{C}(x)$.

We next want to discuss the first of several examples involving square roots of primes. This relies on the basic fact that such square roots are always irrational: we pause to recall the proof.

Lemma 1.15. [`lem-root-p`]
If p is prime then $\sqrt{p} \notin \mathbb{Q}$.

Proof. Suppose for a contradiction that $\sqrt{p}$ is rational. We can then write $\sqrt{p}$ in the form a/b, where a and b are integers with $b > 0$ such that a and b are coprime. We then have $(a/b)^2 = p$ in $\mathbb{Q}$, so $a^2 = pb^2$ in $\mathbb{Z}$. This shows that p divides a^2, so p must divide a, say $a = pc$. This gives $p^2c^2 = pb^2$, so $b^2 = pc^2$. This shows that b^2 is divisible by p, so b is divisible by p. Thus a and b have p as a common factor contradicting the assumption that a and b are coprime. □

Proposition 1.16. *Let p be any prime. Then the set*

$$\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$$

is a subfield of $\mathbb{R}$.

Proof. We can write 0 as $0+0\sqrt{p}$, and 1 as $1+0\sqrt{p}$, so 0 and 1 are elements of $\mathbb{Q}(\sqrt{p})$. Now suppose we have two elements $u,v\in\mathbb{Q}(\sqrt{p})$, say $u=a+b\sqrt{p}$ and $v=c+d\sqrt{p}$ with $a,b,c,d\in\mathbb{Q}$. We find that

$$\begin{aligned} u+v &= (a+c)+(b+d)\sqrt{p} \\ uv &= (ac+bdp)+(ad+bc)\sqrt{p} \end{aligned}$$

with $a+c,b+d,ac+bdp,ad+bc\in\mathbb{Q}$, so $u+v,uv\in\mathbb{Q}(\sqrt{p})$. Next, suppose that $u\neq 0$; we must show that $1/u\in\mathbb{Q}(\sqrt{p})$. There are two cases to consider, depending on whether $b=0$ or not. If $b=0$ then u is a nonzero rational number so $1/u$ is again a nonzero rational number, so $1/u\in\mathbb{Q}(\sqrt{p})$. If $b\neq 0$ we note that a/b cannot be $\pm\sqrt{p}$ (because $\sqrt{p}$ is irrational) so $(a/b)^2-p\neq 0$, so $a^2-pb^2\neq 0$. It is therefore admissible to define

$$w=\frac{a-b\sqrt{p}}{a^2-pb^2}=\left(\frac{a}{a^2-pb^2}\right)+\left(\frac{-b}{a^2-pb^2}\right)\sqrt{p}\in\mathbb{Q}(\sqrt{p}).$$

If we just expand out uw we get 1, so $w=u^{-1}$, so $u^{-1}\in\mathbb{Q}(\sqrt{p})$ as required. □

Remark 1.17. [rem-not-square]
Here and later in these notes we will mostly focus on the case where p is prime. However, many of the things that we will prove for $\mathbb{Q}(\sqrt{p})$ are also true for $\mathbb{Q}(\sqrt{d})$ whenever d is an integer that is not the square of another integer.

Proposition 1.18. [prop-subfield-meet]
Let K and L be subfields of a field M. Then $K\cap L$ is also a subfield of M.

Proof. As K is a subfield we have $0,1\in K$, and as L is a subfield we have $0,1\in L$; it follows that $0,1\in K\cap L$.

Now suppose that $a,b\in K\cap L$. As $a,b\in K$ and K is a subfield we have $a+b,a-b,ab\in K$. As $a,b\in L$ and L is a subfield we have $a+b,a-b,ab\in L$. It follows that $a+b,a-b,ab\in K\cap L$, so we see that $K\cap L$ is a subring of M. Now suppose that $a\in K\cap L$ and $a\neq 0$. As $a\in K\setminus\{0\}$ and K is a subfield, we see that $a^{-1}\in K$. As $a\in L\setminus\{0\}$ and L is a subfield, we see that $a^{-1}\in L$. It follows that $a^{-1}\in K\cap L$, so we see that $K\cap L$ is a subfield as claimed. □

Definition 1.19. [defn-field-hom]
Let R and S be commutative rings. A *ring homomorphism* from R to S is a function $\phi\colon R\to S$ satisfying

- $\phi(0)=0$ and $\phi(1)=1$.
- For all $a,b\in R$ we have $\phi(a+b)=\phi(a)+\phi(b)$ and $\phi(ab)=\phi(a)\phi(b)$ in S.

We say that ϕ is an *isomorphism* if there is another homomorphism $\psi=\phi^{-1}\colon S\to R$ with $\psi(\phi(a))=a$ for all $a\in R$, and $\phi(\psi(b))=b$ for all $b\in S$. An isomorphism from R to itself is called an *automorphism.*

It will turn out that automorphisms of fields are of central importance in Galois theory. We therefore take some time to exhibit a number of examples.

Example 1.20. [eg-conjugation]
We can define an automorphism $\phi\colon\mathbb{C}\to\mathbb{C}$ by $\phi(z)=\overline{z}$, or in other words $\phi(x+iy)=x-iy$ for all $x,y\in\mathbb{R}$.

Example 1.21. [eg-quadratic-auto]
We claim that there is an automorphism ϕ of $\mathbb{Q}(\sqrt{p})$ given by $\phi(a+b\sqrt{p})=a-b\sqrt{p}$ (for $a,b\in\mathbb{Q}$). Indeed, it is clear that this formula defines a $\mathbb{Q}$-linear map from $\mathbb{Q}(\sqrt{p})$ to itself, which satisfies $\phi(0)=0$ and $\phi(1)=1$. Suppose we have elements $u=a+b\sqrt{p}$ and $v=c+d\sqrt{p}$, with $a,b,c,d\in\mathbb{Q}$. We then have

$$\begin{aligned} uv &= (ac+bdp)+(ad+bc)\sqrt{p} \\ \phi(uv) &= \phi((ac+bdp)+(ad+bc)\sqrt{p})=(ac+bdp)-(ad+bc)\sqrt{p} \\ \phi(u)\phi(v) &= (a-b\sqrt{p})(c-d\sqrt{p})=(ac+bdp)-(ad+bc)\sqrt{p} \end{aligned}$$

so $\phi(uv)=\phi(u)\phi(v)$. This shows that ϕ is a homomorphism of fields. It is also clear that

$$\phi(\phi(a+b\sqrt{p}))=\phi(a-b\sqrt{p})=a+b\sqrt{p},$$

so ϕ is an inverse for itself, so ϕ is an automorphism.

Example 1.22. [eg-mobius-aut]
We can define an automorphism $\tau\colon \mathbb{C}(x) \to \mathbb{C}(x)$ by $\tau(r(x)) = r(x+1)$, so for example

$$\tau\left(\frac{x^2+1}{x^3-1}\right) = \frac{(x+1)^2+1}{(x+1)^3-1} = \frac{x^2+2x+2}{x^3+3x^2+3x}.$$

More generally, given any $a, b, c, d \in \mathbb{C}$ with $ad - bc \neq 0$ we can define an automorphism θ of $\mathbb{C}(x)$ by

$$\theta(r(x)) = r\left(\frac{ax+b}{cx+d}\right).$$

It can be shown that this construction gives all the automorphisms of $\mathbb{C}(x)$ that act as the identity on $\mathbb{C}$. Thus, the group of such automorphisms is the same as the group of Möbius transformations.

Example 1.23. [eg-generic-quintic-i]
Consider the quintic $f(x) = x^5 - 6x + 3$. This has five roots in $\mathbb{C}$, approximately as follows:

$$\begin{aligned}
\alpha_1 &= -1.670935264 \\
\alpha_2 &= -0.1181039226 - 1.587459162i \\
\alpha_3 &= -0.1181039226 + 1.587459162i \\
\alpha_4 &= 0.5055012304 \\
\alpha_5 &= 1.401641879.
\end{aligned}$$

Let K be the subfield of $\mathbb{C}$ generated by these roots. It turns out that the automorphisms of K are essentially the same as the permutations of $\{1, 2, \dots, 5\}$. For example, corresponding to the transposition $(4\ 5)$ there is a unique automorphism ϕ with $\phi(\alpha_4) = \alpha_5$ and $\phi(\alpha_5) = \alpha_4$ and $\phi(\alpha_k) = \alpha_k$ for $k = 1, 2, 3$. Moreover, most (but not all) other quintics behave in essentially the same way. All this will be explained with proofs in Example 7.9.

Example 1.24. [eg-cyclotomic-i]
Fix an integer $n > 1$, put $\zeta = e^{2\pi i/n} \in \mathbb{C}$, and let K be the subfield of $\mathbb{C}$ generated by ζ. We will see in Section 8 that whenever k is coprime to n there is a unique automorphism ϕ_k of K that satisfies $\phi_k(\zeta) = \zeta^k$. Using this we will see that the group of automorphisms of K is isomorphic to the group of invertible elements in the ring $\mathbb{Z}/n\mathbb{Z}$.

Proposition 1.25. [prop-aut-Q]
The only automorphism of $\mathbb{Q}$ is the identity, and the only automorphism of $\mathbb{R}$ is the identity.

Proof. Let ϕ be an automorphism of $\mathbb{Q}$. By definition we have $\phi(0) = 0$ and $\phi(1) = 1$. If $\phi(n) = n$ for some $n \in \mathbb{N}$ then

$$\phi(n+1) = \phi(n) + \phi(1) = n + 1.$$

It follows by induction that $\phi(n) = n$ for all $n \in \mathbb{N}$. We also have $n + \phi(-n) = \phi(n) + \phi(-n) = \phi(n + (-n)) = \phi(0) = 0$, which can be rearranged to give $\phi(-n) = -\phi(n)$. This shows that $\phi(a) = a$ for all $a \in \mathbb{Z}$. Next, an arbitrary rational number q can be written as $q = a/b$ with $a, b \in \mathbb{Z}$ and $b > 0$. This gives $qb = a$ so $\phi(q)\phi(b) = \phi(qb) = \phi(a)$, but $a, b \in \mathbb{Z}$ so $\phi(a) = a$ and $\phi(b) = b$, so $\phi(q)b = a$. This rearranges to give $\phi(q) = a/b = q$, so ϕ is the identity as claimed.

Now instead let ϕ be an automorphism of $\mathbb{R}$. Just as before, we see that $\phi(q) = q$ for all $q \in \mathbb{Q}$. Next, we claim that if $a \leq b$ then $\phi(a) \leq \phi(b)$. Indeed, if $a \leq b$ then $b - a \geq 0$ so $b - a = t^2$ for some $t \in \mathbb{R}$, or equivalently $a + t^2 = b$. We can apply ϕ to get $\phi(a) + \phi(t)^2 = \phi(b)$, and all squares are nonnegative so $\phi(a) \leq \phi(b)$. Now let r be an arbitrary real number. For any $\epsilon > 0$ we can choose rational numbers q_1 and q_2 such that $q_1 \leq r \leq q_2$ with $q_2 - q_1 < \epsilon$. We can then apply ϕ, recalling that ϕ preserves order and acts as the identity on rational numbers. That gives $q_1 \leq \phi(r) \leq q_2$, which implies that $|r - \phi(r)| < \epsilon$. This holds for all $\epsilon > 0$, so we must actually have $\phi(r) = r$ as claimed. □

Proposition 1.26. [prop-Hom-C-R]
There are no homomorphisms from $\mathbb{C}$ to $\mathbb{R}$.

Proof. Suppose we had a homomorphism $\phi\colon \mathbb{C} \to \mathbb{R}$. Put $a = \phi(i) \in \mathbb{R}$. We could then apply ϕ to the equation $i^2 + 1 = 0$ to get $a^2 + 1 = 0$. This is clearly not possible for a real number a, so there cannot be any such homomorphism ϕ. □

For the next result we recall the following definitions, which should hopefully be very familiar:

Definition 1.27. [`defn-jective`]
Let X and Y be sets, and let ϕ be any function from X to Y.

(a) We say that ϕ is *injective* for whenever $x, x' \in X$ and $\phi(x) = \phi(x')$, we have $x = x'$.
(b) We say that ϕ is *surjective* if for every element $y \in Y$, there is an element $x \in X$ with $\phi(x) = y$.
(c) We say that ϕ is *bijective* if it is both injective and surjective.

Remark 1.28. [`rem-bijective`]
It is standard that ϕ is bijective if and only if there is an inverse map $\psi = \phi^{-1}\colon Y \to X$ with $\psi(\phi(x)) = x$ for all $x \in X$, and $\phi(\psi(y)) = y$ for all $y \in Y$.

Proposition 1.29. [`prop-hom-inj`]
Let $\phi\colon K \to L$ be a field homomorphism.

(a) *If $a \in K^\times = K \setminus \{0\}$, then $\phi(a) \in L^\times$ and $\phi(a^{-1}) = \phi(a)^{-1}$.*
(b) *The map ϕ is injective, and the image $\phi(K)$ is a subfield of L.*

Proof. If $a \in K$ is nonzero then we can find an inverse element $a^{-1} \in K$ and we have

$$\phi(a).\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1) = 1.$$

It follows from this that $\phi(a)$ must be nonzero, and $\phi(a^{-1}) = \phi(a)^{-1}$ as claimed.

Now suppose we have elements $a, b \in K$ with $a \neq b$. This means that $a - b \neq 0$, so by the above we have $\phi(a - b) \neq 0$, but $\phi(a - b) = \phi(a) - \phi(b)$, so we conclude that $\phi(a) \neq \phi(b)$. This proves that ϕ is injective.

Next, we have $\phi(0_K) = 0_L$ and $\phi(1_K) = 1_L$, so 0_L and 1_L are in the image of ϕ. If u and v are in the image of ϕ then we have $u = \phi(a)$ and $v = \phi(b)$ for some $a, b \in K$, so $u \pm v = \phi(a \pm b)$ and $uv = \phi(ab)$. This shows that the image of ϕ is closed under addition, subtraction and multiplication, so it is a subring of L. Now suppose that $u = \phi(a)$ again, and that $u \neq 0$. It follows that a must be nonzero, and as at the beginning of this proof we see that $\phi(a^{-1})$ is an inverse for u lying in the image of ϕ. This completes the proof that the image is a subfield. □

Remark 1.30. [`rem-hom-inj`]
If we are studying a problem that involves only one homomorphism $\phi\colon K \to L$, we will often identify K with $\phi(K)$ and thus consider K itself as a subfield of L. This generally leads to more concise and convenient notation. However, this convention can lead to confusion in cases where we need to consider more than one homomorphism from K to L, so we will not adopt it everywhere.

Proposition 1.31. [`prop-fixed-subfield`]
Let H be a set of homomorphisms $L \to L$, and put

$$L^H = \{a \in L \mid \phi(a) = a \text{ for all } \phi \in H\}.$$

Then L^H is a subfield of L.

Proof. For any homomorphism ϕ, we have $\phi(0) = 0$ and $\phi(1) = 1$. It follows that $0, 1 \in L^H$. Next, suppose we have $a, b \in L^H$, and consider $\phi \in H$. As ϕ is a homomorphism, we have $\phi(a \pm b) = \phi(a) \pm \phi(b)$. As $a, b \in L^H$ we also have $\phi(a) = a$ and $\phi(b) = b$, so $\phi(a \pm b) = a \pm b$. This holds for all $\phi \in H$, so we conclude that $a \pm b \in L^H$. Essentially the same argument shows that $ab \in L^H$. Also, if $a \neq 0$ we see (from Proposition 1.29(a)) that $\phi(a^{-1}) = \phi(a)^{-1} = a^{-1}$ for all $\phi \in H$, so $a^{-1} \in L^H$. This shows that L^H is a subfield. □

Proposition 1.32. [`prop-hom-char`]

(a) *Suppose that there exists a homomorphism $\phi\colon K \to L$. Then K and L have the same characteristic.*
(b) *Suppose that K has characteristic zero. Then there is a unique homomorphism $\phi\colon \mathbb{Q} \to K$.*

(c) *Suppose instead that K has characteristic $p > 0$. Then there is a unique homomorphism $\phi\colon \mathbb{F}_p \to K$.*

Proof.

(a) Put $I = \{n \in \mathbb{Z} \mid n.1_K = 0\}$ and $J = \{n \in \mathbb{Z} \mid n.1_L = 0\}$. As I determines the characteristic of K, and J determines the characteristic of L, it will suffice to show that $I = J$. As ϕ is a homomorphism we have $\phi(1_K) = 1_L$ and so $\phi(n.1_K) = n.1_L$. In particular, if $n \in I$ then $n.1_L = \phi(n.1_K) = \phi(0) = 0$ and so $n \in J$; thus $I \leq J$. Conversely, if $n \in J$ then $\phi(n.1_K) = n.1_L = 0$, but ϕ is injective by Proposition 1.29, so $n.1_K = 0$, so $n \in I$. This shows that $J \leq I$ and so $I = J$ as required.

(b) This is related to proposition 1.25. Suppose that K has characteristic zero. We can certainly define $\phi_0\colon \mathbb{N} \to K$ by $\phi_0(n) = 1 + \cdots + 1$ (with n terms). We can then extend this over $\mathbb{Z}$ by $\phi_0(-n) = -\phi_0(n)$, and one can check that the resulting map $\phi_0\colon \mathbb{Z} \to K$ is a homomorphism. As K has characteristic zero, we know that $\phi_0(b)$ is invertible for all positive integers b. Any rational number $x \in \mathbb{Q}$ can be written as $x = a/b$ for some $a, b \in \mathbb{Z}$ with $b > 0$. We then put $\phi(x) = \phi_0(a)\phi_0(b)^{-1}$. This is well-defined, because if x is also c/d then $ad = bc$ in $\mathbb{Z}$, and $\phi_0\colon \mathbb{Z} \to K$ is a homomorphism, so $\phi_0(a)\phi_0(d) = \phi_0(b)\phi_0(c)$, so $\phi_0(a)\phi_0(b)^{-1} = \phi_0(c)\phi_0(d)^{-1}$. We leave it to the reader to check that this gives a homomorphism $\phi\colon \mathbb{Q} \to K$, and that it is the unique such homomorphism.

(c) Now suppose instead that K has characteristic $p > 0$. We again have a unique homomorphism $\phi_0\colon \mathbb{Z} \to K$. By assumption we have $\phi_0(p) = 0$, but $\phi_0(k) \neq 0$ for $0 < k < p$. We would like to define $\phi\colon \mathbb{F}_p \to K$ by $\phi(\overline{n}) = \phi_0(n)$. To check that this is well-defined, we must show that $\phi_0(n) = \phi_0(m)$ whenever $\overline{n} = \overline{m}$. If $\overline{n} = \overline{m}$ then we must have $n = m + kp$ for some $k \in \mathbb{Z}$ so $\phi_0(n) = \phi_0(m) + \phi_0(k)\phi_0(p) = \phi_0(m) + \phi_0(k).0 = \phi_0(m)$ as required. This gives a function $\phi\colon \mathbb{F}_p \to K$, and one can easily check that it is a homomorphism, and indeed that it is the only homomorphism.

□

Exercises

Exercise 1.1. [`ex-which-fields`]
Which of the following sets (with the usual definition of addition and multiplication) are fields?

$$\begin{aligned}
K_0 &= \{x \in \mathbb{R} \mid x \geq 0\} \\
K_1 &= \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \\
K_2 &= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \\
K_3 &= \{a + b\sqrt{2} \mid a, b \in \mathbb{R}\} \\
K_4 &= \{a + b.2^{1/3} \mid a, b \in \mathbb{Q}\} \\
K_5 &= \mathbb{Q} \times \mathbb{R} = \{(a, b) \mid a \in \mathbb{Q} \text{ and } b \in \mathbb{R}\} \\
K_6 &= \mathbb{Z}/6\mathbb{Z} \\
K_7 &= \mathbb{Z}/7\mathbb{Z}
\end{aligned}$$

Exercise 1.2. [`ex-Ri-field`]
For any ring R we can construct a new ring $R[i]$ of "complex numbers over R": the elements are expressions $a + bi$ with $a, b \in R$, and the multiplication rule is

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

so that $i^2 = -1$. Prove that $\mathbb{F}_3[i]$ is a field, but $\mathbb{F}_2[i]$ and $\mathbb{F}_5[i]$ are not.

Exercise 1.3. [`ex-Qp-subfields`]
Show that the only subfields of $\mathbb{Q}(\sqrt{p})$ are $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{p})$.

Exercise 1.4. [ex-nth-root-aut]
Let n be an odd prime, and $a \in \mathbb{Q}$. Show that there are no non-trivial automorphisms of $\mathbb{Q}(a^{1/n})$.

Exercise 1.5. [ex-aut-F-four]
Consider the field $\mathbb{F}_4$ from Example 1.11. This has precisely one automorphism that is not the identity; what is it?

Exercise 1.6. [ex-equaliser]
Let L and M be fields, and suppose we have two homomorphisms $\phi, \psi \colon L \to M$. Show that the set $K = \{a \in L \mid \phi(a) = \psi(a)\}$ is a subfield of L.

Exercise 1.7. [ex-product-ring]
Let K_0 and K_1 be fields. Show that $K_0 \times K_1$ is a commutative ring but not a field. (You should check a representative sample of the ring axioms, but not necessarily the whole list.)

2. Vector spaces

Definition 2.1. [defn-vector-space]
A vector space over a field K is a set V, together with an element $0 \in V$ and a definition of what it means to add elements of V or multiply them by elements of K, such that

(a) If u and v are elements of V, then $u + v$ is an also an element of V.
(b) If v is an element of V and t is an element of K, then tv is an element of V.
(c) For any elements $u, v, w \in V$ and any elements $s, t \in K$, the following equations hold:
  (1) $0 + v = v$
  (2) $u + v = v + u$
  (3) $u + (v + w) = (u + v) + w$
  (4) $0u = 0$
  (5) $1u = u$
  (6) $(st)u = s(tu)$
  (7) $(s + t)u = su + tu$
  (8) $s(u + v) = su + sv$.

Example 2.2. [eg-Kn-vs]
We write K^n for the set of column vectors of length n with entries in K. We define addition and scalar multiplication in the obvious way: for $n = 4$ this reduces to

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix} = \begin{bmatrix} u_1+v_1 \\ u_2+v_2 \\ u_3+v_3 \\ u_4+v_4 \end{bmatrix} \qquad t \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} = \begin{bmatrix} tu_1 \\ tu_2 \\ tu_3 \\ tu_4 \end{bmatrix}.$$

This makes K^n into a vector space over K.

Example 2.3. [eg-MnK-vs]
We write $M_n(K)$ for the set of $n \times n$ matrices with entries in K. We define addition and scalar multiplication in the obvious way: for $n = 2$ this reduces to

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \qquad t \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ta & tb \\ tc & td \end{bmatrix}.$$

This makes $M_n(K)$ into a vector space over K.

Example 2.4. [eg-rational-vs]
Recall that $K[x]$ is the set of all polynomials over K. We can add together two polynomials to get a new polynomial, or we can multiply a polynomial by an element of K to get a new polynomial, and these operations satisfy all the usual algebraic rules. Thus, $K[x]$ is a vector space over K. The field $K(x)$ (of rational functions over K, as in example 1.4) is also a vector space over K.

Example 2.5. [eg-R-C-vs]
We can add together two complex numbers to get a new complex number, or we can multiply a complex number by a real number to get a new complex number, and these operations satisfy all the usual algebraic rules. Thus, $\mathbb{C}$ is a vector space over $\mathbb{R}$. It can of course be identified with $\mathbb{R}^2$ by the usual rule $a+bi \leftrightarrow \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$.

Example 2.6. [eg-extension-vs]
More generally, whenever L is a field and K is a subfield, we can regard L as a vector space over K. Example 2.4 includes the case where $L = K(x)$, and Example 2.5 is the case where $K = \mathbb{R}$ and $L = \mathbb{C}$. Examples of this type will be very important in our study of the structure of fields.

Remark 2.7. [rem-different-fields]
The same set can often be regarded as a vector space over many different fields. For example, the set $\mathbb{C}(x)$ can be regarded as a vector space over $\mathbb{Q}$, a vector space over $\mathbb{R}$, a vector space over $\mathbb{C}$ or a vector space over $\mathbb{C}(x)$ itself. These different points of view can all be useful for different purposes, and there is no contradiction between them.

Definition 2.8. [defn-subspace]
Let V be a vector space over a field K. A *vector subspace* (or just *subspace*) of V is a subset $W \subseteq V$ such that

(a) $0 \in W$
(b) Whenever u and v lie in W, the element $u+v$ also lies in W. (In other words, W is closed under addition.)
(c) Whenever u lies in W and t lies in K, the element tu also lies in W. (In other words, W is closed under scalar multiplication.)

These conditions mean that W is itself a vector space.

Definition 2.9. [defn-linear]
Let V and W be vector spaces over a field K, and let $\phi\colon V \to W$ be a function (so for each element $v \in V$ we have an element $\phi(v) \in W$). We say that ϕ is *linear* if

(a) For any v and v' in V, we have $\phi(v+v') = \phi(v) + \phi(v')$ in W.
(b) For any $t \in K$ and $v \in V$ we have $\phi(tv) = t\phi(v)$ in W.

By taking $t = v = 0$ in (b), we see that a linear map must satisfy $\phi(0) = 0$. Further simple arguments also show that $\phi(v - v') = \phi(v) - \phi(v')$.

Remark 2.10. [rem-linear]
One can check that ϕ is linear if and only if it satisfies the single axiom that $\phi(tv + t'v') = t\phi(v) + t\phi(v')$ for all $t, t' \in K$ and $v, v' \in V$.

Definition 2.11. [defn-ker-img]
Let $\phi\colon V \to W$ be a linear map of vector spaces over a field K. We put

$$\begin{aligned} \ker(\phi) &= \{v \in V \mid \phi(v) = 0\} \subseteq V \\ \operatorname{image}(\phi) &= \{\phi(v) \mid v \in V\} \subseteq W. \end{aligned}$$

Remark 2.12. [rem-ker-img]
It is not hard to see that $\ker(\phi)$ and $\operatorname{image}(\phi)$ are subspaces of V and W respectively. Moreover, ϕ is injective iff $\ker(\phi) = 0$, and ϕ is surjective iff $\operatorname{image}(\phi) = W$.

Definition 2.13. [defn-basis]
Let K be a field, let V be a vector space over K, and let $\mathcal{V} = v_1, \dots, v_n$ be a finite list of elements of V. We define a map $\mu_{\mathcal{V}}\colon K^n \to V$ by $\mu_{\mathcal{V}}(\lambda) = \sum_i \lambda_i v_i$.

- We say that $\mathcal{V}$ is *linearly independent* if $\ker(\mu_{\mathcal{V}}) = 0$, or equivalently, $\mu_{\mathcal{V}}$ is injective.
- We say that $\mathcal{V}$ *spans* V if $\operatorname{image}(\mu_{\mathcal{V}}) = V$, or equivalently, $\mu_{\mathcal{V}}$ is surjective.
- We say that $\mathcal{V}$ is a *basis* for V if it is linearly independent and it also spans.
- It can be shown that if V has a basis then all bases have the same length; we call this length the *dimension* of V over K, and write it as $\dim_K(V)$. If V has no basis then we say that the dimension is infinite.

We recall without proof some basic facts about these concepts:

Proposition 2.14. [thm-vect-misc]
Let K be a field, and let V be a vector space of dimension $d < \infty$ over K.

(a) *Any linearly independent list in V has length at most d.*
(b) *Any spanning list in V has length at least d.*
(c) *Any linearly independent list of length d is a basis. More generally, if $\mathcal{V}$ is a linearly independent list of length less than d then we can add extra elements on the end to make a basis.*
(d) *Any spanning list of length d is also a basis.* □

Example 2.15. [eg-dim]
K^n has dimension n over K, and $M_n(K)$ has dimension n^2. The spaces $K[x]$ and $K(x)$ have infinite dimension over K.

Example 2.16. [eg-dim-R-Cn]
$\mathbb{C}$ has dimension two over $\mathbb{R}$. If we put

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \qquad e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \qquad e_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

then the list e_1, e_2, e_3 is a basis for $\mathbb{C}^3$ over $\mathbb{C}$, so $\dim_{\mathbb{C}}(\mathbb{C}^3) = 3$, as mentioned in the previous example. However, we can also regard $\mathbb{C}^3$ as a vector space over $\mathbb{R}$, and the list e_1, e_2, e_3 does not span $\mathbb{C}^3$ over $\mathbb{R}$, so it is not a basis. Instead, we can use the formula

$$\begin{bmatrix} x_1+iy_1 \\ x_2+iy_2 \\ x_3+iy_3 \end{bmatrix} = x_1e_1 + y_1(ie_1) + x_2e_2 + y_2(ie_2) + x_3e_3 + y_3(ie_3)$$

to show that the list $e_1, ie_1, e_2, ie_2, e_3, ie_3$ is a basis for $\mathbb{C}^3$ over $\mathbb{R}$, so $\dim_{\mathbb{R}}(\mathbb{C}^3) = 6$. In exactly the same way, we have $\dim_{\mathbb{R}}(\mathbb{C}^n) = 2n$ for all $n \geq 0$.

Remark 2.17. [rem-partial-fractions]
We have set up our definitions so that bases are by definition finite lists. It is also possible to set up a theory of infinite bases, but this involves some subtleties that we will not take the time to explain. It then works out that the set $\mathcal{X} = \{x^n \mid n \geq 0\}$ is a basis for $\mathbb{C}[x]$ over $\mathbb{C}$. Moreover, using the Fundamental Theorem of Algebra (Theorem 4.31) and the theory of partial fractions one can show that the (uncountable) set

$$\mathcal{X} \cup \{(x-\lambda)^{-n} \mid \lambda \in \mathbb{C},\ n > 0\}$$

is a basis for $\mathbb{C}(x)$ over $\mathbb{C}$.

Definition 2.18. [defn-extension-degree]
If K is a subfield of L, then we write $[L : K] = \dim_K(L)$, the dimension of L considered as a vector space over K. We also say that L is an *extension* of K, and the number $[L : K]$ is called the *degree* of the extension.

Definition 2.19. [defn-hom-degree]
For a slightly more general picture, suppose we have two fields K and L and a homomorphism $\phi \colon K \to L$. Then the image $\phi(K)$ is a subfield of L, so we have a (possibly infinite) number $[L : \phi(K)]$. We write $\deg(\phi)$ for this, and call it the degree of ϕ.

Example 2.20. [eg-degrees]
The list $1, i$ is a basis for $\mathbb{C}$ over $\mathbb{R}$, so $[\mathbb{C} : \mathbb{R}] = 2$. Similarly, the list $1, \sqrt{p}$ is a basis for $\mathbb{Q}(\sqrt{p})$ over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$. More generally, for any $n > 1$ we can consider the field $K = \mathbb{Q}(p^{1/n})$ and we find that the list $1, p^{1/n}, p^{2/n}, \dots, p^{(n-1)/n}$ is a basis for K over $\mathbb{Q}$, so $[K : \mathbb{Q}] = n$. We can also consider a second prime $q \neq p$ and the field $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ generated by $\sqrt{p}$ and $\sqrt{q}$. We will check in Proposition 7.2 that the list $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$ is a basis for L over $\mathbb{Q}$, so $[L : \mathbb{Q}] = 4$.

Example 2.21. [eg-infinite-degree]
On the other hand, it can be shown that $[\mathbb{R} : \mathbb{Q}] = \infty$. One proof of this uses the theory of countability: standard methods show that $\mathbb{Q}^n$ is countable for all n but $\mathbb{R}$ is uncountable, so $\mathbb{R}$ cannot be isomorphic to $\mathbb{Q}^n$ for any n. Another proof uses the fact (which we shall not justify) that the powers $1, e, e^2, \dots$ (where $e \simeq 2.71828$ is the base of natural logarithms) are linearly independent over $\mathbb{Q}$. A third proof uses Section 10

below. It follows from results given there that the list $\sqrt{2}, \sqrt{3}, \sqrt{7}, \sqrt{11}, \dots$ (of square roots of all primes) is linearly independent over $\mathbb{Q}$, which would not be possible if $[\mathbb{R} : \mathbb{Q}]$ were finite.

Proposition 2.22. [prop-degree-product]
If K is a subfield of L and L is a subfield of M then $[M : L][L : K] = [M : K]$. More precisely, if $\alpha_1, \dots, \alpha_n$ is a basis for L over K (so that $[L : K] = n$) and $\beta_1, \dots, \beta_m$ is a basis for M over L (so that $[M : L] = m$) then the nm elements $\alpha_i\beta_j$ form a basis for M over K.

Remark 2.23. [rem-degree-product]
We will prove this under the assumption that m and n are finite. It is also true that if L has infinite dimension over K or M has infinite dimension over L then M has infinite dimension over K. We leave this as an exercise.

Proof. Consider an element $u \in M$. As the elements β_j span M over L, there must exist elements $v_1, \dots, v_m \in L$ with $u = \sum_j v_j\beta_j$. Now $v_j \in L$ and the elements $\alpha_1, \dots, \alpha_n$ span L over K, so there must exist elements $w_{1j}, \dots, u_{nj} \in K$ with

$$v_j = w_{1j}\alpha_1 + w_{2j}\alpha_2 + \dots + w_{nj}\alpha_n = \sum_{i=1}^{n} w_{ij}\alpha_i.$$

It follows that

$$u = \sum_{j=1}^{m} v_j\beta_j = \sum_{j=1}^{m}\sum_{i=1}^{n} w_{ij}\alpha_i\beta_j.$$

This shows that u is a K-linear combination of the elements $\alpha_i\beta_j$, so these elements span M over K.

We now need to prove that these elements are linearly independent. This essentially just reverses the steps already taken. In detail, a linear relation between the elements $\alpha_i\beta_j$ is a system of elements $w_{ij} \in K$ for which $\sum_{i,j} w_{ij}\alpha_i\beta_j$ is zero. If we put $v_j = \sum_i w_{ij}\alpha_i$ then the relation can be written as $\sum_j v_j\beta_j = 0$. Here $v_j \in L$ and the elements β_j are assumed to be linearly independent over L, so we must have $v_j = 0$ for all j. This means that $\sum_i w_{ij}\alpha_i = 0$, and here $w_{ij} \in K$ and the elements α_i are assumed to be linearly independent over K, so we must have $w_{ij} = 0$ for all i and j, so our original linear relation between the elements $\alpha_i\beta_j$ is the trivial relation. □

We can restate the same fact in different notation as follows:

Corollary 2.24. [cor-degree-product]
Let K, L and M be fields, and let $K \xrightarrow{\phi} L \xrightarrow{\psi} M$ be homomorphisms of fields. Then $\deg(\psi\phi) = \deg(\psi)\deg(\psi)$.

Proof. Put $K' = \phi(K) \leq L$ and $K'' = \psi(K') \leq M$ and $L'' = \psi(L) \leq M$, so

$$\deg(\phi) = [L : K'] \qquad \deg(\psi) = [M : L''] \qquad \deg(\psi\phi) = [M : K''].$$

The previous proposition tells us that $[M : K''] = [M : L''][L'' : K'']$, so $\deg(\psi\phi) = \deg(\psi)[L'' : K'']$, so it will be enough to prove that $[L'' : K''] = [L : K']$. The homomorphism ψ gives an isomorphism $L \to L''$ that carries K' to K''. It is straightforward to check that a list $\alpha_1, \dots, \alpha_d$ is a basis for L over K' if and only if $\psi(\alpha_1), \dots, \psi(\alpha_d)$ is a basis for L'' over K'', and this means that $[L'' : K''] = [L : K']$ as claimed.

The fields considered can be displayed as follows:

$$\begin{tikzcd}
 & & M \\
 & L \arrow[ur, "\psi"] \arrow[r, "\simeq", "\psi"'] & L'' \arrow[u, tail, "\subseteq"'] \\
K \arrow[ur, "\phi"] \arrow[r, "\simeq", "\phi"'] & K' \arrow[u, tail, "\subseteq"'] \arrow[r, "\simeq", "\psi"'] & K'' \arrow[u, tail, "\subseteq"']
\end{tikzcd}$$

□

Proposition 2.25. [prop-deg-one]
A homomorphism $\phi \colon K \to L$ is an isomorphism if and only if $\deg(\phi) = 1$.

Proof. Put $K' = \phi(K)$ as before, so ϕ gives an isomorphism $K \to K'$, so the question is whether $K' = L$ or not. If $\deg(\phi) = 1$, then L has dimension one over K', so any nonzero element of L gives a basis for L over K'. In particular, the element 1 gives a basis for L over K', so $L = K'.1 = K'$ as required. The converse is also clear. □

Exercises

Exercise 2.1. [`ex-which-linear`]
Which of the following maps are $\mathbb{C}$-linear?

- The map $\phi_0 \colon M_2(\mathbb{C}) \to M_2(\mathbb{C})$ given by $\phi_0(A) = A^2$.
- The map $\phi_1 \colon M_2(\mathbb{C}) \to M_2(\mathbb{C})$ given by $\phi_1(A) = A - A^T$.
- The map $\phi_2 \colon \mathbb{C}^2 \to \mathbb{C}[x]$ given by $\phi_2 \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] = ax + bx^2$
- The map $\phi_3 \colon \mathbb{C}^2 \to \mathbb{C}[x]$ given by $\phi_3 \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] = ax + (bx)^2$
- The map $\phi_4 \colon \mathbb{C}[x] \to \mathbb{C}^2$ given by $\phi_4(f(x)) = \left[\begin{smallmatrix} f(2) \\ f(-2) \end{smallmatrix}\right]$
- The map $\phi_5 \colon \mathbb{C}[t] \to \mathbb{C}$ given by $\phi(f(x)) = f(0)f(1)f(2)$.

Exercise 2.2. [`ex-degrees-possible`]
Do there exist fields K, L, M with $\mathbb{Q} < K < M$ and $\mathbb{Q} < L < M$ and degrees as follows?

$$[K : \mathbb{Q}] = 3 \qquad [L : \mathbb{Q}] = 4 \qquad [M : L] = 5 \qquad [M : K] = 7.$$

Exercise 2.3. [`ex-find-degrees`]
Suppose we have fields $K < L < M < N$ (all different) such that $[M : K] = 6$ and $[N : L] = 15$. Find $[L : K]$, $[M : L]$ and $[N : M]$.

Exercise 2.4. [`ex-basis-i`]
Recall that the *trace* of a square matrix is the sum of the diagonal entries. Find a basis for the space

$$V = \{M \in M_3(\mathbb{C}) \mid M^T = M \text{ and } \operatorname{trace}(M) = 0\}$$

(considered as a vector space over $\mathbb{C}$).

Exercise 2.5. [`ex-matrix-subspaces`]
Recall that for a matrix $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in M_2(\mathbb{C})$, we write $A^\dagger = \left[\begin{smallmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{smallmatrix}\right]$. Put $V = \{A \in M_2(\mathbb{C}) \mid A + A^\dagger = 0\}$.

(a) Show that if we consider $M_2(\mathbb{C})$ as a vector space over $\mathbb{C}$, then V is not a subspace.
(b) Show that if we consider $M_2(\mathbb{C})$ as a vector space over $\mathbb{R}$, then V is a subspace of dimension 4.

Exercise 2.6. [`ex-rational-extension`]
Let L be the field $\mathbb{C}(x)$ of rational functions of x, and let K be the subfield $\mathbb{C}(x^n)$. Prove that $[L : K] = n$.

3. Ideals and quotient rings

Definition 3.1. [`defn-ideal`]
Let R be a commutative ring. An *ideal* in R is a subset $I \subseteq R$ such that

(a) $0 \in I$
(b) If $a, b \in I$ then $a + b \in I$
(c) If $a \in R$ and $b \in I$ then $ab \in I$.

For any element $x \in R$, the set $Rx = \{ax \mid a \in R\}$ is an ideal in R; ideals of this form are called *principal* ideals, and we say that x is a *generator* of Rx.

Remark 3.2. [rem-ideal-subtract]
If $b \in I$ then $-b = (-1).b \in I$ by the case $a = -1$ of axiom (c). It follows that if $a, b \in I$ then $a - b = a + (-b) \in I$ by axiom (b).

Example 3.3. [eg-silly-ideals]
In any ring R, the subsets $\{0\}$ and R itself are ideals. These are both principal, because $\{0\} = R.0$ and $R = R.1$.

Example 3.4. [eg-field-ideals]
Now let K be a field. We claim that $\{0\}$ and K are the *only* ideals in K. Indeed, let I be an ideal that is different from $\{0\}$. Then there is a nonzero element $b \in I$. As K is a field, there is an inverse element $b^{-1} \in K$. Now Axiom (c) tells us that $b^{-1}b \in I$, or in other words $1 \in I$. Now for any element $a \in K$ we can use Axiom (c) again to see that $a.1 \in I$, or in other words $a \in I$; so $I = K$.

Example 3.5. [eg-poly-ideals]
Consider the following subsets of $\mathbb{R}[x]$:

$$\begin{aligned}
I_0 &= \{f(x) \mid f(0) = 1\} \\
I_1 &= \{f(x) \mid f(0) = f(1)\} \\
I_2 &= \{f(x) \mid f(0)f(1) = 0\} \\
I_3 &= \{f(x) \mid f(0) = f'(0) = f(1) = 0\}.
\end{aligned}$$

We claim that I_3 is an ideal, but that the other sets are not. Indeed, the zero polynomial does not lie in I_0, so Axiom (a) is violated. The constant polynomial 1 lies in I_1, but $x.1$ is not in I_1, so Axiom (c) is violated. The polynomials x and $1 - x$ both lie in I_2 but $x + (1 - x)$ does not, so Axiom (b) is violated. However, it is clear that $0 \in I_3$. If $f(x), g(x) \in I_3$ and $h(x) = f(x) + g(x)$ then

$$\begin{aligned}
h(0) &= f(0) + g(0) = 0 + 0 = 0 \\
h'(0) &= f'(0) + g'(0) = 0 + 0 = 0 \\
h(1) &= f(1) + g(1) = 0 + 0 = 0
\end{aligned}$$

so $h \in I_3$. Similarly, if $f(x) \in \mathbb{R}[x]$ and $g(x) \in I_3$ and $h(x) = f(x)g(x)$ then $g(0) = g'(0) = g(1) = 0$ and $h'(x) = f'(x)g(x) + f(x)g'(x)$ so

$$\begin{aligned}
h(0) &= f(0)g(0) = f(0).0 = 0 \\
h'(0) &= f'(0)g(0) + f(0)g'(0) = f'(0).0 + f(0).0 = 0 \\
h(1) &= f(1)g(1) = f(1).0 = 0,
\end{aligned}$$

so again $h \in I_3$. Thus all axioms are satisfied and I_3 is an ideal. In fact it is not hard to see that $I_3 = \mathbb{R}[x].(x^3 - x^2)$, so I_3 is a principal ideal.

Proposition 3.6. [prop-ker-ideal]
Let $\phi \colon R \to S$ be a homomorphism of rings, and put $\ker(\phi) = \{a \in R \mid \phi(a) = 0\}$. Then $\ker(\phi)$ is an ideal in R. Moreover, ϕ is injective if and only if $\ker(\phi) = \{0\}$.

Proof. As ϕ is a homomorphism we have $\phi(0) = 0$, so $0 \in \ker(\phi)$. Now suppose that $a, b \in \ker(\phi)$. We then have $\phi(a) = \phi(b) = 0$, so $\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$, so $a + b \in \ker(\phi)$. Suppose instead that $a \in R$ and $b \in \ker(\phi)$. We then have $\phi(b) = 0$ and so $\phi(ab) = \phi(a)\phi(b) = \phi(a).0 = 0$, so $ab \in \ker(\phi)$. This shows that $\ker(\phi)$ is an ideal as claimed.

Now suppose that ϕ is injective. If $a \in \ker(\phi)$ then we have $\phi(a) = 0 = \phi(0)$, so by injectivity we have $a = 0$; thus $\ker(\phi) = \{0\}$.

Conversely, suppose we have $\ker(\phi) = \{0\}$. If $a, b \in R$ satisfy $\phi(a) = \phi(b)$, then $\phi(a-b) = \phi(a) - \phi(b) = 0$, so $a - b \in \ker(\phi) = \{0\}$, so $a - b = 0$, so $a = b$. This shows that ϕ is injective as claimed. □

Proposition 3.7. [prop-ideal-ops]
Let R be a commutative ring, and let I and J be ideals in R. Put

$$I + J = \{a \in R \mid a = u + v \text{ for some } u \in I \text{ and } v \in J\}.$$

Then $I + J$ and $I \cap J$ are both ideals in R.

Proof. We first consider $I \cap J$. As I and J are ideals we have $0 \in I$ and $0 \in J$, so $0 \in I \cap J$, so Axiom (a) is satisfied. Now suppose that $a, b \in I \cap J$. As $a, b \in I$ and I is an ideal we have $a + b \in I$. As $a, b \in J$ and J is an ideal we have $a + b \in J$. Thus $a + b \in I \cap J$, so Axiom (b) is satisfied. Now suppose instead that $a \in R$ and $b \in I \cap J$. As $a \in R$ and $b \in I$ and I is an ideal we see that $ab \in I$. As $a \in R$ and $b \in J$ and J is an ideal we also have $ab \in J$. It follows that $ab \in I \cap J$, so Axiom (c) is satisfied. Thus $I \cap J$ is an ideal as claimed.

Now consider $I + J$. We can write 0 as $0 + 0$ with $0 \in I$ and $0 \in J$, so $0 \in I + J$, so Axiom (a) is satisfied. Now suppose that $a, b \in I + J$. As $a \in I + J$ we can write $a = u + v$ for some $u \in I$ and $v \in J$. Similarly we can write $b = x + y$ for some $x \in I$ and $y \in J$. We now have $a + b = u + v + x + y = (u + x) + (v + y)$. Here $u + x \in I$ and $v + y \in J$, so we see that $a + b \in I + J$, so Axiom (b) is satisfied. Finally, suppose instead that $a \in R$ and $b \in I + J$. We can write $b = x + y$ as before, with $x \in I$ and $y \in J$. As I is an ideal we have $ax \in I$, and as J is an ideal we have $ay \in J$. We can write ab as $ax + ay$ with $ax \in I$ and $ay \in J$, so $ab \in I + J$. Thus Axiom (c) is satisfied and $I + J$ is an ideal. □

Definition 3.8. [defn-R-mod-I]
Let R be a commutative ring, and let I be an ideal in R. For any $a \in R$ we put $a + I = \{a + b \mid b \in I\} \subseteq R$. A *coset* of I in R is a set of the form $a + I$ for some $a \in R$. We write R/I for the set of all cosets. We define a map $\pi \colon R \to R/I$ by $\pi(a) = a + I$.

Proposition 3.9. [prop-R-mod-I]

(a) *If $a - b \in I$ then the cosets $\pi(a) = a + I$ and $\pi(b) = b + I$ are the same; but if $a - b \notin I$ then they are disjoint.*
(b) *The set R/I has a unique ring structure such that π is a homomorphism.*

Proof. (a) First suppose that the element $a - b$ lies in I. Then any element of $a + I$ can be written as $a + x$ for some $x \in I$, but $a + x = b + ((a - b) + x)$ with $(a - b) + x \in I$, so $a + x \in b + I$. This shows that $a + I \subseteq b + I$, and a symmetrical argument shows that $b + I \subseteq a + I$, so $a + I = b + I$. Next suppose that $a + I$ and $b + I$ are not disjoint, so we can choose an element $u \in (a + I) \cap (b + I)$. As $u \in a + I$ we have $u = a + x$ for some $x \in I$. As $u \in b + I$ we have $u = b + y$ for some $y \in I$. We now see that $a + x = b + y$, which can be rearranged as $a - b = y - x$. Here x and y lie in I so $y - x \in I$, so $a - b \in I$. As we argued above, this means that in fact $a + I = b + I$.

(b) Suppose that $A, B \in R/I$, so A and B are subsets of R. We define

$$\begin{aligned} 0_{R/I} &= \pi(0) = I \\ 1_{R/I} &= \pi(1) = 1 + I \\ A + B &= \{x + y \mid x \in A \text{ and } y \in B\} \\ AB &= \{xy + t \mid x \in A \text{ and } y \in B \text{ and } t \in I\}. \end{aligned}$$

We now claim $A + B$ is always a coset. Indeed, the sets A and B are cosets by assumption, so we can choose a and b such that $A = a + I = \pi(a)$ and $B = b + I = \pi(b)$. We claim more precisely that $A + B = \pi(a + b)$. Indeed, every element $x \in A$ can be written as $x = a + u$ for some $u \in I$, and every element $y \in B$ can be written as $y + v$ for some $v \in I$. It follows that $x + y = (a + b) + (u + v)$ with $u + v \in I$, so $A + B \subseteq a + b + I = \pi(a + b)$. Conversely, if $z \in \pi(a + b)$ then $z = a + b + w$ for some $w \in I$, and so $z = (a + w) + (b + 0) \in A + B$; so $\pi(a + b) = A + B$ as required. Using the special case $b = 0$ we see in particular that $A + 0_{R/I} = A$.

Similarly, we claim that AB is a coset, namely $AB = \pi(ab)$. Indeed, any element of AB can be written as $xy + t$ for some $x \in A$ and $y \in B$ and $t \in I$. Equivalently, it can be written as $(a + u)(b + v) + t$ with $u, v, t \in I$, and thus as $ab + (ub + av + uv + t)$ with $ub + av + uv + t \in I$. This shows that $AB \subseteq \pi(ab)$. Conversely, any element $z \in \pi(ab)$ can be written as $ab + t$ for some $t \in I$, and $a \in A$ and $b \in B$ so $ab + t \in AB$. This shows that $\pi(ab) = AB$ as claimed. Using the special case $b = 1$ we see in particular that $A.1_{R/I} = A$.

We next claim that these operations make R/I into a ring. Consider for example the distributive law: we must show that if $A, B, C \in R/I$ then $A(B + C) = AB + AC$. As A, B and C are cosets, there must exist elements $a, b, c \in R$ such that $A = \pi(a)$ and $B = \pi(b)$ and $C = \pi(c)$. From what we proved above, we then have $B + C = \pi(b + c)$ and then

$$\begin{aligned} A(B + C) &= \pi(a)\pi(b + c) = \pi(a(b + c)) = \pi(ab + ac) \\ &= \pi(ab) + \pi(ac) = \pi(a)\pi(b) + \pi(a)\pi(c) = AB + AC. \end{aligned}$$

All the other axioms are obvious or can be proved in the same way.

We have shown that $\pi(0) = 0$ and $\pi(1) = 1$ and $\pi(a + b) = \pi(a) + \pi(b)$ and $\pi(ab) = \pi(a)\pi(b)$, so $\pi\colon R \to R/I$ is a homomorphism of rings. We leave it to the reader to check that our ring structure is the unique one with this property.

□

Proposition 3.10. [prop-induced-hom]
Let $\phi\colon R \to S$ be a homomorphism of rings, and let I be an ideal in R such that $\phi(a) = 0$ for all $a \in I$ (so $I \subseteq \ker(\phi)$). Then there is a unique homomorphism $\overline{\phi}\colon R/I \to S$ with $\overline{\phi} \circ \pi = \phi\colon R \to S$. Moreover, if ϕ is surjective and $\ker(\phi) = I$ *then $\overline{\phi}$ is an isomorphism.*

The rings and homomorphisms under consideration can be displayed in a diagram as follows:

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, "\overline{\phi}"'] & \end{tikzcd}$$

The equation $\overline{\phi} \circ \pi = \phi$ says that the two routes around the diagram from R to S are actually the same. The standard terminology for this is to say that the diagram *commutes*.

Proof. Suppose that $A \in R/I$, so $A \subseteq R$. If $a, b \in A$ then Proposition 3.9 tells us that $a - b \in I$, so $\phi(a) - \phi(b) = \phi(a - b) = 0$, so $\phi(a) = \phi(b)$. There is thus a well-defined map $\overline{\phi}\colon R/I \to S$ given by $\overline{\phi}(A) = \phi(a)$ for any $a \in A$. For a general element $x \in R$ we have $x \in \pi(x) \in R/I$, so $\overline{\phi}(\pi(x)) = \phi(x)$, which shows that $\overline{\phi} \circ \pi = \phi$. We now claim that $\overline{\phi}$ is a homomorphism. Indeed, the additive and multiplicative identity elements in R/I are $\pi(0)$ and $\pi(1)$, and using $\overline{\phi} \circ \pi = \phi$ we see that these are sent by $\overline{\phi}$ to 0 and 1 in S. Next, consider elements $A, B \in R/I$. We can then choose $a, b \in R$ with $A = \pi(a)$ and $B = \pi(b)$. It then follows that $A + B = \pi(a + b)$, and so

$$\overline{\phi}(A + B) = \overline{\phi}(\pi(a + b)) = \phi(a + b) = \phi(a) + \phi(b) = \overline{\phi}(\pi(a)) + \overline{\phi}(\pi(b)) = \overline{\phi}(A) + \overline{\phi}(B).$$

A similar argument shows that $\overline{\phi}(AB) = \overline{\phi}(A)\overline{\phi}(B)$, so $\overline{\phi}$ is a homomorphism as claimed.

Now suppose that ϕ is surjective and $\ker(\phi) = I$. For each $c \in S$, we put $\psi(c) = \{a \in R \mid \phi(a) = c\} \subseteq R$. We claim that $\psi(c)$ is a coset of I. Indeed, as ϕ is surjective we see that $\psi(c)$ is nonempty, so we can choose $a \in \psi(c)$, so $\phi(a) = c$. If $u \in I$ then $\phi(u) = 0$ so $\phi(a + u) = \phi(a) + \phi(u) = c + 0 = c$, so $a + u \in \psi(c)$. It follows that $a + I \subseteq \psi(c)$. Conversely, if $b \in \psi(c)$ then $\phi(b) = c = \phi(a)$, so $\phi(b - a) = \phi(b) - \phi(a) = c - c = 0$, so $b - a \in \ker(\phi) = I$, so $b \in a + I$. This shows that $\psi(c) \in R/I$, so we have defined a function $\psi\colon S \to R/I$. One can see directly from the definitions that $\psi(\overline{\phi}(A)) = A$ and $\overline{\phi}(\psi(c)) = c$, so ψ is inverse to $\overline{\phi}$. This means that $\overline{\phi}$ is a bijective homomorphism and thus an isomorphism. □

Exercises

Exercise 3.1. [ex-F-four-ideal]
Find an ideal $I \leq \mathbb{Z}[x]$ such that $\mathbb{Z}[x]/I$ is isomorphic to the field $\mathbb{F}_4$ in Example 1.11.

Exercise 3.2. [ex-ideals-twelve]
Find all the principal ideals in the ring $\mathbb{Z}/12\mathbb{Z}$.

4. Polynomials over fields

Definition 4.1. [defn-poly-degree]
Consider a polynomial $f(t) = \sum_{i=0}^{d} a_i t^i$. The *degree* of $f(t)$ is the largest d for which a_d is nonzero. (This is only meaningful if $f(t)$ is nonzero; the degree of the zero polynomial is undefined.) If this coefficient a_d is equal to one, we say that $f(t)$ is *monic*.

Remark 4.2. [rem-degree]
We now have three different (but related) meanings for the word "degree". The degree $[L : K]$ of a field extension was introduced in Definition 2.18, and the degree of a homomorphism $\phi\colon K \to L$ in Definition 2.19. These are related by the fact that $\deg(\phi) = [L : \phi(K)]$, and $[L : K]$ is the degree of the inclusion homomorphism $K \to L$. The connection between these and Definition 4.1 will emerge in Section 5.

Example 4.3. [eg-poly-degree]
The polynomial $f(t) = 1 + 2t + 3t^3 \in \mathbb{Q}[t]$ has degree 3 and is not monic. The polynomial $i + t^6 \in \mathbb{C}[t]$ is monic and has degree 6.

Lemma 4.4. [lem-deg-prod]
If $f(t)$ and $g(t)$ are nonzero polynomials over a field K then $f(t)g(t) \neq 0$ and $\deg(f(t)g(t)) = \deg(f(t)) + \deg(g(t))$. Moreover, if $f(t)$ and $g(t)$ are both monic then so is $f(t)g(t)$.

Proof. Put $d = \deg(f(t))$ and $e = \deg(g(t))$, so $f(t) = at^d +$ lower terms and $g(t) = bt^e +$ lower terms for some $a, b \in K$ with $a \neq 0$ and $b \neq 0$. We then have $f(t)g(t) = abt^{d+e} +$ lower terms, and $ab \neq 0$ by Lemma 1.5, so $f(t)g(t) \neq 0$ and $\deg(f(t)g(t)) = d + e$. The claim about the monic case is also clear now. □

Proposition 4.5. [prop-poly-division]
Let $f(t)$ and $g(t)$ be polynomials over a field K, with $f(t) \neq 0$. Then there is a unique pair of polynomials $(q(t), r(t))$ such that

- *$g(t) = f(t)q(t) + r(t)$*
- *Either $r(t) = 0$ or $\deg(r(t)) < \deg(f(t))$.*

We can rephrase this result as saying that $q(t)$ and $r(t)$ are the quotient and remainder when $g(t)$ is divided by $f(t)$. One way to prove it would be to explain and analyse the whole process of long division of polynomials. The proof below is essentially equivalent to that, but arranged a little differently. We will only analyse the first step of long division explicitly, and the remaining steps will be handled implicitly by the inductive structure of the argument.

Proof of Proposition 4.5. First suppose we have pairs $(q_1(t), r_1(t))$ and $(q_2(t), r_2(t))$ that both have the stated properties. We then have

$$f(t)q_1(t) + r_1(t) = g(t) = f(t)q_2(t) + r_2(t),$$

which can be rearranged to give

$$f(t)(q_1(t) - q_2(t)) = r_2(t) - r_1(t).$$

Suppose that $q_1(t) - q_2(t) \neq 0$. It follows that the left hand side is nonzero, with degree at least as large as $\deg(f(t))$, but the right hand side is either zero or has degree less than $\deg(f(t))$, which is a contradiction. We must therefore have $q_1(t) - q_2(t) = 0$, and thus $r_1(t) - r_2(t) = -f(t)(q_1(t) - q_2(t)) = 0$, so $(q_1, r_1) = (q_2, r_2)$. Thus, the pair (q, r) is unique if it exists. In the case $g(t) = 0$ we have $q(t) = r(t) = 0$.

From now on we assume that $g(t) \neq 0$, and work by induction on the degree of $g(t)$. Put $m = \deg(f(t))$. If $\deg(g(t)) < m$ then we can take $q(t) = 0$ and $r(t) = g(t)$; this starts the induction. Now suppose that $\deg(g(t)) = n \geq m$. We then have $g(t) = at^n +$ lower terms and $f(t) = bt^m +$ lower terms for some nonzero constants $a, b \in K$. Put $q_0(t) = ab^{-1}t^{n-m}$ and $g_1(t) = g(t) - q_0(t)f(t)$. The coefficient of t^n in $g_1(t)$ is $a - ab^{-1}b = 0$, so $g_1(t)$ is zero or has degree less than n. By induction, we can write $g_1(t) = f(t)q_1(t) + r(t)$ for some $q_1(t)$ and $r_1(t)$, where $r(t)$ is zero or has degree less than m. Now put $q(t) = q_0(t) + q_1(t)$ and observe that $g(t) = f(t)q(t) + r(t)$ as required. □

Proposition 4.6. [prop-poly-subfield]
Let L be a field and let K be a subfield. Suppose we have polynomials $f(t) \in K[t] \setminus \{0\}$ and $g(t) \in L[t]$ such that $f(t)g(t) \in K[t]$. Then $g(t) \in K[t]$ also.

We will give two proofs of this. The first just considers the coefficients directly:

Proof. The claim is clear if $g(t) = 0$, so we may assume that $g(t) \neq 0$. Put $h(t) = f(t)g(t) \in K[t]$. We can write

$$\begin{aligned} f(t) &= \sum_{i\geq 0} a_i x^i \\ g(t) &= \sum_{j\geq 0} b_j x^j \\ h(t) &= \sum_{k\geq 0} c_k x^k, \end{aligned}$$

where $a_i \in K$ and $b_j \in L$ and $c_k \in K$. The relation $f(t)g(t) = h(t)$ reduces to $c_k = \sum_{i+j=k} a_i b_j$. Let m be the smallest integer such that $a_m \neq 0$. We then find that $c_0 = \cdots = c_{m-1} = 0$ and

$$\begin{aligned} c_m &= a_m b_0 \\ c_{m+1} &= a_{m+1} b_0 + a_m b_1 \\ c_{m+2} &= a_{m+2} b_0 + a_{m+1} b_1 + a_m b_2 \end{aligned}$$

and so on. This can be rearranged as

$$\begin{aligned} b_0 &= c_m / a_m \\ b_1 &= (c_{m+1} - a_{m+1} b_0)/a_m \\ b_2 &= (c_{m+2} - a_{m+2} b_0 - a_{m+1} b_1)/a_m \end{aligned}$$

and so on. As $a_m, c_m \in K$ the first line shows that $b_0 \in K$. This means that everything appearing on the right on the second line is in K, so $b_1 \in K$. This means that everything appearing on the right on the third line is in K, so $b_2 \in K$. By continuing in the same way, we see that $b_j \in K$ for all j, so $g(t) \in K[t]$ as claimed. □

Another approach is to compare the division algorithm in $K[t]$ with the division algorithm in $L[t]$ and argue that they must give the same answer. Details are as follows:

Alternative proof. Put $h(t) = f(t)g(t) \in K[t]$. By the proposition (applied to $K[t]$), there is a unique pair $(q(t), r(t))$ of polynomials in $K[t]$ with $h(t) = f(t)q(t) + r(t)$ and $r(t) = 0$ or $\deg(r(t)) < \deg(f(t))$. As we also have $h(t) = f(t)g(t)$ we see that $f(t)(g(t) - q(t)) = r(t)$. If $g(t) - q(t)$ were nonzero then we would have $\deg(r(t)) = \deg(g(t)-q(t)) + \deg(f(t)) \geq \deg(f(t))$, contrary to assumption. So we must have $g(t)-q(t) = 0$, so $g(t) = q(t)$. By construction $q(t) \in K[t]$, so $g(t) \in K[t]$ as claimed. □

Proposition 4.7. [prop-Kx-pid]
Let K be a field, and let I be an ideal in $K[x]$. Then I is principal. More precisely, we either have $I = \{0\}$ or there is a unique monic polynomial $f(x)$ such that $I = K[x].f(x)$.

Proof. If $I = \{0\}$ then there is nothing more that we need to say, so suppose that $I \neq \{0\}$. Then I contains some nonzero polynomials, each of which has a well-defined degree. Let $\tilde{f}(x)$ be a nonzero polynomial in I whose degree is as small as possible. Put $d = \deg(\tilde{f}(x))$, so $\tilde{f}(x) = ax^d + \text{lower terms}$ for some nonzero element $a \in K$. Put $f(x) = a^{-1}\tilde{f}(x)$, so $f(x)$ is a monic polynomial of degree d. The constant polynomial a^{-1} is an element of $K[x]$, and $\tilde{f}(x) \in I$, so Axiom (c) tells us that $f(x) \in I$. It also follows using Axiom (c) that every multiple of $f(x)$ lies in I, so $K[x].f(x) \subseteq I$. Conversely, let $g(x)$ be an arbitrary element of I. By Proposition 4.5 we have $g(x) = f(x)q(x) + r(x)$ for some $q(x), r(x) \in K[x]$ with $r(x) = 0$ or $\deg(r(x)) < d$. Now $r(x) = g(x) + (-q(x)).f(x)$. Using Axiom (c) we see that $(-q(x)).f(x) \in I$, and also $g(x) \in I$ by assumption, so $r(x) \in I$ by Axiom (b). Now $f(x)$ was chosen to have minimal degree among the nonzero elements of I, so we cannot have $\deg(r(x)) < d$, so we must have $r(x) = 0$. The equation $g(x) = f(x)q(x) + r(x)$ therefore reduces to $g(x) = f(x)q(x)$, so $g(x) \in K[x].f(x)$. This shows that $I \subseteq K[x].f(x)$ and we have already proved the reverse inclusion, so $I = K[x].f(x)$ as claimed.

All that is left is to prove that $f(x)$ is the *unique* monic polynomial that generates I. Suppose that we also have $I = K[x].g(x)$ for some monic polynomial $g(x)$, with $\deg(g(x)) = e$ say. Then certainly $g(x) \in I$, so as above we have $g(x) = f(x)q(x)$ for some polynomial $q(x)$. By Lemma 4.4 we have $e - d = \deg(q(x)) \geq 0$, so $e \geq d$. Similarly, we have $f(x) \in I = K[x].g(x)$, so we must have $f(x) = g(x)p(x)$ for some polynomial $p(x)$. By Lemma 4.4 again we have $d - e = \deg(p(x)) \geq 0$, so $d \geq e$. It now follows that $d = e$ and $\deg(p(x)) = \deg(q(x)) = 0$, so p and q are constants. As $f(x)$ is monic and $p.f(x) = g(x)$ is also monic, we must have $p = 1$, so $f(x) = g(x)$ as required. □

Definition 4.8. [`defn-gcd`]
Let K be a field, and let $f(x)$ and $g(x)$ be nonzero polynomials in $K[x]$.

(a) The *least common multiple* of $f(x)$ and $g(x)$ is the monic generator of the ideal $K[x].f(x) \cap K[x].g(x)$. We write $\mathrm{lcm}(f(x), g(x))$ for this polynomial.

(b) The *greatest common divisor* of $f(x)$ and $g(x)$ is the monic generator of the ideal $K[x].f(x) + K[x].g(x)$. We write $\gcd(f(x), g(x))$ for this polynomial.

(Proposition 3.7 shows that the sets considered really are ideals.)

Proposition 4.9. [`prop-gcd`]
Let $f(x)$ and $g(x)$ be as above.

(a) *The polynomial $\mathrm{lcm}(f(x), g(x))$ is divisible by both $f(x)$ and $g(x)$. Moreover, is $h(x)$ is another polynomial that is divisible by both $f(x)$ and $g(x)$, then $h(x)$ is also divisible by $\mathrm{lcm}(f(x), g(x))$.*

(b) *Both $f(x)$ and $g(x)$ are divisible by $\gcd(f(x), g(x))$. Moreover, if $k(x)$ is another polynomial such that both $f(x)$ and $g(x)$ are divisible by $k(x)$, then $\gcd(f(x), g(x))$ is divisible by $k(x)$.*

(c) *If we let $\overline{f}(x)$ and $\overline{g}(x)$ be the polynomials such that $f(x) = \overline{f}(x)\gcd(f(x), g(x))$ and $g(x) = \overline{g}(x)\gcd(f(x), g(x))$, then*

$$\mathrm{lcm}(f(x), g(x)) = \overline{f}(x)\overline{g}(x)\gcd(f(x), g(x)) = \overline{f}(x)g(x) = f(x)\overline{g}(x).$$

Proof. For brevity we will write $p = \mathrm{lcm}(f, g)$ and $q = \gcd(f, g)$.

By the definition of p we have $K[x]f \cap K[x]g = K[x]p$. In particular, we have $p \in K[x]f \cap K[x]g$, so we can write $p = sf = tg$ for some $s, t \in K[x]$. Moreover, if h is also divisible by both f and g then $h \in K[x]f \cap K[x]g = K[x]p$ so h is divisible by p. This proves (a).

Next, we also have $q \in K[x]q = K[x]f + K[x]g$, so we can write $q = mf + ng$ for some $m, n \in K[x]$. Moreover, as $f = f + 0 \in K[x]f + K[x]g = K[x]q$, we have $f = \overline{f}q$ for some polynomial $\overline{f} \in K[x]$. Similarly, we have $g = \overline{g}q$ for some $\overline{g} \in K[x]$.

Now suppose we have another polynomial k such that both f and g are divisible by k, say $f = uk$ and $g = vk$. We then have $q = mf + ng = muk + nvk = (mu + nv)k$, so q is divisible by k. This proves (b).

Note also that we have $q = mf + ng = m\overline{f}q + n\overline{g}q$, so $(m\overline{f} + n\overline{g} - 1)q = 0$. As $q \neq 0$ we can deduce (using Lemma 4.4) that $m\overline{f} + n\overline{g} - 1 = 0$, so $m\overline{f} + n\overline{g} = 1$. We can also rewrite the equations $p = sf = tg$ as $p = s\overline{f}q = t\overline{g}q$.

Now consider the polynomial $r = \overline{f}\overline{g}q = \overline{f}g = f\overline{g}$. This is visibly a common multiple of f and g, so it must be a multiple of p. Now multiply the equation $1 = m\overline{f} + n\overline{g}$ by p and use $p = s\overline{f}q = t\overline{g}q$ to get

$$p = m\overline{f}p + n\overline{g}p = m\overline{f}t\overline{g}q + n\overline{g}s\overline{f}q = (mt + ns)\overline{f}\overline{g}q = (mt + ns)r.$$

In particular, we see that p is a multiple of r. As p and r are monic polynomials and are multiples of each other, they must be the same. This proves (c). □

Remark 4.10. The gcd of two polynomials $f_0(x)$ and $f_1(x)$ can be calculated by the following procedure, called the *Euclidean algorithm*. We may assume that $\deg(f_1(x)) \leq \deg(f_0(x))$ (otherwise just exchange the two polynomials) and that both polynomials are monic (otherwise just multiply by suitable constants). Suppose that we have defined $f_0(x), \dots, f_m(x)$, and $f_m(x) \neq 0$. We then write $f_{m-1}(x) = f_m(x)q(x) + r(x)$, with $r(x) = 0$ or $\deg(r(x)) < \deg(f_m(x))$. If $r(x) \neq 0$ then we define $f_{m+1}(x)$ to be $r(x)$ divided by its top coefficient (so that $f_{m+1}(x)$ is monic). This ensures that the ideal generated by $f_{m+1}(x)$ and $f_m(x)$ is the same as the ideal generated by $f_m(x)$ and $f_{m-1}(x)$. We then continue the procedure in the same way. On the other hand, if $r(x) = 0$ then the required gcd is just $f_m(x)$.

Definition 4.11. [`defn-irreducible`]
Let K be a field. A nonconstant polynomial $p(x) \in K[x]$ is *reducible over K* if it can be written as $p(x) = f(x)g(x)$ with $\deg(f(x)) > 0$ and $\deg(g(x)) > 0$. If not, we say that $p(x)$ is *irreducible over K*. We

write $\mathcal{P}_K$ (or just $\mathcal{P}$, if K is understood from the context) for the set of all irreducible monic polynomials over K.

Remark 4.12. [rem-irreducible-monic]
Suppose that $p(x)$ is a monic polynomial of degree d, and that $p(x) = f(x)g(x)$. If the leading term of $f(x)$ is ax^k, then the leading term of $g(x)$ must be $a^{-1}x^{d-k}$. It follows that the polynomials $\overline{f}(x) = a^{-1}f(x)$ and $\overline{g}(x) = ag(x)$ are both monic, and they satisfy $p(x) = \overline{f}(x)\overline{g}(x)$. Conversely, if $p(x)$ has no factorisation $p(x) = \overline{f}(x)\overline{g}(x)$ with $\overline{f}(x)$ and $\overline{g}(x)$ monic and nonconstant, then $p(x)$ is irreducible.

Example 4.13. [eg-linear-irreducible]
Any polynomial $p(x) = ax + b$ of degree one is irreducible. Indeed, if $\deg(f(x)) \geq 1$ and $\deg(g(x)) \geq 1$ then $f(x)g(x)$ has degree at least two and so cannot be equal to $p(x)$.

Example 4.14. [eg-misc-irreducible]
The polynomial $p(x) = x^2 + 1$ is reducible over $\mathbb{C}$, because it can be factored as $p(x) = (x + i)(x - i)$. However, we claim that $p(x)$ is irreducible over $\mathbb{R}$. Indeed, by Remark 4.12, it is enough to show that there is no factorisation $p(x) = (x + a)(x + b)$ with $a, b \in \mathbb{R}$. If there were such a factorisation, we would have $p(-a) = (-a + a)(-a + b) = 0$, but also $p(-a) = (-a)^2 + 1 = a^2 + 1$, so we would have $a^2 + 1 = 0$, which is impossible for $a \in \mathbb{R}$. Thus $p(x)$ is irreducible after all.

We next discuss Eisenstein's criterion, which is a useful test for irreducibility of polynomials over $\mathbb{Q}$.

Definition 4.15. [defn-eisenstein]
Let p be a prime number. An *Eisenstein polynomial* for p is a polynomial $q(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + x^d$ such that

(a) All the coefficients $a_0, \ldots, a_{d-1}$ are integers, and are divisible by p.
(b) a_0 is not divisible by p^2.

Proposition 4.16. [prop-eisenstein]
If $q(x)$ is an Eisenstein polynomial for some prime p, then $q(x)$ is irreducible over $\mathbb{Q}$.

Before proving this, we will need some preliminary definitions and auxiliary results. Note that the proposition makes it easy to generate many examples of irreducible polynomials over $\mathbb{Q}$. For example $x^{11} + 10x^2 - 25x + 35$ is Eisenstein for $p = 5$ and so is irreducible over $\mathbb{Q}$.

Remark 4.17. [rem-eisenstein-shift]
For $c \in K$ and $f(x) \in K[x]$, it is easy to see that $f(x)$ is reducible if and only if $f(x + c)$ is irreducible.

The polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$ does not satisfy Eisenstein's criterion at any prime, but the polynomial $f(x + 1) = x^4 + 5x^3 + 10x^2 + 10x + 5$ satisfies the criterion at $p = 5$. It follows that $f(x + 1)$ is irreducible over $\mathbb{Q}$, so $f(x)$ is irreducible. This trick is often useful.

Definition 4.18. [defn-primitive]
Consider a polynomial $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$. We say that $f(x)$ is *primitive* if the greatest common divisor of $a_0, \ldots, a_d$ is equal to one, or equivalently, there is no prime that divides all these coefficients.

Remark 4.19. [rem-primitive]
We can reduce the elements a_i modulo p to get elements $\pi_p(a_i) \in \mathbb{F}_p$. We then define $\pi_p(f)(x) = \sum_i \pi_p(a_i)x^i \in \mathbb{F}_p[x]$. This will be zero if and only if all the original coefficients a_i are divisible by p. Thus, we see that f is primitive if and only if $\pi_p(f) \neq 0$ for all p.

Lemma 4.20. [lem-primitive-product]
Suppose that $f(x), g(x) \in \mathbb{Z}[x]$ are both primitive. Then so is $f(x)g(x)$.

Proof. Consider a prime p. By the above remark we have $\pi_p(f) \neq 0$ and $\pi_p(g) \neq 0$. We also know from Proposition 1.6 that $\mathbb{F}_p$ is a field, so $\pi_p(f)\pi_p(g) \neq 0$ by Lemma 4.4. Moreover, it is clear that $\pi_p(fg) = \pi_p(f)\pi_p(g)$, so $\pi_p(fg) \neq 0$. As this holds for all p we deduce that fg is primitive, as claimed. □

Proposition 4.21. [prop-gauss]
Suppose that $q(x)$ is a monic polynomial in $\mathbb{Z}[x]$, and that there is a factorisation $q(x) = f(x)g(x)$ with f and g monic polynomials in $\mathbb{Q}[x]$. Then in fact f and g lie in $\mathbb{Z}[x]$.

Proof. Let u be the least common multiple of the denominators of the coefficients of f, or equivalently the smallest positive integer such that the polynomial $\overline{f}(x) = uf(x)$ lies in $\mathbb{Z}[x]$. We claim that $\overline{f}$ is primitive. Indeed, if it were not primitive, there would be a prime p that divides all the coefficients of $\overline{f}$, and then $(u/p).f$ would also be in $\mathbb{Z}[x]$, contradicting the definition of u. So $\overline{f}$ must be primitive after all. Similarly, we can find an integer $v > 0$ such that the polynomial $\overline{g}(x) = vg(x)$ is integral and primitive. Now put $\overline{q}(x) = \overline{f}(x)\overline{g}(x)$, and note from Lemma 4.20 that $\overline{q}(x)$ is primitive. On the other hand, we have $\overline{q}(x) = uvf(x)g(x) = uvq(x)$, with $uv \in \mathbb{N}$ and $q(x) \in \mathbb{Z}[x]$. It follows that any prime dividing uv divides all the coefficients of $\overline{q}(x)$, which is impossible because $\overline{q}(x)$ is primitive. It follows that there cannot be any primes dividing uv, so we must have $u = v = 1$. Thus $f(x) = \overline{f}(x) \in \mathbb{Z}[x]$ and $g(x) = \overline{g}(x) \in \mathbb{Z}[x]$ as claimed. □

Lemma 4.22. [lem-monomial-factors]
Let K be a field, and let $f(x)$ and $g(x)$ be polynomials over K such that $f(x)g(x) = x^d$ for some $d \geq 0$. Then we have $f(x) = ax^k$ and $g(x) = a^{-1}x^{d-k}$ for some a and k with $a \in K^\times$ and $0 \leq k \leq d$. In particular, if $f(x)$ is monic then $f(x) = x^k$ and $g(x) = x^{d-k}$.

Proof. Let ax^k be the highest nonzero term in $f(x)$, and let $a'x^{k'}$ be the lowest one. Let bx^j be the highest nonzero term in $g(x)$, and let $b'x^{j'}$ be the lowest one. Then Lemma 4.4 tells us that the highest term in $f(x)g(x)$ is abx^{k+j}, and a similar argument shows that the lowest one is $a'b'x^{k'+j'}$. As $f(x)g(x)$ has only the single term x^d, we must have $ab = a'b' = 1$ and $j + k = j' + k'$. As $j \geq j'$ and $k \geq k'$ this implies that $j = j'$ and $k = k'$, and thus that $f(x) = ax^k$ and $g(x) = bx^j$. It is now clear that we must have $0 \leq k \leq d$ and $j = d - k$ and $b = a^{-1}$. □

Proof of Proposition 4.16. Let $q(x)$ be an Eisenstein polynomial for the prime p, of degree d say. Suppose that $q(x) = f(x)g(x)$, where $f(x)$ and $g(x)$ are monic polynomials in $\mathbb{Q}[x]$, with $\deg(f(x)) = k > 0$ and $\deg(g(x)) = d - k > 0$. We see from Proposition 4.21 that $f(x), g(x) \in \mathbb{Z}[x]$. We can therefore consider the mod p reductions $\pi_p(f), \pi_p(g) \in \mathbb{F}_p[x]$. These are monic polynomials of degrees k and $d - k$ respectively. They satisfy $\pi_p(f)\pi_p(g) = \pi_p(fg) = \pi_p(q)$, and from Definition 4.15 it is clear that $\pi_p(q) = x^d$. We can thus invoke Lemma 4.22 to see that $\pi_p(f) = x^k$ and $\pi_p(g) = x^{d-k}$. In particular, we see that the constant terms $f(0)$ and $g(0)$ are divisible by p. It follows that the constant term $q(0) = f(0)g(0)$ is divisible by p^2, which contradicts the definition of an Eisenstein polynomial. It follows that $q(x)$ must be irreducible as claimed. □

Proposition 4.23. [prop-irreducibles-prime]
Let K be a field, and let $q(x)$ be an irreducible monic polynomial over K. Let $f(x)$ and $g(x)$ be polynomials in $K[x]$ that are not divisible by $q(x)$.

(a) *There exist polynomials $a(x)$ and $b(x)$ with $a(x)f(x) + b(x)q(x) = 1$.*
(b) *The product $f(x)g(x)$ is again not divisible by $q(x)$.*

Proof. For part (a), put $u(x) = \gcd(f(x), q(x))$. We know from Proposition 4.9 that $u(x)$ can be written in the form $u(x) = a(x)f(x) + b(x)q(x)$, so it will be enough to show that $u = 1$. We also know from the same proposition that $u(x)$ divides both $q(x)$ and $f(x)$. As $q(x)$ is irreducible, its only monic divisors are 1 and $q(x)$ itself, so either $u(x) = q(x)$ or $u(x) = 1$. We also know that $u(x)$ divides $f(x)$ but $q(x)$ does not divide $f(x)$, so we must have $u(x) = 1$ as required.

By the same argument, there exist polynomials $c(x)$ and $d(x)$ such that $c(x)g(x) + d(x)q(x) = 1$. We can multiply the equation $af + bq = 1$ by $cg + dq = 1$ to get $acfg + (adf + bcg + bdq)q = 1$. Now suppose for a contradiction that fg is divisible by q, say $fg = eq$. We could then rewrite the previous equation as $(ace + adf + bcg + bdq)q = 1$. This means that the polynomial $v = ace + adf + bcg + bdq$ is nonzero and satisfies $\deg(v) + \deg(q) = 0$ so $\deg(v) = \deg(q) = 0$. This is impossible because q is irreducible and therefore (by definition) not constant. □

Corollary 4.24. [cor-prime-multi]
Suppose that $q(x)$ is monic and irreducible and that none of $f_1(x), \dots, f_k(x)$ is divisible by $q(x)$; then the product $f(x) = \prod_{i=1}^k f_i(x)$ is also not divisible by $q(x)$.

Proof. We can argue by induction on k. The case $k = 1$ is obvious, and the case $k = 2$ is just part (b) above. More generally, part (b) can be used to deduce the case $k = m$ from the case $k = m - 1$. □

Corollary 4.25. [cor-quotient-field]
If $q(x)$ is monic and irreducible then the quotient ring $L = K[x]/(K[x].q(x))$ is a field.

Proof. Put $I = K[x].q(x)$, and let $\pi\colon K[x] \to L$ be the quotient map, as usual. Suppose that F is a nonzero element of L. We can then find $f(x) \in K[x]$ such that $F = \pi(f)$. As F is not the zero element we see that $f \notin I$. Part (a) of Proposition 4.23 tells us that there exist polynomials a and b such that $af + bq = 1$. We can apply π to this to get $\pi(a)\pi(f) + \pi(b)\pi(q) = \pi(1)$, but $q \in I$ so $\pi(q) = 0$, so we get $\pi(a)F = \pi(1)$. Here $\pi(1)$ is the multiplicative identity element for the quotient ring L, so we see that $\pi(a)$ is an inverse for F. This shows that all nonzero elements of L are invertible. Moreover, as $q(x)$ is irreducible it is nonconstant and so does not divide $1_{K[x]}$, so $1 \neq 0$ in L. This means that L is a field as claimed. □

Proposition 4.26. [prop-ufd]
Let K be a field, let $\mathcal{M}$ be the set of monic polynomials in $K[x]$, and let $\mathcal{P}$ be the subset of irreducible polynomials (as before). Then every element of $\mathcal{M}$ can be written in a unique way as a product of powers of elements of $\mathcal{P}$. More precisely, let $\mathcal{N}$ be the set of functions $v\colon \mathcal{P} \to \mathbb{N}$ such that $\{q \in \mathcal{P} \mid v(q) > 0\}$ is finite. Then there is a bijection $\mu\colon \mathcal{N} \to \mathcal{M}$ given by $\mu(v) = \prod_{q\in\mathcal{P}} q^{v(q)}$, with inverse $\lambda\colon \mathcal{M} \to \mathcal{N}$ given

$$\lambda(f)(q) = \max\{n \in \mathbb{N} \mid f \textit{ is divisible by } q^n\}.$$

Proof. First consider a polynomial $f \in \mathcal{M}$. We will prove by induction on $\deg(f)$ that $f = \mu(v)$ for some v. If $\deg(f) = 0$ then we must have $f = 1$ (because f is monic) and so $f = \mu(0)$. This starts the induction. Now suppose that $\deg(f) = d > 0$, and that the statement is true for all monic polynomials of degree less than d. If f is reducible then we can write $f = gh$ with $\deg(g) < d$ and $\deg(h) < d$. By the induction hypothesis there are elements $t, u \in \mathcal{N}$ with $\mu(t) = g$ and $\mu(u) = h$, and it follows that $\mu(t + u) = gh = f$ as required. On the other hand, if f is irreducible, we have $f \in \mathcal{P}$. We can therefore define $v \in \mathcal{N}$ by $v(f) = 1$ and $v(q) = 0$ for all $q \neq f$, and we find that $\mu(v) = f$. This completes the induction step, so we see that μ is surjective.

Now suppose that $q \in \mathcal{P}$ and $v \in \mathcal{N}$ and that $v(q) = 0$. We claim that $\mu(v)$ is not divisible by q. Indeed, by the definition of $\mathcal{N}$ there is a finite set $r_1, \dots, r_k$ of distinct irreducibles such that $v(r_i) > 0$ for all i, and $v(s) = 0$ for all other irreducibles, so $\mu(v) = \prod_{i=1}^{k} r_i^{v(r_i)}$. As $v(r_i) > 0$ and $v(q) = 0$ we have $r_i \neq q$. As r_i and q are both monic irreducibles, it follows that r_i cannot be divisible by q. It follows using Corollary 4.24 that $\mu(v)$ is not divisible by q either.

We now claim that for any v we have $\lambda(\mu(v)) = v$. Equivalently, we claim that $\mu(v)$ is divisible by $q^{v(q)}$, but not by any higher power of q. To see this, define $w \in \mathcal{N}$ by $w(q) = 0$, and $w(r) = v(r)$ for all $r \neq q$. From this it is clear that $\mu(v) = q^{v(q)}\mu(w)$, so $\mu(v)$ is certainly divisible by $q^{v(q)}$. Suppose that $\mu(v)$ is in fact divisible by $q^{v(q)+1}$, say $\mu(v) = q^{v(q)+1}f$. We then have $q^{v(q)}(\mu(w) - qf) = 0$, so $\mu(w) = qf$. This is impossible by the previous paragraph, because $w(q) = 0$. It follows that $\lambda(\mu(v)) = v$ as claimed.

Finally we claim that $\mu(\lambda(f)) = f$ for all $f \in \mathcal{M}$. Indeed, we have already seen that $f = \mu(v)$ for some v. It follows that $\lambda(f) = \lambda(\mu(v))$, which is equal to v by the last paragraph. We can substitute $\lambda(f) = v$ back into the equation $f = \mu(v)$ to get $f = \mu(\lambda(f))$ as claimed. This shows that μ is a bijection with inverse λ, as claimed. □

Definition 4.27. [defn-root]
Let K be a field, let $f(x)$ be a polynomial in $K[x]$, and let α be an element of K. We say that α is a *root* of f if $f(\alpha) = 0$.

Proposition 4.28. [prop-root]
The element α is a root of $f(x)$ if and only if $f(x)$ is divisible in $K[x]$ by $x - \alpha$.

Proof. If $f(x)$ is divisible by $x - \alpha$ then $f(x) = g(x)(x - \alpha)$ for some polynomial $g(x) \in K[x]$. It follows that $f(\alpha) = g(\alpha)(\alpha - \alpha) = 0$ as required.

Conversely, suppose that $f(\alpha) = 0$. Proposition 4.5 tells us that we can write $f(x) = q(x)(x - \alpha) + r(x)$, where either $r(x) = 0$ or $\deg(r(x)) < \deg(x - \alpha) = 1$. This means that $r(x)$ is a constant, say $r(x) = c \in K$, so $f(x) = q(x)(x - \alpha) + c$. Now put $x = \alpha$ to get $0 = f(\alpha) = q(\alpha)(\alpha - \alpha) + c = 0 + c$, so $c = 0$. We can substitute this back in to see that $f(x) = q(x)(x - \alpha)$, which is divisible by $x - \alpha$ as claimed. □

Proposition 4.29. [prop-several-roots]
Suppose that $\alpha_1,\dots,\alpha_k$ are distinct roots of a polynomial $f(x)$. Then there exists a polynomial $g(x)$ such that $f(x)=g(x)\prod_{i=1}^k(x-\alpha_i)$. In particular, if $f(x)$ is monic and $\deg(f(x))=k$ then $f(x)=\prod_{i=1}^k(x-\alpha_i)$.

Proof. We argue by induction on k, noting that Proposition 4.28 covers the case $k=1$. For general k, we may assume inductively that $f(x)=h(x)\prod_{i=1}^{k-1}(x-\alpha_i)$ for some polynomial $h(x)$. We then have

$$h(\alpha_k)\prod_{i=1}^{k-1}(\alpha_k-\alpha_i)=f(\alpha_k)=0.$$

By hypothesis the roots α_j are distinct, so $\alpha_k-\alpha_i\neq 0$ for $1\leq i\leq k-1$, so $\prod_{i=1}^{k-1}(\alpha_k-\alpha_i)\neq 0$. It follows that we must instead have $h(\alpha_k)=0$. We can now apply Proposition 4.28 to $h(x)$ to get a factorisation $h(x)=g(x)(x-\alpha_k)$. We can then combine this with $f(x)=h(x)\prod_{i=1}^{k-1}(x-\alpha_i)$ to get $f(x)=g(x)\prod_{i=1}^k(x-\alpha_i)$ as required.

Now suppose that $\deg(f(x))=k$. It follows that we must have $\deg(g(x))=0$, so $g(x)$ is constant. If $f(x)$ is also monic then by considering the coefficient of x^k we see that $g(x)=1$ and so $f(x)=\prod_{i=1}^k(x-\alpha_i)$. □

Corollary 4.30. [cor-num-roots]
If $f(x)$ is a nonzero polynomial of degree d, then $f(x)$ has at most d roots. □

Theorem 4.31 (The Fundamental Theorem of Algebra)**.** [thm-fta]
If $f(x)\in\mathbb{C}[x]$ and $\deg(f(x))>0$ then $f(x)$ has a root in $\mathbb{C}$.

Remark 4.32. [rem-alg-cl]
A field K is said to be *algebraically closed* if it has the property mentioned above, that every nonconstant polynomial in $K[x]$ has a root in K. Thus, the theorem says that $\mathbb{C}$ is algebraically closed.

Sketch proof. Despite the traditional name, this is really a theorem in analysis, so we will only outline the argument. After dividing through by a constant, we can assume that $f(x)$ is monic, of degree $d\geq 1$ say. We can write $f(x)=\sum_{k=0}^d a_kx^k$, with $a_d=1$.

Suppose for a contradiction that $f(x)$ has no roots. It follows that the formula $g(x)=1/f(x)$ defines a continuous function $g\colon\mathbb{C}\to\mathbb{C}$. (In fact, this function is even analytic, and we could shortcut some of the following steps by using some further theory of analytic functions.) Next, for $r\geq 0$ we define

$$h(r)=\int_{t=0}^{2\pi}g(re^{it})\,dt.$$

Using some standard lemmas from analysis, we see that h is continuously differentiable, with derivative given by differentiating under the integral sign:

$$h'(r)=\frac{\partial}{\partial r}\int_{t=0}^{2\pi}g(re^{it})\,dt=\int_{t=0}^{2\pi}\frac{\partial}{\partial r}g(re^{it})\,dt=\int_{t=0}^{2\pi}e^{it}g'(re^{it})\,dt.$$

On the other hand, we also have

$$\frac{\partial}{\partial t}g(re^{it})=ire^{it}g'(re^{it}),$$

so we can rewrite the above as

$$h'(r)=\tfrac{1}{ir}\int_{t=0}^{t=2\pi}\tfrac{\partial}{\partial t}g(re^{it})\,dt=\tfrac{1}{ir}\left[g(re^{it})\right]_{t=0}^{2\pi}=(g(1)-g(1))/(ir)=0.$$

It follows that $h(r)$ is constant, so $h(r)=h(0)$ for all r. It is clear from the formula that $h(0)=2\pi g(0)=2\pi/f(0)\neq 0$. Now suppose that $|x|$ is very large, and in particular, much larger than any of the coefficients $a_0,\dots,a_{d-1}$. Then the term x^d in $f(x)$ will be much larger than any of the other terms, so $|f(x)|$ will be approximately $|x|^d$, and $|g(x)|$ will be approximately $|x|^{-d}$. It follows that when r is very large we have

$$|h(r)|=\left|\int_{t=0}^{2\pi}g(re^{it})\,dt\right|\leq\int_{t=0}^{2\pi}|g(re^{it})|\,dt\simeq\int_{t=0}^{2\pi}r^{-d}\,dt=2\pi r^{-d}.$$

It follows that $h(r)\to 0$ as $r\to\infty$. This is inconsistent with the fact that h is constant, and $h(0)\neq 0$. It follows that $f(x)$ has a root after all. □

Corollary 4.33. [cor-fta]
Let $f(x)$ be a monic polynomial of degree d over $\mathbb{C}$. Then $f(t)=\prod_{k=1}^{d}(x-\alpha_k)$ for some list $\alpha_1,\dots,\alpha_d$ of elements of $\mathbb{C}$.

Proof. We argue by induction on d. The case $d=0$ is clear, if we recall the standard convention that the product of no terms is equal to one. The case $d=1$ is also clear, because any monic polynomial of degree one certainly has the form $f(x)=x-\alpha_1$ for some $\alpha_1\in\mathbb{C}$. Consider a general monic polynomial $f(x)$ of degree $d>1$. The thearem tells us that there exists $\alpha_d\in\mathbb{C}$ with $f(\alpha_d)=0$. Using Proposition 4.28 we see that $f(x)=g(x)(x-\alpha_d)$ for some monic polynomial $g(x)\in\mathbb{C}[x]$ of degree $d-1$. By induction, we may assume that $g(x)=\prod_{k=1}^{d-1}(x-\alpha_k)$ for some list $\alpha_1,\dots,\alpha_{d-1}$ of elements of $\mathbb{C}$. It follows that $f(x)=\prod_{k=1}^{d}(x-\alpha_k)$, as claimed. □

It is useful to be able to extend Proposition 4.28 to determine when $f(x)$ is divisible by some higher power $(x-\alpha)^m$. For this, we need an algebraic theory of derivatives.

Definition 4.34. [defn-derivative]
Let K be a field, and let $f(x)=\sum_{i=0}^{d}a_ix^i$ be a polynomial in $f(x)$. The *algebraic derivative* of $f(x)$ is the polynomial $f'(x)$ defined by $f'(x)=\sum_{i=1}^{d}a_ix^{i-1}$. We also define $f^{(0)}(x)=f(x)$, $f^{(1)}(x)=f'(x)$, $f^{(2)}(x)=f''(x)$ and so on, so in general $f^{(n+1)}(x)$ is the algebraic derivative of $f^{(n)}(x)$.

Remark 4.35. [rem-derivative]
In the case $K=\mathbb{R}$, the derivative is usually defined by $f'(x)=\lim_{h\to0}(f(x+h)-f(x))/h$, and it is a theorem rather than a definition that $f'(x)=\sum_{i=1}^{d}a_ix^{i-1}$. For a general field K (especially when the characteristic is not zero) we may not be able to make sense of limits. However, we can still define algebraic derivatives by the above formula, and we will find that they still have most of the familiar properties of derivatives as used in calculus.

Lemma 4.36. [lem-derivative]
In the ring $K[x][y]$ we have

$$f(x+y)=f(x)+f'(x)y+\text{ terms divisible by }y^2.$$

Moreover, $f'(x)$ is the only polynomial with this property.

Proof. By the binomial expansion (or by induction on i) we have $(x+y)^i-x^i=ix^{i-1}y$ plus terms divisible by y^2. If $f(x)=\sum_i a_ix^i$, it follows that

$$\begin{aligned}f(x+y)-f(x)&=\sum_i a_i((x+y)^i-x^i)=\sum_i ia_ix^{i-1}y+\text{ terms divisible by }y^2\\&=f'(x)y+\text{ terms divisible by }y^2\end{aligned}$$

as claimed. If we also have $f(x+y)=f(x)+g(x)y$ plus terms divisible by y^2 then we find that $(f'(x)-g(x))y$ is divisible by y^2, which easily implies that $f'(x)-g(x)=0$ as required. □

Proposition 4.37. [prop-leibniz]
If $f(x)=g(x)h(x)$ then $f'(x)=g'(x)h(x)+g(x)h'(x)$.

We will give two different proofs.

First proof. Lemma 4.36 tells us that for some $r(x,y)$ and $s(x,y)$ in $K[x][y]$ we have

$$\begin{aligned}g(x+y)&=g(x)+g'(x)y+r(x,y)y^2\\h(x+y)&=h(x)+h'(x)y+s(x,y)y^2.\end{aligned}$$

We can multiply these and rearrange to get

$$\begin{aligned}f(x+y)=&(g(x)+g'(x)y+r(x,y)y^2)(h(x)+h'(x)y+s(x,y)y^2)\\=&g(x)h(x)+(g'(x)h(x)+g(x)h'(x))y+\\&(g'(x)h'(x)+g(x)s(x,y)+h(x)r(x,y)+g'(x)s(x,y)y+h'(x)r(x,y)y+r(x,y)s(x,y)y^2)y^2\\=&f(x)+(g'(x)h(x)+g(x)h'(x))y+\text{ terms divisible by }y^2.\end{aligned}$$

We must therefore have $f'(x) = g'(x)h(x) + g(x)h'(x)$ as claimed. □

Second proof. Suppose that $g(x) = \sum_i b_i x^i$ and $h(x) = \sum_j c_j x^j$. Then $f(x) = \sum_k a_k x^k$, where $a_k = \sum_{i=0}^k b_i c_{k-i}$. It follows that $h'(x) = \sum_k k a_k x^{k-1}$. On the other hand, we have

$$\begin{aligned} g'(x) &= \sum_i i b_i x^{i-1} \\ h'(x) &= \sum_j j c_j x^{j-1} \\ g'(x)h(x) &= \sum_i \sum_j i b_i c_j x^{i+j-1} \\ g(x)h'(x) &= \sum_i \sum_j j b_i c_j x^{i+j-1} \\ g'(x)h(x) + g(x)h'(x) &= \sum_i \sum_j (i+j) b_i c_j x^{i+j-1} = \sum_k k x^{k-1} \sum_{i+j=k} b_i c_j \\ &= \sum_k k a_k x^{k-1} = h'(x). \end{aligned}$$

□

Corollary 4.38. [`cor-deriv-pow`]
If $f(x) = g(x)^n$ then $f'(x) = ng(x)^{n-1}g'(x)$.

Proof. This is clear for $n = 0$ or $n = 1$. Suppose that the function $h(x) = g(x)^k$ satisfies $h'(x) = kg(x)^{k-1}g'(x)$, and we consider $f(x) = g(x)^{k+1} = g(x)h(x)$. Using the proposition we deduce that

$$\begin{aligned} f'(x) &= g'(x)h(x) + g(x)h'(x) = g'(x)g(x)^k + g(x).kg(x)^{k-1}g'(x) \\ &= g(x)^k g'(x) + kg(x)^k g'(x) = (k+1)g(x)^k g'(x), \end{aligned}$$

so the claim holds for $n = k+1$ as well. It follows by induction that it is true for all n. □

Lemma 4.39. [`lem-deriv-shift`]
If we put $g(x) = f(x+\alpha)$, then $g'(x) = f'(x+\alpha)$. More generally, we have $g^{(n)}(x) = f^{(n)}(x+\alpha)$ for all $n \geq 0$.

Proof. We have $f(x+y) = f(x) + f'(x)y + r(x,y)y^2$ for some $r(x,y) \in K[x][y]$. It follows that

$$g(x+y) = f(x+\alpha+y) = f(x+\alpha) + f'(x+\alpha)y + r(x+\alpha,y)y^2 = g(x) + f'(x+\alpha)y + \text{ terms divisible by } y^2,$$

so $g'(x) = f'(x+\alpha)$ as claimed. The more general statement then follows by induction. □

Proposition 4.40. [`prop-multiple-roots`]
Let K be a field of characteristic zero, let $f(x)$ be a polynomial in $K[x]$, and let α be an element of K. Then $f(x)$ is divisible by $(x-\alpha)^n$ if and only if $f(\alpha) = f'(\alpha) = \cdots = f^{(n-1)}(\alpha) = 0$.

Proof. We first consider the case $\alpha = 0$, where the claim is that $f(x)$ is divisible by x^n if and only if $f^{(i)}(0) = 0$ for all $i < n$. Suppose that $f(x) = \sum_i a_i x^i$. One can then check that

$$f^{(r)}(x) = \sum_{i \geq r} i(i-1)(i-2)\cdots(i-r+1)a_i x^{i-r},$$

and thus $f^{(r)}(0) = r!a_r$. As K has characteristic zero, we know that $r!$ is invertible in K and so $f^{(r)}(0) = 0$ if and only if $a_r = 0$. It is clear that $f(x)$ is divisible by x^n if and only if the coefficients $a_0, \ldots, a_{n-1}$ are all zero, and we now see that this happens if and only if $f^{(i)}(0) = 0$ for all $i < n$.

Now consider the general case where α need not be zero, and put $g(x) = f(x+\alpha)$. Then $f(x)$ is divisible by $(x-\alpha)^n$ if and only if $g(x)$ is divisible by x^n. By our special case, this holds if and only if $g^{(i)}(0) = 0$ for all $i < n$. Using Lemma 4.39 we see that $g^{(i)}(0) = f^{(i)}(\alpha)$, and the proposition now follows. □

Remark 4.41. [rem-multiple-roots]
The above proposition does not extend to fields of nonzero characteristic. Indeed, in $\mathbb{F}_p[x]$ the polynomial $f(x) = x^p$ has $f'(x) = px^{p-1} = 0$ and so $f^{(k)}(0) = 0$ for all $k > 0$, but $f(x)$ is not divisible by x^{p+1}.

Proposition 4.42. [prop-distinct-roots]
Let L be a field of characteristic zero, and let K be a subfield of L. Suppose that $f(x) \in K[x]$ is irreducible over K (but not necessarily over L). Then there is no $\alpha \in L$ such that $f(x)$ is divisible by $(x-\alpha)^2$ in $L[x]$.

Proof. Suppose that $\deg(f(x)) = d > 0$, so $\deg(f'(x)) = d - 1$. Let $u(x)$ be the greatest common divisor of $f(x)$ and $f'(x)$. This is a monic divisor of the irreducible polynomial $f(x)$, so we must have $u(x) = 1$ or $u(x) = f(x)$. However, $u(x)$ must also divide $f'(x)$ and $f(x)$ cannot divide $f'(x)$ because $\deg(f(x)) > \deg(f'(x))$, so we cannot have $u(x) = f(x)$. We must therefore have $u(x) = 1$ instead. We also know from Proposition 4.9 that there exist polynomials $a(x)$ and $b(x)$ in $K[x]$ with $a(x)f(x) + b(x)f'(x) = u(x) = 1$. Now consider an element $\alpha \in L$, and suppose for a contradiction that $f(x)$ is divisible by $(x-\alpha)^2$. By Proposition 4.40, this means that $f(\alpha) = f'(\alpha) = 0$. We can thus substitute $x = \alpha$ in the equation $a(x)f(x) + b(x)f'(x) = 1$ to get $0 = 1$, which is impossible. □

Exercises

Exercise 4.1. [which-irreducible]
Which of the following polynomials are irreducible over $\mathbb{Q}$?

$$\begin{aligned}
f_0(x) &= x^4 + 9x + 12 \\
f_1(x) &= x^3 - x^2 - x - 2 \\
f_2(x) &= x^2 - 3x - 18 \\
f_3(x) &= x^5 + 5x^4 + 55x^3 + 555x^2 + 5555x + 55555.
\end{aligned}$$

Exercise 4.2. [ex-euclid]
Use the Euclidean algorithm to find $\gcd(f(x), f'(x))$, where $f(x) = x^4 + 2x^3 + 3x^2 + 2x + 1$. Use this to factorise $f(x)$.

Exercise 4.3. [ex-eisenstein-shift]
Use the method of Remark 4.17 to show that the polynomial $f(x) = x^4 - 5x^3 + 9x^2 - 5x + 1$ is irreducible over $\mathbb{Q}$.

Exercise 4.4. [ex-modular-irreducible]
Show, by considering all potential factors, that the polynomial $x^5 + x^2 + 1$ is irreducible in $\mathbb{F}_2[x]$. Deduce that it is also irreducible in $\mathbb{Q}[x]$

Exercise 4.5. [ex-x-to-the-p]
Let p be a prime number, and put $R = \{f(x) \in \mathbb{F}_p[x] \mid f'(x) = 0\}$. What can you say about this set?

5. Adjoining roots

Definition 5.1. [defn-bullet]
Let $\phi\colon R \to S$ be a homomorphism of rings. We then define $\phi_\bullet\colon R[x] \to S[x]$ by

$$\phi_\bullet(\sum_i a_i x^i) = \sum_i \phi(a_i) x^i.$$

We leave it to the reader to check that $\phi_\bullet$ is again a ring homomorphism.

Proposition 5.2. [prop-quotient-basis]
Let K be a field, let $f(x)$ be a polynomial of degree $d > 0$ in $K[x]$ and consider the quotient ring $R = K[x]/(K[x].f(x))$. Then the list $\Pi = \pi(1), \pi(x), \dots, \pi(x^{d-1})$ is a basis for R over K, so $\dim_K(R) = d$.

Proof. Any element $G \in R$ can be written as $G = \pi(g)$ for some polynomial $g(x) \in K[x]$. By Proposition 4.5 we can write $g(x) = f(x)q(x) + r(x)$ where $q(x)$ and $r(x)$ are polynomials with $r(x) = 0$ or $\deg(r(x)) < d$. In all cases we can write $r(x) = \sum_{i=0}^{d-1} c_i x^i$ for some system of coefficients c_i. Now we can apply π to the relation $g(x) = f(x)q(x) + r(x)$ and recall that $\pi(q) = 0$ to get $G = \pi(g) = \pi(f).0 + \pi(r) = \pi(r) = \sum_i a_i \pi(x^i)$. It follows that Π spans R over K. Now suppose we have a linear relation $a_0\pi(1) + a_1\pi(x) + \cdots + a_{d-1}\pi(x^{d-1}) = 0$. If we put $h(x) = \sum_{i=0}^{d-1} a_i x^i$, this can be rewritten as $\pi(h(x)) = 0$, so $h(x) \in K[x].f(x)$. As $f(x)$ has degree d, we see that any nonzero multiple of $f(x)$ has degree at least d. However, $h(x)$ is a multiple of $f(x)$ and has degree less than d, so it must be zero, so $a_0 = \cdots = a_{d-1} = 0$. This shows that Π is linearly independent, so it is a basis as claimed. □

Proposition 5.3. [prop-adjoin-root]
Let K be a field, and let $f(x)$ be a polynomial of degree $d > 0$ in $K[x]$. Then there exists a homomorphism $\phi\colon K \to L$ such that $\phi_\bullet(f)$ has a root in L, and $\deg(\phi) \leq d$.

Proof. Using Proposition 4.26 (or a more direct argument) we see that $f(x)$ has at least one monic irreducible factor. Let $q(x)$ be such a factor. Put $L = K[t]/(K[t].q(t))$, which is a field by Corollary 4.25. Let π be the usual quotient map $K[t] \to L$. Let ϕ be the restriction of ϕ to $K \subset K[t]$, and put $\alpha = \pi(t) \in L$. We claim that α is a root of $\phi_\bullet(q)$. To see this, suppose that $q(t) = \sum_{i=0}^{n} a_i t^i$. We then have

$$\begin{aligned} \phi_\bullet(q(x)) &= \sum_{i=0}^{n} \pi(a_i) t^i \\ \phi_\bullet(q(\alpha)) &= \sum_{i=0}^{n} \pi(a_i)\pi(t)^i = \pi\left(\sum_{i=0}^{n} a_i t^i\right) \\ &= \pi(q(t)) = 0, \end{aligned}$$

as required. Note also that Proposition 5.2 gives $\deg(\phi) = \deg(q) \leq \deg(f) = d$. □

Remark 5.4. [rem-adjoin-root]
If we are willing to identify K with $\phi(K)$ as in Remark 1.30, we obtain the following statement: for any nonconstant polynomial $f(x) \in K[x]$, there is an extension field $L \supseteq K$ such that $[L : K] \leq \deg(f(x))$ and $f(x)$ has a root in L.

Definition 5.5. [defn-algebraic]
Consider a field L, a subfield K, and an element $\alpha \in L$. We write $K(\alpha)$ for the smallest subfield of L that contains K and α. We also define an ideal $I(\alpha, K) \subseteq K[x]$ by

$$I(\alpha, K) = \{f(x) \in K[x] \mid f(\alpha) = 0 \in L\}.$$

(a) If $I(\alpha, K) = \{0\}$ we say that α is *transcendental* over K.
(b) Suppose instead that $I(\alpha, K) \neq 0$. We then say that α is *algebraic* over K. We see from Proposition 4.7 that there is a unique monic polynomial $\min(\alpha, K) \in K[x]$ (called the *minimal polynomial* of α) that generates $I(\alpha, K)$. The *degree* of α over K is defined to be the degree of the polynomial $\min(\alpha, K)$.
(c) If $K(\alpha) = L$, we say that α is a *primitive element* for L over K.

Remark 5.6. [rem-algebraic]
It is sometimes convenient to consider a slightly more general situation. Suppose we have a homomorphism $\phi\colon K \to L$, and an element $\alpha \in L$. We put $K' = \phi(K)$, so K' is a subfield of L, and ϕ can be considered as an isomorphism $K \to K'$. We put

$$I(\alpha, \phi) = \{f(x) \in K[x] \mid (\phi_\bullet f)(\alpha) = 0\}.$$

If this is nonzero, then we write $\min(\alpha, \phi)$ for the unique monic generator of $I(\alpha, \phi)$. This clearly correspond to $I(\alpha, K')$ under the isomorphism $\phi_\bullet\colon K[x] \to K'[x]$. We also say that α is a *primitive element* for ϕ if $L = K'(\alpha)$.

Remark 5.7. [rem-Q-bar]
In some sense, almost all complex numbers are transcendental over $\mathbb{Q}$. The simplest way to see this is to use the theory of countability. Put

$$\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ is algebraic over } \mathbb{Q}\} = \bigcup_{0 \neq f(x) \in \mathbb{Q}[x]} \{ \text{ roots of } f(x)\}.$$

Fairly standard methods show that $\mathbb{Q}[x]$ is countable, and it follows that $\overline{\mathbb{Q}}$ is countable. However, $\mathbb{R}$ and $\mathbb{C}$ are both uncountable, and so are much bigger than $\overline{\mathbb{Q}}$. Despite this, it is hard work to show that any particular number is transcendantal. It is known that both π and e are transcendental, but we will not discuss the proofs here.

Proposition 5.8. [prop-simple-algebraic]
Suppose that α is algebraic over K. Then the minimal polynomial $\min(\alpha, K)$ *is irreducible, and there is a unique homomorphism $\overline{\chi}\colon K[x]/(K[x].\min(\alpha, K)) \to K(\alpha)$ that acts as the identity on K and sends x to α. Moreover, this homomorphism is an isomorphism, and so $[K(\alpha) : K] = \dim_K(K(\alpha)) = \deg(\min(\alpha, K))$. In particular, if α is a primitive element for L over K, then L itself is isomorphic to $K[x]/(K[x].\min(\alpha, K))$.*

Proof. First put $q(x) = \min(\alpha, K)(x)$ and let d be the degree of $q(x)$. Suppose that $q(x) = u(x)v(x)$, where $u(x)$ and $v(x)$ are both nonconstant and so both have degree less than d. This means that neither $u(x)$ nor $v(x)$ are divisible by $q(x)$, so they do not lie in $I(\alpha, K)$, so $u(\alpha)$ and $v(\alpha)$ are nonzero elements of the field L. It follows that $q(\alpha) = u(\alpha)v(\alpha) \neq 0$, which contradicts the definition of $q(x)$. It follows that $q(x)$ has no such factorisation, so it is irreducible as claimed. It then follows by Corollary 4.25 that the quotient ring $L' = K[x]/(K[x].q(x)) = K[x]/I(\alpha, K)$ is actually a field.

Now define $\chi\colon K[x] \to L$ by $\chi(\sum_i a_i x^i) = \sum_i a_i \alpha^i$, or equivalently $\chi(f(x)) = f(\alpha)$. This is clearly the unique homomorphism that acts as the identity on K and sends x to α. We have $\chi(f(x)) = 0$ iff $f(\alpha) = 0$ iff $f(x) \in I(\alpha, K)$, so $\ker(\chi) = I(\alpha, K) = K[x].q(x)$. We therefore have an induced homomorphism $\overline{\chi}\colon L' \to L$ as in Proposition 3.10, and a subfield $L'' = \overline{\chi}(L') \subseteq L$ as in Proposition 1.29. We claim that $L'' = K(\alpha)$. Indeed, it is clear that L'' contains K and α, so it contains $K(\alpha)$. Conversely, $K(\alpha)$ is closed under multiplication and contains K and α, so by induction it contains all elements of the form $a\,\alpha^k$. It is also closed under addition, so it contains all elements of the form $\sum_{i=0}^n a_i \alpha^i$. In other words, it contains the image of χ, which is the same as the image of $\overline{\chi}$, which is L''. We can now regard χ as a surjective homomorphism $K[x] \to K(\alpha)$ with kernel $I(\alpha, K)$, so the induced map $L' = K[x]/I(\alpha, K) \to K(\alpha)$ is an isomorphism as claimed (by Proposition 3.10). □

We can restate essentially the same fact as follows:

Corollary 5.9. [cor-simple-algebraic]
Suppose we have a homomorphism $\phi\colon K \to L$, and an element $\alpha \in L$ that is algebraic over the subfield $K' = \phi(K)$. Then there is an isomorphism

$$\overline{\chi}\colon K[x]/(K[x].\min(\alpha, \phi)) \to K'(\alpha) \subseteq L$$

given by

$$\overline{\chi}(f(x) + K[x].\min(\alpha, \phi)) = (\phi_\bullet f)(\alpha),$$

or more explicitly by

$$\overline{\chi}(\sum_i a_i x^i + K[x].\min(\alpha, \phi)) = \sum_i \phi(a_i)\alpha^i.$$

It follows that $\deg(\phi) = \deg(q(x))$. *In particular, if α is a primitive element for ϕ then*

$$L \simeq K[x]/(K[x].\min(\alpha, \phi)). \quad \square$$

Proposition 5.10. [prop-finite-algebraic]
Suppose we have a field K and an extension field L such that $[L : K] < \infty$. Then every element of L is algebraic over K.

Proof. Put $d = [L : K] = \dim_K(L)$. Consider an element $\alpha \in L$. The list $\mathcal{A} = 1, \alpha, \alpha^2, \ldots, \alpha^d$ has length $d + 1$, which is larger than the dimension of L, so $\mathcal{A}$ must be linearly dependent. We therefore have a linear relation $a_0.1 + a_1.\alpha + a_2.\alpha^2 + \cdots + a_d.\alpha^d = 0$, where not all the coefficients a_i are zero. If we put

$f(x) = \sum_i a_i x^i \in K[x]$ then this means that $f(x) \neq 0$ but $f(\alpha) = 0$. It follows that $f(x)$ is a nonzero element of $I(\alpha, K)$, as required. □

This is a convenient point to introduce another useful result that uses a related method.

Proposition 5.11. [prop-subring-subfield]
Suppose we have a field K, and extension L, and a subring $R \subseteq L$ such that $K \subseteq R$ and $\dim_K(R) < \infty$. Then R is actually a subfield of L.

Proof. Suppose that α is a nonzero element of R; we need to show that α has an inverse in R. Just as above we see that the powers of α are linearly dependent, so $I(\alpha, K) \neq 0$, so we have an irreducible monic polynomial $q(x) = \min(\alpha, K)(x) = \sum_{i=0}^d a_i x^i$ say, with $q(\alpha) = 0$. We claim that $q(0) \neq 0$. Indeed, if $q(0)$ were zero then x would be a nonconstant monic factor of the irreducible polynomial $q(x)$, which would mean that x would have to equal $q(x)$, so the equation $q(\alpha) = 0$ would give $\alpha = 0$, contradicting our assumption that α is nonzero. Thus, the constant term $a_0 = q(0)$ is nonzero, and thus invertible in K. We now put $\beta = -\sum_{i=1}^d a_0^{-1} a_i \alpha^{i-1} \in R$. The equation $\sum_{i=0}^d a_i \alpha^i = 0$ can then be rearranged to give $\alpha\beta = 1$, so β is the required inverse to α in R. □

Proposition 5.12. [prop-subfield-join]
Suppose we have fields K, L, M, N with $K \subseteq L \subseteq N$ and $K \subseteq M \subseteq N$, where $[L : K] < \infty$ and $[M : K] < \infty$. Put

$$LM = \{x \in M \mid x = a_1 b_1 + \dots + a_r b_r \text{ for some } a_1, \dots, a_r \in L \text{ and } b_1, \dots, b_r \in M\}.$$

Then LM is a subfield of N, and it is the smallest subfield that contains both L and M. Moreover, we have $[LM : K] \leq [L : K][M : K] < \infty$.

Proof. For any $b \in L$ we can write $b = b.1$ with $b \in L$ and $1 \in M$, so $b \in LM$. This means that $L \subseteq LM$, and similarly $M \subseteq LM$. In particular, this means that LM contains 0 and 1.

It is clear by definition that LM is closed under addition. If we have an element $x = \sum_i a_i b_i \in LM$ then $-x = \sum_i (-a_i) b_i$ which also lies in LM. It follows that LM is also closed under subtraction. Now suppose we have another element $y = \sum_j c_j d_j \in LM$, with $c_j \in L$ and $d_j \in M$. We can thus write xy as a finite sum of terms $(a_i c_j)(b_i d_j)$, where $a_i c_j \in L$ and $b_i d_j \in M$. It follows that $xy \in LM$. We now see that LM is a subring of N, but it is not yet clear that it is closed under taking inverses.

Now choose a basis $e_1, \dots, e_p$ for L over K, and a basis $f_1, \dots, f_q$ for M over K. Note that $p = [L : K]$ and $q = [M : K]$. Let V be the span over K of the elements $e_i f_j$. Any element $v \in V$ can be written as a sum of terms $v_{ij} e_i f_j$ with $v_{ij} \in K$, so $v_{ij} e_i \in L$ and $f_j \in M$, so $v \in LM$. Conversely, if $a \in L$ and $b \in M$ we can write $a = \sum_i x_i e_i$ and $b = \sum_j y_j f_j$ for some elements $x_i, y_j \in K$. It follows that $ab = \sum_{ij} x_i y_j e_i f_j$, with $x_i y_j \in K$. This means that $ab \in V$, and any element of LM is a sum of terms like ab, so it also lies in V. This proves that $LM = V$, so $\dim_K(LM) \leq pq = [L : K][M : K]$. In particular, we see that LM is a subring of N of finite dimension over K, so Proposition 5.11 tells us that it is actually a subfield.

We have already seen that LM contains both L and M. Let F be any other subfield of N that contains both L and M. Consider an element $x = \sum_i a_i b_i \in LM$. We then have $a_i \in L \subseteq F$ and $b_j \in M \subseteq F$ and F is closed under multiplication and addition so we must have $x \in F$. This proves that $LM \subseteq F$, so LM is the *smallest* subfield of N that contains both L and M. □

Definition 5.13. [defn-split]
Suppose we have a field K, an extension field L, and a monic polynomial $f(x) \in K[x]$ of degree d. We say that $f(x)$ *splits over* L if there is a list $\alpha_1, \dots, \alpha_d$ of elements of L such that $f(x) = \prod_{i=1}^d (x - \alpha_i)$. If the elements α_i are all different, we say that $f(x)$ *splits properly* over L. Similarly, if we have a homomorphism $\psi \colon K \to M$, we say that $f(x)$ is *(properly) split by* ψ if $(\psi_\bullet f)(x)$ splits (properly) in M.

Remark 5.14. [rem-distinct-roots]
If K has characteristic zero and $f(x)$ is irreducible in $K[x]$ and $f(x)$ splits over L, we see from Proposition 4.42 that the splitting is automatically proper.

Remark 5.15. [rem-fta-split]
Corollary 4.33 can now be rephrased as saying that every monic polynomial in $\mathbb{C}[x]$ actually splits over $\mathbb{C}$.

We will also use a slightly sharper concept:

Definition 5.16. [defn-splitting-field]
Suppose we have a field K, an extension field L, and a monic polynomial $f(x) \in K[x]$ of degree d. We say that L is a *splitting field for* $f(x)$ (or a *minimal splitting field*, if emphasis is necessary) if $f(x)$ splits in L, and L is generated over K by the roots of $f(x)$. Similarly, we say that a homomorphism $\psi\colon K \to M$ is a *(minimal) splitting homomorphism* for $f(x)$ if $(\psi_\bullet f)(x)$ splits in M, and M is generated over $\psi(K)$ by the roots of $(\psi_\bullet f)(x)$.

Proposition 5.17. [prop-construct-splitting]
Suppose that $f(x)$ is a monic polynomial of degree d in $K[x]$. Then $f(x)$ has a splitting field of degree at most $d!$ over K.

Proof. We will argue by induction on d. If $d = 0$ then $f(x) = 1$, which splits in K as a product of no factors. If $d = 1$ then $f(x)$ must have the form $f(x) = x - \alpha$ for some $\alpha \in K$, so again $f(x)$ is already split in K. For the general case, Remark 5.4 tells us that there is an extension $L \subseteq K$ with $[L : K] \leq d$, and an element $\alpha_d \in L$ with $f(\alpha_d) = 0$. It follows by Proposition 4.28 that there is a monic polynomial $g(x) \in L[x]$ of degree $d-1$ such that $f(x) = g(x)(x - \alpha_d)$. By induction we may assume that there is a field $M \supseteq L$ with $[M : L] \leq (d-1)!$, and a splitting $g(x) = \prod_{i=1}^{d-1}(x - \alpha_i)$ in $M[x]$. This in turn gives a splitting $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$ in $M[x]$, and $[M : K] = [M : L][L : K] \leq (d-1)! \times d = d!$ as required. □

Proposition 5.18. [prop-split-factor]
Suppose we have a splitting $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$ in $K[x]$, and also a factorisation $f(x) = g(x)h(x)$ in $K[x]$ (where $g(x)$ and $h(x)$ are monic). Then there is a subset $I \subseteq \{1, \dots, d\}$ such that $g(x) = \prod_{i \in I}(x - \alpha_i)$ and $h(x) = \prod_{i \not\in I}(x - \alpha_i)$.

Proof. Proposition 4.26 says that $g(x)$ and $h(x)$ can be written as products of irreducible elements, and by combining these we get an expression for $f(x)$ as a product of irreducible elements. On the other hand, the equation $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$ also factors $f(x)$ as a product of irreducible elements, and Proposition 4.26 implies that there is a unique such factorisation up to order. It follows that $g(x)$ must be the product of some subset of the terms $(x - \alpha_i)$, and $h(x)$ must be the product of the remaining terms. □

Remark 5.19. [rem-split-factor]
In the case where the elements α_i are all different, the proof can be simplified. We can then take $I = \{i \mid g(\alpha_i) = 0\}$, and $J = \{i \mid h(\alpha_i) = 0\}$. Note that for all i we have $g(\alpha_i)h(\alpha_i) = f(\alpha_i) = 0$, so either $g(\alpha_i) = 0$ or $h(\alpha_i) = 0$. This means that $I \cup J = \{1, \dots, d\}$, and so $|I| + |J| = d + |I \cap J|$. On the other hand, $g(x)$ has $|I|$ distinct roots, so $\deg(g(x)) \geq |I|$. Similarly $\deg(h(x)) \geq |J|$, and so

$$d = \deg(f(x)) = \deg(g(x)h(x)) = \deg(g(x)) + \deg(h(x)) \geq |I| + |J| = d + |I \cap J|.$$

The only way this can be consistent is if $I \cap J = \emptyset$ and $\deg(g(x)) = |I|$ and $\deg(h(x)) = |J|$. It follows in turn that $g(x) = \prod_{i \in I}(x - \alpha_i)$ and $h(x) = \prod_{j \in J}(x - \alpha_j) = \prod_{j \not\in I}(x - \alpha_j)$ as claimed.

Proposition 5.20. [prop-proper-splitting]
Let K be a field of characteristic zero. Suppose that $f(x)$ is a monic polynomial in $K[x]$, and that $L \supseteq K$ is a splitting field for $f(x)$. Then there is a polynomial $g(x) \in K[x]$ such that $g(x)$ splits properly in L and has the same roots in L as $f(x)$. In particular, L is also a splitting field for $g(x)$.

Proof. Proposition 4.26 tells us that $f(x)$ can be written in the form

$$f(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r},$$

where $p_1(x), \dots, p_r(x)$ are distinct monic irreducible polynomials in $K[x]$, and $n_1, \dots, n_r > 0$. Put $g(x) = p_1(x) \cdots p_r(x)$. This divides $f(x)$ and therefore splits over L by Proposition 5.18. If $g(\alpha) = 0$ then $p_i(\alpha) = 0$ for some i, so $f(\alpha) = 0$. Conversely, if $f(\alpha) = 0$ then $p_i(\alpha)^{n_i} = 0$ for some i, and so $p_i(\alpha) = 0$, so $g(\alpha) = 0$. Thus $g(x)$ has the same roots in L as $f(x)$. All that is left is to show that $g(x)$ splits *properly*, so it has no repeated roots. If $i \neq j$ then $p_i(x)$ and $p_j(x)$ are distinct monic irreducibles, so their greatest common divisor must be 1, so we have $a(x)p_i(x) + b(x)p_j(x) = 1$ for some $a(x), b(x) \in K[x]$. If $p_i(\alpha) = 0$ then we can substitute $x = \alpha$ to get $b(\alpha)p_j(\alpha) = 1$, so $p_j(\alpha) \neq 0$. This means that the roots of $p_i(x)$ and $p_j(x)$

are disjoint, so it will suffice to show that $p_i(x)$ has no repeated roots. As $p_i(x)$ is irreducible and K has characteristic zero, this follows from Proposition 4.42. □

Exercises

Exercise 5.1. [`ex-splitting-misc-i`]
Find the splitting fields for the following polynomials over $\mathbb{Q}$.

$$\begin{aligned} f_0(x) &= x^2 - 2x + 1 & f_1(x) &= x^4 - 5x^2 + 6 \\ f_2(x) &= x^2 - x + 1 & f_3(x) &= x^3 - 2 \\ f_4(x) &= x^4 - 4x^2 + 1 & f_5(x) &= x^4 - 2 \\ f_6(x) &= x^6 - 1 & f_7(x) &= x^6 - 8 \end{aligned}$$

Exercise 5.2. [`ex-splitting-misc-ii`]
Determine the degree over $\mathbb{Q}$ of the splitting fields of the following polynomials:

(a) $x^4 + 1$;
(b) $x^4 + x^2 + 1$ (note that this is reducible);
(c) $x^6 + 1$ (and so is this);
(d) $x^6 + x^3 + 1$.

Exercise 5.3. [`ex-transcendental`]
Suppose that $\alpha \in L \supset K$ and that α is transcendental over K. Let $K(x)$ be the field of rational functions over K (as in Example 1.4). Show that there is an isomorphism $\phi\colon K(x) \to K(\alpha)$ with $\phi(x) = \alpha$.

Exercise 5.4. [`ex-cayley`]
Suppose we have a field K, an extension field L such that $d = [L : K] < \infty$, and an element $\alpha \in L$. By applying the Cayley-Hamilton theorem to a suitable K-linear endomorphism of L, give another proof that α is algebraic over K.

Exercise 5.5. [`ex-Q-bar`]
Let $\overline{\mathbb{Q}}$ denote the set of all numbers $\alpha \in \mathbb{C}$ such that α is algebraic over $\mathbb{Q}$ (as in Remark 5.7).

(a) For $\alpha \in \mathbb{C}$, show that the following are equivalent:
  (i) $\alpha \in \overline{\mathbb{Q}}$
  (ii) $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$
  (iii) There exists a subfield $K \subseteq \mathbb{C}$ with $\alpha \in K$ and $[K : \mathbb{Q}] < \infty$.
(b) Show that $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.
(c) Show that if $\alpha \in \mathbb{C}$ and α is algebraic over $\overline{\mathbb{Q}}$ then $\alpha \in \overline{\mathbb{Q}}$.
(d) Deduce that $\overline{\mathbb{Q}}$ is algebraically closed.

(You should use part (a) to help you with (b) and (c).)

Exercise 5.6. [`ex-F-sixteen`]
We have seen that there is a field $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, where α has minimal polynomial $t^2 + t + 1$ over $\mathbb{F}_2$. You may assume that there is also a field $\mathbb{F}_{16} = \mathbb{F}_2(\beta)$, where β has minimal polynomial $t^4 + t^3 + t^2 + t + 1$ over $\mathbb{F}_2$.

(a) Write down a basis for $\mathbb{F}_4$ over $\mathbb{F}_2$, and list the four elements of $\mathbb{F}_4$.
(b) Write down a basis for $\mathbb{F}_{16}$ over $\mathbb{F}_2$, and list the sixteen elements of $\mathbb{F}_{16}$.
(c) Check that $\beta^5 = 1$.
(d) There are precisely two homomorphisms from $\mathbb{F}_4$ to $\mathbb{F}_{16}$. Find them.

6. Extending homomorphisms

Definition 6.1. [defn-E]
Suppose we have fields K, L and M and homomorphisms $\phi\colon K\to L$ and $\psi\colon K\to M$. We write $E(\phi,\psi)$ for the set of homomorphisms $\theta\colon L\to M$ with $\theta\phi=\psi$. The fields and homomorphisms mentioned here can be displayed as follows:

$$\begin{tikzcd}
L \arrow[rr, dotted, "\theta"] & & M \\
& K \arrow[ul, "\phi"] \arrow[ur, "\psi"'] &
\end{tikzcd}$$

We also put $G(\phi)=E(\phi,\phi)$.

In particular, suppose we have a field F with subfields K, L and M such that $K\subseteq L\cap M$. We then have inclusion maps $\mathrm{inc}_K^L\colon K\to L$ and $\mathrm{inc}_K^m\colon K\to M$, and we write

$$E_K(L,M)=E(\mathrm{inc}_K^L,\mathrm{inc}_K^M)=\{\theta\colon L\to M\mid \theta|_K=1_K\}.$$

We also write $G(L/K)$ for $E_K(L,L)$.

Remark 6.2. [rem-E-empty]
Because $\deg(\theta\phi)=\deg(\theta)\deg(\phi)\geq\deg(\phi)$, we see that $E(\phi,\psi)$ can only be nonempty when $\deg(\phi)\leq\deg(\psi)$.

Proposition 6.3. [prop-galois-group]
If $\deg(\phi)<\infty$ then $G(\phi)$ is a group under composition. In alternative notation, if $[L:K]<\infty$ then $G(L/K)$ is a group under composition. (These groups are called Galois groups.*)*

Proof. First, if $\theta,\eta\in G(\phi)$ then $\theta\phi=\phi$ and $\eta\phi=\phi$ so $(\theta\eta)\phi=\theta(\eta\phi)=\theta\phi=\phi$, so $\theta\eta\in G(\phi)$.

$$\begin{tikzcd}
L \arrow[r, "\eta"] & L \arrow[r, "\theta"] & L \\
& K \arrow[ul, "\phi"] \arrow[u, "\phi"] \arrow[ur, "\phi"'] &
\end{tikzcd}$$

Next, the identity map 1_L lies in $G(\phi)$ and serves as a two-sided identity element for composition. Finally, if $\deg(\phi)<\infty$ and $\theta\in G(\phi)$ then we can cancel $\deg(\phi)$ in the identity $\deg(\phi)=\deg(\theta\phi)=\deg(\theta)\deg(\phi)$ to see that $\deg(\theta)=1$. It follows from Proposition 2.25 that θ is an isomorphism. We can compose both sides of the identity $\phi=\theta\phi$ with θ^{-1} to see that $\theta^{-1}\phi=\phi$, so $\theta^{-1}\in G(\phi)$ and serves there as an inverse for θ. □

It turns out to be important to understand the size of the sets $E(\phi,\psi)$. The most basic fact is as follows:

Proposition 6.4. [prop-E-bound]
For any ϕ and ψ as above, we have $|E(\phi,\psi)|\leq\deg(\phi)$.

After some preliminaries, we will give two different proofs, each of which introduces new concepts that will be useful later.

The following result (or a minor variant) is often called Dedekind's Lemma:

Proposition 6.5. [prop-dedekind]
Let L and M be fields, let $\theta_1,\dots,\theta_n\colon L\to M$ be distinct homomorphisms, and let $b_1,\dots,b_n$ be elements of M. Suppose that for all $a\in K$ we have $\sum_{i=1}^n b_i\theta_i(a)=0$. Then $b_1=b_2=\ldots=b_n=0$.

Proof. We will argue by induction on n. If $n=1$ then we have $b_1\theta_1(a)=0$ for all $a\in K$, and we can take $a=1$ to see that $b_1=0$; this starts the induction. Now suppose that $n>1$. Fix some $t\in L$, and put $c_i=b_i(\theta_i(t)-\theta_n(t))$, so $c_n=0$. We claim that $\sum_{i=1}^{n-1}c_i\theta_i(a)=0$ for all $a\in L$. Indeed, the relation $\sum_{i=1}^n b_i\theta_i(a)=0$ is valid for all $a\in L$, so it works for ta in place of a, which give $\sum_{i=1}^n b_i\theta_i(t)\theta_i(a)=0$. On the other hand, we can just multiply the relation $\sum_{i=1}^n b_i\theta_i(a)=0$ by $\theta_n(t)$ to get $\sum_{i=1}^n b_i\theta_n(t)\theta_i(a)=0$, and then subtract this from the previous relation to get $\sum_{i=1}^{n-1}c_i\theta_i(a)=0$ as claimed. We deduce from the induction hypothesis that $c_1=\cdots=c_{n-1}=0$, so $b_i(\theta_i(t)-\theta_n(t))=0$ for all $i<n$ (and all $t\in L$, because t was arbitrary). By assumption the homomorphisms θ_i are all different, so for each $i<n$ we can choose

$t_i \in L$ with $\theta_i(t_i) \neq \theta_n(t_i)$. We can then take $t = t_i$ in the relation $b_i(\theta_i(t) - \theta_n(t)) = 0$ to get $b_i = 0$. This shows that $b_1 = \dots = b_{n-1} = 0$, so the relation $\sum_{i=1}^n b_i\theta_i(a)$ reduces to $b_n\theta_n(a) = 0$ for all a. Now take $a = 1$ to see that $b_n = 0$ as well. □

First proof of Proposition 6.4. Let $e_1, \dots, e_m$ be a basis for L over $\phi(K)$ (so $m = \deg(\phi)$). Let $\theta_1, \dots, \theta_n$ be the distinct elements of $E(\phi, \psi)$, so $\theta_i\phi = \psi \colon K \to M$. Define $v_1, \dots, v_n \in M^m$ by $v_i = (\theta_i(e_1), \dots, \theta_i(e_m))$. We claim that these n vectors are linearly independent over M. To see this, consider a linear relation $b_1v_1 + \dots + b_nv_n = 0$ (with $b_1, \dots, b_n \in M$). This means that $\sum_{i=1}^n b_i\theta_i(e_j) = 0$ for all j. Now consider an arbitrary element $a \in L$. As the elements e_j give a basis for L over $\phi(K)$, we can write $a = \sum_{j=1}^m \phi(x_j)e_j$ for some $x_1, \dots, x_m \in K$. We can then apply θ_i to this, recalling that $\theta_i\phi = \psi$, to get $\theta_i(a) = \sum_{j=1}^m \psi(x_j)\theta_i(e_j)$. It follows that

$$\sum_{i=1}^n b_i\theta_i(a) = \sum_{i=1}^n\sum_{j=1}^m b_i\psi(x_j)\theta_i(e_j) = \sum_{j=1}^m \left(\psi(x_j)\sum_{i=1}^n b_i\theta_i(e_j)\right) = 0.$$

Proposition 6.5 therefore tells us that $b_1 = \dots = b_n = 0$. We deduce that the vectors $v_1, \dots, v_n$ in M^m are linearly independent as claimed. The length of any linearly independent list is at most the dimension of the containing space, so we have $n \leq m$, or in other words $|E(\phi, \psi)| \leq \deg(\phi)$. □

We next discuss a different approach, which starts by discusing the case where ϕ has a primitive element, and then extends this by induction.

Lemma 6.6. [`lem-E-bound`]
Suppose we have ϕ and ψ as above, and that α is a algebraic primitive element for ϕ, with minimal polynomial $q(x) = \min(\alpha, \phi) \in K[x]$ say. Then $E(\phi, \psi)$ bijects with the set of roots of $(\psi_\bullet q)(x)$ in M, and $|E(\phi, \psi)| \leq \deg(q(x)) = \deg(\phi)$.

Proof. Let d be the degree of $q(x)$, or equivalently the degree of the homomorphism ϕ. Let F be the set of roots of $(\psi_\bullet q)(x)$ in M, so Corollary 4.30 tells us that $|F| \leq d$.

We can write $q(x)$ in the form $q(x) = a_0 + a_1x + \dots + a_dx^d$, where $a_d = 1$ because $q(x)$ is monic. By definition we have $(\phi_\bullet q)(\alpha) = 0$, or equivalently $\sum_i \phi(a_i)\alpha^i = 0$. Suppose that $\theta \in E(\phi, \psi)$, so $\theta\phi = \psi : K \to M$. We can then apply θ to the above equation to get

$$(\psi_\bullet q)(\theta(\alpha)) = \sum_i \psi(a_i)\theta(\alpha)^i = \theta(\sum_i a_i\alpha^i) = \theta(0) = 0,$$

so $\theta(\alpha) \in F$. We can thus define a map $P \colon E(\phi, \psi) \to F$ by $P(\theta) = \theta(\alpha)$.

Now suppose we have two elements $\theta_0, \theta_1 \in E(\phi, \psi)$ with $P(\theta_0) = P(\theta_1)$, so $\theta_0(\alpha) = \theta_1(\alpha) = \beta$ say. It follows from Corollary 5.9 that every element $\sigma \in L$ can be written in the form $\sigma = \sum_{j=0}^{d-1} \phi(b_j)\alpha^j$, for some elements $b_j \in K$. Using $\theta_i(\phi(b)) = \psi(b)$ and $\theta_i(\alpha) = \beta$ we deduce that $\theta_0(\sigma) = \sum_j \psi(b_j)\beta^j = \theta_1(\sigma)$. As σ was arbitrary this means that $\theta_0 = \theta_1$, so we see that P is injective.

Finally, consider a general element $\beta \in F$, so β is a root of $(\psi_\bullet q)(x)$. We can then define a homomorphism $\lambda \colon K[x] \to M$ by $\lambda(f(x)) = (\psi_\bullet f)(\beta)$, or more explicitly

$$\lambda(\sum_i b_ix^i) = \sum_i \psi(b_i)\beta^i.$$

We then have $\lambda(q(x)) = 0$, so $\lambda(K[x].q(x)) = 0$. Proposition 3.10 therefore gives us a homomorphism

$$\overline{\lambda} \colon K[x]/(K[x].q(x)) \to M,$$

which we can compose with the inverse of the isomorphism $\overline{\chi} \colon K[x]/(K[x].q(x)) \to L$ to get a homomorphism $\theta = \overline{\lambda} \circ \overline{\chi}^{-1} \colon L \to M$ which clearly satisfies $P(\theta) = \beta$. This means that P is also surjective, so it is a bijection, so $|E(\phi, \psi)| = |F| \leq d$. □

Proposition 6.7. [`prop-E-comp`]
Suppose we have homomorphisms

$$L \xleftarrow{\zeta} N \xleftarrow{\xi} K \xrightarrow{\psi} M.$$

Then $|E(\zeta\xi, \psi)| = \sum_{\theta \in E(\xi, \psi)} |E(\zeta, \theta)|$.

Proof. Let F be the set of pairs (θ,η) such that $\theta \in E(\xi,\psi)$ and $\eta \in E(\zeta,\theta)$. It is clear that $|F| = \sum_{\theta\in E(\xi,\psi)} |E(\zeta,\theta)|$, so it will suffice to show that F bijects with $E(\zeta\xi,\psi)$.

If $\eta \in E(\zeta\xi,\psi)$ then $\eta\zeta\xi = \psi$, so the homomorphism $\theta = \eta\zeta \colon N \to M$ satisfies $\theta\xi = \psi$, so $\theta \in E(\xi,\phi)$. From the definition $\theta = \eta\zeta$ we also see that $\eta \in E(\zeta,\theta)$, so $(\theta,\eta) \in F$. We can thus define $P \colon E(\xi\zeta,\psi) \to F$ by $P(\eta) = (\eta\zeta,\eta)$, and this is clearly a bijection with $P^{-1}(\eta) = (\eta\zeta,\eta)$.

The following diagram may help to follow the argument:

$$\begin{tikzcd}
K \arrow[r, "\xi"] \arrow[d, "\psi"'] & N \arrow[r, "\zeta"] \arrow[d, dotted, "\theta"] & L \arrow[d, dotted, "\eta"] \\
M \arrow[r, "1"'] & M \arrow[r, "1"'] & M.
\end{tikzcd}$$

□

Proof of Proposition 6.4. If $\deg(\phi) = \infty$ then there is nothing to prove, so we may assume that $\deg(\phi) < \infty$. We will argue by induction on $\deg(\phi)$. If $\deg(\phi) = 1$ then ϕ is an isomorphism (by Proposition 2.25) and so $|E(\phi,\psi)| = |\{\psi\phi^{-1}\}| = 1$ as required. Now consider the general case, where $\deg(\phi) = k > 1$ say, and assume inductively that the proposition is valid for all homomorphisms of degree less than k. Put $K' = \phi(K)$. As ϕ is not an isomorphism, we have $K' < L$, so we can choose $\alpha \in L \setminus K'$. If $K'(\alpha) = L$ then the claim holds by Lemma 6.6. Otherwise, let ζ be the inclusion $K'(\alpha) \to L$, and let ξ be ϕ regarded as a homomorphism $K \to K'(\alpha)$, so $\zeta\xi = \phi$. Proposition 6.7 then gives

$$|E(\phi,\psi)| = |E(\zeta\xi,\psi)| = \sum_{\theta\in E(\xi,\psi)} |E(\zeta,\theta)|.$$

As $\alpha \notin K'$ and $K'(\alpha) \neq L$ we see that $\deg(\zeta), \deg(\xi) > 1$, but $\deg(\zeta)\deg(\xi) = \deg(\phi) = k$, so $\deg(\zeta), \deg(\xi) < k$. We can thus apply the induction hypothesis to see that $|E(\xi,\psi)| \leq \deg(\xi)$ and $|E(\zeta,\theta)| \leq \deg(\zeta)$. Feeding this into the above equation gives

$$|E(\phi,\psi)| \leq \sum_{\theta\in E(\xi,\psi)} \deg(\zeta) = |E(\xi,\psi)| \deg(\zeta) \leq \deg(\xi)\deg(\zeta) = \deg(\phi)$$

as required. □

Definition 6.8. [`defn-normal`]
Let $\psi \colon K \to M$ be an extension of finite degree. We say that ψ is *normal* if it has the following property: for every irreducible polynomial $f(x) \in K[x]$ such that $(\psi_\bullet f)(x)$ has a root, $f(x)$ is properly split by ψ.

Lemma 6.9. [`lem-splitting-ext`]
Suppose we have a field K, a monic polynomial $f(x) \in K[x]$, and a proper splitting field L for $f(x)$. Then $|G(L/K)| = d = [L : K]$.

Proof. We have a splitting $f(x) = \prod_{i=1}^{r}(x - \alpha_i)$ in $L[x]$, with all the roots α_i being different. Put $K_0 = K$, and $K_i = K_{i-1}(\alpha_i)$ for $i > 0$, so $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$. Moreover, K_r is a subfield of L that contains K and all the roots α_i, so it must be all of L. Put $d_i = [K_i : K_{i-1}]$, so $d = \prod_{i=1}^{r} d_i$. The claim is that there are precisely d different homomorphisms $\theta \colon L \to L$ with $\theta|_K = 1$. More generally, we claim that the number of homomorphisms $\theta \colon K_i \to L$ with $\theta|_K = 1$ is precisely $\prod_{j=1}^{i} d_j$. This is true for $i = 0$ (where the product has no terms and so is equal to one). It will thus be enough to prove the following induction step: given $\theta \colon K_{i-1} \to L$ with $\theta|_K = 1$, there are precisely d_i ways to extend it to a homomorphism $\theta' \colon K_i \to L$. To see this, put $g_i(x) = \min(\alpha_i, K_{i-1})$, which is a polynomial of degree d_i. Lemma 6.6 tells us that the extensions of θ biject with the roots of $(\theta_\bullet g_i)(x)$, so it will be enough to show that that polynomial is properly split. Note that $f(x) \in K[x] \subseteq K_{i-1}[x]$ and note that $f(\alpha_i) = 0$, so $f(x)$ must be divisible in $K_{i-1}[x]$ by $g_i(x)$, say $f(x) = g_i(x)h_i(x)$. We now apply $\theta_\bullet$ to this equation, noting that $\theta_\bullet f = f$ because $f(x) \in K[x]$ and $\theta|_K = 1$. We find that $(\theta_\bullet g)(x)(\theta_\bullet h)(x) = f(x)$, so Proposition 5.18 tells us that $(\theta_\bullet g)(x)$ is properly split as required. □

Remark 6.10. [`rem-splitting-ext`]
Suppose that K has characteristic zero, and that L is a (not necessarily proper) splitting field for some monic

polynomial $f(x) \in K[x]$. Remark 5.19 tells us that L is a proper splitting field for some polynomial $g(x)$ that divides $f(x)$, and we can apply the above lemma to $g(x)$ to see that $|G(L/K)| = [L : K]$ again.

Proposition 6.11. [`prop-normal`]
Let $\psi\colon K \to M$ be a homomorphism of finite degree. Then the following are equivalent:

(a) *For every field L and homomorphism $\phi\colon K \to L$, we have either $|E(\phi, \psi)| = 0$ or $|E(\phi, \psi)| = \deg(\phi)$.*
(b) *$|G(\psi)| = \deg(\psi)$.*
(c) *ψ is normal.*
(d) *ψ is a proper splitting extension for some polynomial $f(x) \in K[x]$.*

Proof. First suppose that (a) holds. Recall that $G(\psi) = E(\psi, \psi)$, and this set clearly contains the identity map 1_M, so it is nonempty. It follows by (a) that we must have $|G(\psi)| = \deg(\psi)$, so (b) holds.

Conversely, suppose that (b) holds. Suppose we have a homomorphism $\phi\colon K \to L$ such that $E(\phi, \psi) \neq \emptyset$, so we can choose $\theta \in E(\phi, \psi)$, so $\theta\phi = \psi\colon K \to M$. It follows from our assumptions and Proposition 6.7 that

$$\begin{aligned}\deg(\phi)\deg(\theta) = \deg(\psi) &= |E(\psi, \psi)| = |E(\theta\phi, \psi)| \\ &= \sum_{\lambda \in E(\phi,\psi)} |E(\theta, \lambda)| \leq \sum_{\lambda \in E(\phi,\psi)} \deg(\theta) = |E(\phi, \psi)| \deg(\theta).\end{aligned}$$

This can be rearranged to give $|E(\phi, \psi)| \geq \deg(\phi)$, and Proposition 6.4 gives the reverse inequality, so (b) holds. We now see that (a) and (b) are equivalent.

Now suppose that (a) and (b) hold, and consider (c). Suppose we have an irreducible polynomial $f(x) \in K[x]$, of degree d. Put $L = K[x]/(K[x].f(x))$ as in Proposition 5.3, so L is a field equipped with an obvious homomorphism $\phi\colon K \to L$ of degree d. We let α denote the image of x in L, which is a primitive element for ϕ, with minimal polynomial $f(x)$. We see from Lemma 6.6 that the number of roots of $(\psi_\bullet f)(x)$ is $|E(\phi, \psi)|$, which is either 0 or d by (b). Thus, if there is at least one root then there are d distinct roots, say $\beta_1, \ldots, \beta_d$. It follows by Proposition 4.29 that $(\psi_\bullet f)(x) = \prod_{i=1}^{d}(x - \beta_i)$, so $(\psi_\bullet f)(x)$ is split as required.

Now suppose that (c) holds, so ψ is normal. Choose a basis $\alpha_1, \ldots, \alpha_d$ for M over $\psi(K)$, and put $f_i(x) = \min(\alpha_i, \psi)$ and $f(x) = \prod_i f_i(x)$. Then $(\psi_\bullet f_i)(x)$ has a root α_i and ψ is normal so $(\psi_\bullet f_i)(x)$ must be split. It follows that $(\psi_\bullet f)(x)$ is also split, and the roots include the elements α_i, so they certainly generate M. Thus (d) holds.

Finally, Lemma 6.9 shows that (d) implies (b), completing the cycle. □

Remark 6.12. [`rem-normal-not-transitive`]
Suppose we have fields $K \subseteq L \subseteq M$, where L is normal over K, and M is normal over L. It need not be the case that L is normal over K. For an example (which will be revisited as Example 7.6), take $\alpha = \sqrt{3 + \sqrt{7}}$ and consider the chain $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{7}) \subseteq \mathbb{Q}(\alpha)$. Here $\mathbb{Q}(\sqrt{7})$ is a splitting field for $x^2 - 7$ over $\mathbb{Q}(\sqrt{7})$, and $\mathbb{Q}(\alpha)$ is a splitting field for $x^2 - 3 - \sqrt{7}$ over $\mathbb{Q}(\sqrt{7})$, so both these extensions are normal. However, we claim that $\mathbb{Q}(\alpha)$ is not normal over $\mathbb{Q}$. Indeed, α is a root of the polynomial $f(x) = x^4 - 6x^2 + 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion at the prime 2. The element $\beta = \sqrt{3 - \sqrt{7}}$ is another root of $f(x)$ in $\mathbb{R}$. We will show in Example 7.6 that $\beta \notin \mathbb{Q}(\alpha)$ (a key point being that $\alpha\beta = \sqrt{2}$). It follows that $f(x)$ does not split in $\mathbb{Q}(\alpha)[x]$, and thus that $\mathbb{Q}(\alpha)$ is not normal over $\mathbb{Q}$, as claimed.

Corollary 6.13. [`cor-normal-closure`]
Let $\xi\colon K \to N$ be a homomorphism of finite degree. Then there is a field M and a homomorphism $\eta\colon N \to M$ such that $\eta\xi$ is normal.

Proof. Choose a basis $e_1, \ldots, e_n$ for N over $\xi(K)$. Put $f_i(t) = \min(e_i, \xi)$ and $f(t) = \prod_i f_i(t) \in K[t]$. Let $\eta\colon N \to M$ be a splitting homomorphism for $(\xi_\bullet f)(t)$ (which is possible by Proposition 5.17). Let M' be the subfield of M generated by $\eta\xi(K)$ together with the roots of the polynomial $g(t) = ((\eta\xi)_\bullet f)(t)$. As $(\xi_\bullet f_i)(e_i) = 0$ we see that $g(\eta(e_i)) = 0$, and the elements e_i generate L over $\xi(K)$ so the elements $\eta(e_i)$ generate $\eta(L)$ over $\eta\xi(K)$, so $\eta(L) \subseteq M'$. Moreover, as η is a splitting homomorphism for $(\xi_\bullet f)(t)$ we know that the roots of $g(t)$ generate M over $\eta(L)$. It follows that $M = M'$, so $\eta\xi$ is a splitting homomorphism for $f(t)$. It follows that $\eta\xi$ is normal as claimed. □

Proposition 6.14. [prop-top-normal]
Let $K \xrightarrow{\xi} N \xrightarrow{\eta} M$ be homomorphisms such that $\eta\xi$ is normal. Then:

(a) *η is also normal.*
(b) *Suppose we have a homomorphism $\zeta\colon N \to L$ such that $E(\zeta\xi, \eta\xi) \neq \emptyset$ (and so $|E(\zeta\xi, \eta\xi)| = \deg(\zeta\xi) = \deg(\zeta)\deg(\xi)$). Then also $E(\zeta, \eta) \neq \emptyset$ (and so $|E(\zeta, \eta)| = \deg(\zeta)$).*

Proof. We start with the second statement. Let ξ, η and ζ be as in (b). We apply Lemma 6.7 (with $\psi = \eta\xi$) to see that

$$\deg(\zeta)\deg(\xi) = |E(\zeta\xi, \eta\xi)| = \sum_{\theta \in E(\xi, \eta\xi)} |E(\zeta, \theta)|.$$

The number of terms in the sum is $|E(\xi, \eta\xi)| \leq \deg(\xi)$, and each term $|E(\zeta, \theta)|$ is at most $\deg(\zeta)$. Thus, the only way that the sum can be equal to $\deg(\zeta)\deg(\xi)$ is if all these inequalities are actually equalities, so $|E(\xi, \eta\xi)| = \deg(\xi)$ and $|E(\zeta, \theta)| = \deg(\zeta)$ for all $\theta \in E(\xi, \eta\xi)$. Recall here that $\theta \in E(\xi, \eta\xi)$ just means that $\theta\xi = \eta\xi$, so certainly $\eta \in E(\xi, \eta\xi)$. We can thus take $\theta = \eta$ in the previous statement to see that $|E(\zeta, \eta)| = \deg(\zeta)$ as claimed (so in particular $E(\zeta, \eta) \neq \emptyset$).

We now deduce that η is normal. Consider $\zeta\colon N \to L$ such that $E(\zeta, \eta) \neq \emptyset$. This means that there exists $\sigma\colon L \to M$ with $\sigma\zeta = \eta$. It follows that $\sigma\zeta\xi = \eta\xi$, so $\sigma \in E(\zeta\xi, \eta\xi)$, so we can apply (b) to see that $|E(\zeta, \eta)| = \deg(\zeta)$. By Proposition 6.11(a), this means that η is normal.

The homomorphisms considered above can be displayed as follows:

$$\begin{tikzcd}
L \arrow[rr, dotted, "\sigma"] & & M \\
& N \arrow[ul, "\zeta"'] \arrow[ur, "{\eta,\theta}"'] & \\
& K \arrow[u, "\xi"'] &
\end{tikzcd}$$

□

Corollary 6.15. [cor-top-normal-a]
Let $K \xrightarrow{\xi} N \xrightarrow{\eta} M$ be homomorphisms such that $\eta\xi$ is normal, and let $\zeta\colon N \to M$ be a homomorphism such that $\zeta\xi = \eta\xi$. Then η is normal, and there exists $\sigma\colon M \to M$ with $\sigma\zeta = \eta$.

Proof. This is a special case of part (b) of the proposition, where $L = M$ and $\zeta\xi = \eta\xi$. In this context, the homomorphism 1_M is an element of $E(\zeta\xi, \eta\xi)$, so $E(\zeta\xi, \eta\xi) \neq \emptyset$. The proposition then tells us that $E(\zeta, \eta) \neq \emptyset$, so we can choose $\sigma \in E(\zeta, \xi)$, which means precisely that $\sigma\zeta = \eta$ as claimed. □

Corollary 6.16. [cor-top-normal-b]
Suppose we have a chain of finite extension $K \subseteq N \subseteq M$ such that M is normal over K. Then M is also normal over N. Moreover, for any homomorphism $\zeta\colon N \to M$ such that $\zeta|_K = 1_K$, there is an automorphism σ of M such that $\sigma|_N = \zeta$. Also, if σ' is any other automorphism of M with $\sigma'|_N = \zeta$ then $\sigma' = \sigma\tau$ for some $\tau \in G(M/N)$.

Proof. The first claim is a special case of the previous corollary, where $\xi\colon K \to N$ and $\eta\colon N \to M$ are just the inclusion maps. Now suppose we have another automorphism σ' with $\sigma'|_N = \zeta$. Put $\tau = \sigma^{-1}\sigma'\colon M \to M$, so $\sigma' = \sigma\tau$. If $a \in N$ then $\sigma'(a) = \zeta(a) = \sigma(a)$ and we can apply σ^{-1} to this equation to see that $\tau(a) = a$. This shows that $\tau \in G(M/N)$ as claimed. □

We next discuss the action of Galois groups on sets of roots. Suppose we have a field extension $K \subseteq L$, and a polynomial $f \in K[x]$. Put $R = \{\alpha \in L \mid f(\alpha) = 0\}$, the (finite) set of roots of f in L. We write Σ_R for the set of permutations of R, or in other words the set of bijective functions $\sigma\colon R \to R$.

It is more usual to discuss the group Σ_n of permutations of the finite set $N = \{1, \dots, n\}$, but but it is no harder to consider permutations of an arbitrary finite set, as we do here. For example, suppose we have a set $R = \{\alpha, \beta, \gamma\}$ of size three. We then have a transposition $\tau = (\alpha\ \beta)$, defined by $\tau(\alpha) = \beta$ and $\tau(\beta) = \alpha$ and $\tau(\gamma) = \gamma$. We also have a three-cycle $\rho = (\alpha\ \beta\ \gamma)$, defined by $\rho(\alpha) = \beta$ and $\rho(\beta) = \gamma$ and $\rho(\gamma) = \alpha$. The full group Σ_R consists of the identity permutation, the three-cycles ρ and $\rho^{-1} = (\gamma\ \beta\ \alpha)$, and the transpositions $\tau = (\alpha\ \beta)$, $(\beta\ \gamma)$ and $(\gamma\ \alpha)$. In general, if $|R| = n$ then Σ_R is isomorphic to Σ_n. To see this, we choose a numbering of the elements of R, say $R = \{\alpha_1, \dots, \alpha_n\}$. Then for any $\sigma \in \Sigma_R$ we must have $\sigma(\alpha_i) = \alpha_{\overline{\sigma}(i)}$ for some index $\overline{\sigma}(i)$. It is easy to see that $\overline{\sigma}$ is then a permutation of $\{1, \dots, n\}$, and the correspondence $\sigma \leftrightarrow \overline{\sigma}$ gives an isomorphism $\Sigma_R \simeq \Sigma_n$.

Proposition 6.17. [prop-root-perms]
Let R be the set of roots in L of a polynomial $f(x) \in K[x]$, with $K \leq L$.

(a) *If $\sigma \in G(L/K)$ and $\alpha \in R$ then $\sigma(\alpha) \in R$. Thus, there is a homomorphism $G(L/K) \to \Sigma_R$ given by $\sigma \mapsto \sigma|_R$.*
(b) *If L is a splitting field for $f(x)$ then this homomorphism is injective, so $G(L/K)$ can be regarded as a subgroup of Σ_R.*
(c) *If $f(x)$ is irreducible then for all $\alpha, \beta \in R$ there exists $\sigma \in G(L/K)$ such that $\sigma(\alpha) = \beta$. In other words, the group $G(L/K)$ acts transitively on R.*

Proof. (a) We can write $f(x) = \sum_{i=0}^{d} a_i x^i$, where $a_i \in K$. Suppose that $\alpha \in R$, so $\sum_{i=0}^{d} a_i \alpha^i = f(\alpha) = 0$. We can apply σ to this to get $\sum_{i=0}^{d} \sigma(a_i)\sigma(\alpha)^i = \sigma(0) = 0$. However, we have $\sigma \in G(L/K)$ so $\sigma|_K = 1_K$, and $a_i \in K$ so $\sigma(a_i) = a_i$. We therefore have $\sum_{i=0}^{d} a_i \sigma(\alpha)^i = 0$, or in other words $f(\sigma(\alpha)) = 0$, so $\sigma(\alpha) \in R$ as claimed. We can therefore restrict σ to give a map $\sigma|_R \colon R \to R$. Now $G(L/K)$ is a group, so we have an inverse element $\sigma^{-1} \in G(L/K)$, which we can also restrict to get another map $\sigma^{-1}|_R \colon R \to R$. This is easily seen to be inverse to $\sigma|_R$, so $\sigma|_R$ is a bijection and thus an element of Σ_R. It is also clear that restriction is compatible with composition and thus that the map $\sigma \mapsto \sigma|_R$ is a homomorphism $G(L/K) \to \Sigma_R$.

(b) Now suppose that L is a splitting field for $f(x)$, so L is generated over K by R, so the only field L' with $K \cup R \subseteq L' \subseteq L$ is L itself. Put $H = \{\sigma \in G(L/K) \mid \sigma|_R = 1_R\}$, which is the kernel of our homomorphism $G(L/K) \to \Sigma_R$. Consider the subfield

$$L^H = \{a \in L \mid \sigma(a) = a \text{ for all } \sigma \in H\}$$

(as in Proposition 1.31). Clearly $R \subseteq L^H$ by the definition of H. Moreover, all elements of $G(L/K)$ act as the identity on K (by the definition of $G(L/K)$) so $K \subseteq L^H$. As L is generated over K by R, we must have $L^H = L$. This means that for all $\sigma \in H$ we have $\sigma(a) = a$ for all $a \in L$, so $\sigma = 1_L$. This shows that $H = \{1_L\}$, so our homomorphism $G(L/K) \to \Sigma_R$ has trivial kernel and is therefore injective.

(c) Now suppose that $f(x)$ is irreducible, so $\min(\alpha, K) = f(x)$ for all $\alpha \in R$. Consider a pair of roots $\alpha, \beta \in R$. Note that α is a primitive element for $K(\alpha)$ and that β is a root of $\min(\alpha, K)$. It therefore follows from Lemma 6.6 that there is a unique homomorphism $\theta \colon K(\alpha) \to L$ with $\theta|_K = 1_K$ and $\theta(\alpha) = \beta$. Corollary 6.16 (applied to the chain $K \subseteq K(\alpha) \subseteq L$) now tells us that there is an automorphism σ of L such that $\sigma|_{K(\alpha)} = \theta$, and in particular $\sigma(\alpha) = \theta(\alpha) = \beta$ as required.

□

Remark 6.18. [rem-generic-galois]
If L is a splitting field for a randomly generated polynomial $f(x) \in K[x]$ (for an infinite field K), the most common situation is that the map $G(L/K) \to \Sigma_R$ is an isomorphism. However, we will mostly consider special cases where the Galois group is smaller than Σ_R, as these tend to have a more interesting structure.

Exercises

Exercise 6.1. [ex-abelian-transitive]
Let A be an abelian subgroup of Σ_n that acts transitively on the set $N = \{1, 2, \dots, n\}$. Show that if $\sigma \in A$ and $\sigma(i) = i$ for some $i \in N$, then σ is the identity. (In other words, the action is free.) Deduce that $|A| = n$.

Exercise 6.2. [ex-root-sqrt]
Consider a monic polynomial $f(x) \in \mathbb{Q}[x]$ of degree $d > 1$.

(a) Show that if $f(x^2)$ is irreducible, then so is $f(x)$.

(b) Give an example where $f(x)$ is irreducible but $f(x^2)$ is not.
(c) Suppose that $f(x^2)$ is irreducible. Let K be the splitting field of $f(x)$ in $\mathbb{C}$, and let L be the splitting field of $f(x^2)$. How much can you say about the relationship between K and L, and the corresponding Galois groups?

Exercise 6.3. [`ex-sqrt-chain`]
Consider the field $K=\mathbb{Q}(\sqrt{111+\sqrt{11+\sqrt{1111}}})$. This can be considered as the top of a chain of extensions

$$\mathbb{Q}=K_0\subset\mathbb{Q}(\sqrt{1111})=K_1\subset\mathbb{Q}(\sqrt{11+\sqrt{1111}})=K_2\subset\mathbb{Q}(\sqrt{111+\sqrt{11+\sqrt{1111}}})=K_3=K.$$

(a) Analyse all the field homomorphisms $\phi_1\colon K_1\to\mathbb{R}$.
(b) For each such homomorphism, analyse the possible extensions $\phi_2\colon K_2\to\mathbb{R}$.
(c) For each such extensions, analyse the possible extensions $\phi_3\colon K_3\to\mathbb{R}$.
(d) Deduce the value of $|E_{\mathbb{Q}}(K,\mathbb{R})|$ (and observe that it is less than $[K:\mathbb{Q}]$, as we proved in lectures).
(e) Check in a similar way that $|E_{\mathbb{Q}}(K,\mathbb{C})|=[K:\mathbb{Q}]$.

Exercise 6.4. [`ex-dedekind-direct`]
Put $L=\mathbb{Q}(\sqrt{p},\sqrt{q})$ where p and q are distinct primes. There are homomorphisms $\theta_0,\dots,\theta_3\colon L\to L$ given by

$$\begin{array}{llll}\theta_0(\sqrt{p})=\sqrt{p} & \theta_1(\sqrt{p})=\sqrt{p} & \theta_2(\sqrt{p})=-\sqrt{p} & \theta_3(\sqrt{p})=-\sqrt{p}\\ \theta_0(\sqrt{q})=\sqrt{q} & \theta_1(\sqrt{q})=-\sqrt{q} & \theta_2(\sqrt{q})=\sqrt{q} & \theta_3(\sqrt{q})=-\sqrt{q}\end{array}$$

Dedekind's Lemma tells us that if $b_0,\dots,b_3\in L$ with $\sum_i b_i\theta_i=0$ then we must have $b_0=b_1=b_2=b_3=0$. Give a more direct proof of this fact.

Exercise 6.5. [`ex-basis-misc-i`]
Put $\alpha=2^{1/4}\in\mathbb{R}$ and $K=\mathbb{Q}(\alpha,i)\subseteq\mathbb{C}$. Then K is spanned over $\mathbb{Q}(i)$ by $1,\alpha,\alpha^2,\alpha^3$, but it is not completely clear that these are linearly independent. We can check this and prove some other facts as follows.
(a) Prove that $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$.
(b) Prove that $[K:\mathbb{Q}(\alpha)]=2$, and that $[\mathbb{Q}(i):\mathbb{Q}]=2$.
(c) Deduce that $[K:\mathbb{Q}(i)]=4$.
(d) Prove that K is normal over $\mathbb{Q}(i)$, and that $G(K/\mathbb{Q}(i))$ is cyclic of order 4.

Exercise 6.6. [`ex-which-normal-cyclic`]
Which of the following extensions are normal? When they are normal, say whether the Galois groups are cyclic or not.
(a) $K=\mathbb{Q}$, $L=K(e^{2\pi i/5})$
(b) $K=\mathbb{Q}(e^{2\pi i/5})$, $L=\mathbb{Q}(e^{2\pi i/25})$
(c) $K=\mathbb{Q}$, $L=K(\sqrt[5]{12})$
(d) $K=\mathbb{Q}(e^{2\pi i/5})$, $L=K(\sqrt[5]{3})$

7. Some extensions of small degree

Proposition 7.1. [`prop-quadratic`]
Let K be a field of characteristic not equal to two, and let L be an extension of K of degree two.
(a) *There is an element $\alpha\in L\setminus K$ such that $L=K(\alpha)$ and $\alpha^2\in K$.*
(b) *The element α has the following uniqueness property: if $L=K(\beta)$ for some other element $\beta\in L\setminus K$ with $\beta^2\in K$, then $\beta=q\alpha$ for some $q\in K$.*
(c) *There is an automorphism $\sigma\colon L\to L$ that acts as the identity on K and satisfies $\sigma(\alpha)=-\alpha$.*

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

Proof. First choose any element $\lambda \in L \setminus K$. We claim that 1 and λ are linearly independent over K. To see this, consider a linear relation $a.1 + b\lambda = 0$ with $a, b \in K$. If $b \neq 0$ we can rearrange to get $\lambda = -ab^{-1} \in K$, contrary to assumption. We therefore have $b = 0$ so the original relation reduces to $a = 0$ as required. As $\dim_K(L) = 2$ this means that $1, \lambda$ is a basis for L over K. We can therefore write $-\lambda^2$ in terms of this basis, say as $-\lambda^2 = b\lambda + c$, or equivalently $\lambda^2 + b\lambda + c = 0$. Next, as K does not have characteristic two we know that 2 is invertible in K so we can put $\alpha = \lambda - b/2 \in L$ and $a = b^2/4 - c \in K$. We find that $\alpha^2 = \lambda^2 - b\lambda + b^2/4 = b^2/4 - c = a$. By the same logic as for λ we also see that $1, \alpha$ is a basis for L and so $L = K(\alpha)$, proving (a).

Now suppose we have another element $\beta \in L \setminus K$ with $\beta^2 \in K$. We can write $\beta = p + q\alpha$ for some $p, q \in K$. As $\beta \notin K$ we have $q \neq 0$. This gives $\beta^2 = (p^2 + q^2 a) + 2pq\alpha$, which is assumed to lie in K, so we must have $2pq = 0$. As $q \neq 0$ and 2 is invertible this gives $p = 0$ and thus $\beta = q\alpha$, proving (b).

Next, as $1, \alpha$ is a basis, we can certainly define a K-linear map $\sigma\colon L \to L$ by $\sigma(x + y\alpha) = x - y\alpha$. This clearly satisfies $\sigma(\sigma(x + y\alpha)) = \sigma(x - y\alpha) = x + y\alpha$, so $\sigma^2 = 1$. It also has $\sigma(0) = 0$ and $\sigma(1) = 1$. Now consider elements $\mu = u + v\alpha$ and $\nu = x + y\alpha$ in L. We have

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

It follows that σ is an automorphism. Now let τ be any other automorphism of L with $\tau|_K = 1$. We can apply τ to the equation $\alpha^2 - a = 0$ to get $\tau(\alpha)^2 - a = 0$, or in other words $\tau(\alpha)^2 - \alpha^2 = 0$, or in other words $(\tau(\alpha) - \alpha)(\tau(\alpha) + \alpha) = 0$, so either $\tau(\alpha) = \alpha$ or $\tau(\alpha) = -\alpha$. In the first case we have $\tau = 1$, and in the second case we have $\tau = \sigma$. It follows that $G(L/K) = \{1, \sigma\}$ as claimed. □

Proposition 7.2. [prop-biquadratic]
Let p *and* q *be distinct prime numbers, put* $B = \{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\} \subset \mathbb{R}$, *and let* K *be the span of* B *over* $\mathbb{Q}$.

(a) *The set* B *is linearly independent over* $\mathbb{Q}$, *so it gives a basis for* K, *and* $[K : \mathbb{Q}] = 4$.
(b) K *is a splitting field for the polynomial* $(x^2 - p)(x^2 - q) \in \mathbb{Q}[x]$.
(c) *There are automorphisms* σ *and* τ *of* K *given by*

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

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

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

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

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

$$\begin{aligned} wx &= yzq \\ w^2 + px^2 &= (y^2 + pz^2)q. \end{aligned}$$

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

$$\begin{aligned} yz &= \overline{w}\overline{x}q \\ y^2 + pz^2 &= (\overline{w}^2 + p\overline{x}^2)q. \end{aligned}$$

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

For (b), the main point to check is that K is actually a subfield of $\mathbb{R}$. To see this, write $e_0 = 1$, $e_1 = \sqrt{p}$, $e_2 = \sqrt{q}$ and $e_3 = \sqrt{pq}$. By a straightforward check of the 16 possible cases, we see that e_ie_j is always a rational multiple of e_k for some k (for example $e_1e_3 = pe_2$). In particular, we have $e_ie_j \in K$. Now suppose we have two elements $x, y \in K$, say $x = \sum_{i=0}^{3} x_ie_i$ and $y = \sum_{j=0}^{3} y_je_j$. Then $xy = \sum_{i,j} x_iy_je_ie_j$ with $x_iy_j \in \mathbb{Q}$ and $e_ie_j \in K$, and K is a vector space over $\mathbb{Q}$, so $xy \in K$. We therefore see that K is a subring of $\mathbb{R}$. As K is finite-dimensional we can use Proposition 5.11 to see that K is a subfield of $\mathbb{R}$. It is clearly generated by the roots of the polynomial

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

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

Next, we can regard K as a degree two extension of $\mathbb{Q}(\sqrt{q})$ obtained by adjoining a square root of p. Proposition 7.1 therefore gives us an automorphism σ of K that acts as the identity on $\mathbb{Q}(\sqrt{q})$, and this is clearly described by the formula stated above. Similarly, we obtain the automorphism τ by regarding K as $\mathbb{Q}(\sqrt{p})(\sqrt{q})$ rather than $\mathbb{Q}(\sqrt{q})(\sqrt{p})$. This proves (c).

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

We next consider two different cubic equations for which the answers work out quite neatly. In Section 12 we will see that general cubics are conceptually not too different, although the formulae are typically less tidy.

Example 7.3. [`eg-nice-cubic`]
We will construct and study a splitting field for the polynomial $f(x) = x^3 - 3x - 3 \in \mathbb{Q}[x]$. This is an Eisentstein polynomial for the prime 3, so it is irreducible over $\mathbb{Q}$. We start by noting that $(3 + \sqrt{5})/2$ is a positive real number, with inverse $(3 - \sqrt{5})/2$. We let β denote the real cube root of $(3 + \sqrt{5})/2$, so that β^{-1} is the real cube root of $(3 - \sqrt{5})/2$. Then put $\omega = (\sqrt{-3} - 1)/2 \in \mathbb{C}$, so $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$. Finally, put $\alpha_i = \omega^i\beta + 1/(\omega^i\beta)$ for $i = 0, 1, 2$. We claim that these are roots of $f(x)$. Indeed, we have

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

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

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

We also claim that there is an automorphism ρ of K with $\rho(\alpha_0) = \alpha_1$ and $\rho(\alpha_1) = \alpha_2$ and $\rho(\alpha_2) = \alpha_0$. Indeed, part (c) of Proposition 6.17 tells us that there is an automorphism λ such that $\lambda(\alpha_0) = \alpha_1$. We know that λ permutes the set $R = \{\alpha_0, \alpha_1, \alpha_2\}$ of roots of $f(x)$, so it must either be the three-cycle $(\alpha_0\ \alpha_1\ \alpha_2)$ or the transposition $(\alpha_0\ \alpha_1)$. In the first case, we can just take $\rho = \lambda$; in the second, we can take $\rho = \lambda\sigma$. It is now easy to check that the set $\{1, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$ gives all six permutations of R. It follows by Proposition 6.17 that the Galois group $G(L/K)$ is the full group $\Sigma_R \simeq \Sigma_3$.

Example 7.4. [`eg-special-cubic`]
Consider the polynomial $f(x) = x^3 + x^2 - 2x - 1$. We first claim that this is irreducible over $\mathbb{Q}$. Indeed, if it were reducible we would have $f(x) = g(x)h(x)$ for some monic polynomials $g(x), h(x) \in \mathbb{Q}[x]$ with $\deg(g(x)) = 1$ and $\deg(h(x)) = 2$. Proposition 4.21 would then tell us that $g(x), h(x) \in \mathbb{Z}[x]$. This would

mean that $g(x) = x - a$ for some $a \in \mathbb{Z}$, and thus $f(a) = 0$. However, we have $f(2m) = 2(4m^3 + 2m^2 - m) - 1$ and $f(2m + 1) = 2(4m^3 + 8m^2 + 3m) - 1$ so $f(a)$ is odd for all $a \in \mathbb{Z}$, which is a contradiction.

Now put

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

We claim that α, β and γ are roots of $f(x)$. To see this, we start with the observation that $\zeta^7 = 1$, so $\zeta^4 = \zeta^{-3}$, so

$$(\zeta - 1)(\zeta^{-3} + \zeta^{-2} + \zeta^{-1} + 1 + \zeta + \zeta^2 + \zeta^3) = \zeta^4 - \zeta^{-3} = 0,$$

but $\zeta - 1 \neq 0$, so

$$\zeta^{-3} + \zeta^{-2} + \zeta^{-1} + 1 + \zeta + \zeta^2 + \zeta^3 = 0.$$

On the other hand,

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

If we add together the left hand sides we get $f(\alpha)$, and if we add together the right hand sides we get $\sum_{i=-3}^{3} \zeta^i = 0$, so $f(\alpha) = 0$. By essentially the same calculation we also have

$$f(\beta) = \sum_{i=-3}^{3} \zeta^{2i} = \zeta^{-6} + \zeta^{-4} + \zeta^{-2} + 1 + \zeta^2 + \zeta^4 + \zeta^6.$$

We can rewrite the right hand side using $\zeta^6 = \zeta^{-1}$ and $\zeta^4 = \zeta^{-3}$ (so $\zeta^{-6} = \zeta$ and $\zeta^{-4} = \zeta^3$). After reordering the terms we just get $\sum_{i=-3}^{3} \zeta^i$ again, which is zero. This shows that $f(\beta) = 0$, and similarly $f(\gamma) = 0$. This gives three distinct roots for the cubic polynomial $f(x)$, so we have

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

Next, we observe that

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

The first of these shows that $\beta \in Q(\alpha)$, and so $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$. We can also use the other equations to see that $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, so

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

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

Next, Proposition 6.17 tells us that there is an automorphism σ of $\mathbb{Q}(\alpha)$ with $\sigma(\alpha) = \beta$. Now σ is a homomorphism and $\beta = \alpha^2 - 2$ so

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

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

Example 7.5. [eg-cyclic-quartic]
Consider the polynomial $f(x) = x^4 - 10x^2 + 20$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion at the prime 5. This is a quadratic function of x^2, so by the usual formula it vanishes when $x^2 = (10 \pm \sqrt{100 - 4 \times 20})/2 = 5 \pm \sqrt{5}$ (and both of these values are positive real numbers). The roots of $f(x)$ are therefore α, β, $-\alpha$ and $-\beta$ where $\alpha = \sqrt{5 + \sqrt{5}}$ and $\beta = \sqrt{5 - \sqrt{5}}$. It is a special feature of this example

that β can be expressed in terms of α. To see this, note that $\alpha^2 = 5 + \sqrt{5}$ and so $\alpha^4 = 30 + 10\sqrt{5}$. Then put $\beta' = \frac{1}{2}\alpha^3 - 3\alpha$ and note that

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

This shows that $\alpha\beta' = \alpha\beta$, so $\beta = \beta' = \frac{1}{2}\alpha^3 - \alpha \in \mathbb{Q}(\alpha)$. This shows that all roots of $f(x)$ lie in $\mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$ over $\mathbb{Q}$. By Proposition 6.17 there is an automorphism σ of $\mathbb{Q}(\alpha)$ with $\sigma(\alpha) = \beta$. It follows that

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

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

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

Example 7.6. [eg-even-quartic]
Consider the polynomial $f(x) = x^4 - 6x^2 + 2 = (x^2 - 3 - \sqrt{7})(x^2 - 3 + \sqrt{7})$, which is irreducible over $\mathbb{Q}$, by Eisenstein's criterion at the prime 2. The roots are α, $-\alpha$, β and $-\beta$, where $\alpha = \sqrt{3 + \sqrt{7}}$ and $\beta = \sqrt{3 - \sqrt{7}}$. Let K be the splitting field, which is generated by α and β. Note that this contains the elements $\sqrt{7} = \alpha^2 - 3$ and $\sqrt{2} = \alpha\beta$. We can draw the set R of roots in a square as follows:

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

We claim that $G(L/\mathbb{Q})$ can be identified with the group D_8 of rotations and reflections of this square. Indeed, we can define a permutation $\mu = (\alpha\ -\alpha)(\beta\ -\beta) \in \Sigma_R$, and we put $H = \{\sigma \in \Sigma_R \mid \sigma\mu\sigma^{-1} = \mu\}$. One can see that H is a proper subgroup of Σ_R containing D_8, so $|H|$ is divisible by $|D_8| = 8$ and strictly less than $|\Sigma_R| = 24$, so $|H| = 8$ and $H = D_8$. Next, if $\sigma \in G(K/\mathbb{Q})$ then σ satisfies $\sigma(-a) = -\sigma(a)$ for all $a \in K$, so we have $\sigma\mu = \mu\sigma$, so $\sigma \in H = D_8$. It follows that $G(K/\mathbb{Q})$ is a subgroup of D_8 of order equal to $[K : \mathbb{Q}]$, so it will suffice to check that $[K : \mathbb{Q}] = 8$. As $f(x)$ is irreducible we certainly have $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x)) = 4$ and $K = \mathbb{Q}(\alpha)(\beta)$ with $\beta^2 = 3 - \sqrt{7} \in \mathbb{Q}(\sqrt{7}) \subseteq \mathbb{Q}(\alpha)$, so $[K : \mathbb{Q}(\alpha)]$ is either 1 (if $\beta \in \mathbb{Q}(\alpha)$) or 2 (if $\beta \notin \mathbb{Q}(\alpha)$). It would be an odd coincidence if β were already in $\mathbb{Q}(\alpha)$ and the reader may wish to take it on trust that this is not the case. However, for completeness we will give a proof below. Assuming this, we have $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ as required.

For the proof that $\beta \notin \mathbb{Q}(\alpha)$, we first observe that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4 > 2 = [\mathbb{Q}(\sqrt{7}) : \mathbb{Q}]$, so $\beta \notin \mathbb{Q}(\sqrt{7})$. Similarly, we have $\alpha \notin \mathbb{Q}(\sqrt{7})$. We also claim that $\beta/\alpha \notin \mathbb{Q}(\sqrt{7})$. Indeed, if it were we could multiply by $\alpha^2 = 3 + \sqrt{7} \in \mathbb{Q}(\sqrt{7})$ to see that $\sqrt{2} = \alpha\beta \in \mathbb{Q}(\sqrt{7})$, which would contradict the case $(p, q) = (2, 7)$ of Proposition 7.2. Now suppose (for a contradiction) that $\beta \in \mathbb{Q}(\alpha)$. We can then write $\beta = u + v\alpha$ for some $u, v \in \mathbb{Q}(\sqrt{7})$. As $\beta \notin \mathbb{Q}(\sqrt{7})$ we must have $v \neq 0$, and as $\beta/\alpha \notin \mathbb{Q}(\sqrt{7})$ we must have $u \neq 0$. We can now square the relation $\beta = u + v\alpha$ and rearrange to get $\alpha = (\beta^2 - u^2 - v^2\alpha^2)/(2uv)$. As $u, v, \alpha^2, \beta^2 \in \mathbb{Q}(\sqrt{7})$ this gives $\alpha \in \mathbb{Q}(\sqrt{7})$, which is the required contradiction.

For a randomly chosen polynomial of degree d, it will usually work out that the Galois group of the splitting field is the whole permutation group Σ_d. However, in any given case, it may not be so easy to verify this. We will now consider some examples where it is not too hard to verify this.

Lemma 7.7. [lem-all-perms]
Let p be a prime, and let G be a subgroup of Σ_p. Suppose that

(a) *G contains at least one transposition.*

(b) *For all $i, j \in \{1, \dots, n\}$ there exists $\sigma \in G$ with $\sigma(i) = j$. (In other words, G is transitive.)*
Then G is all of Σ_p.

Proof. Put $P = \{1, \dots, p\}$, and introduce a relation on P by $i \sim j$ if $i = j$ or $(i\ j) \in G$. It is clear that $i \sim i$, and that $i \sim j$ if and only if $j \sim i$. In other words, the relation is reflexive and symmetric. We claim that it is also transitive. To see this, suppose that $i \sim j$ and $j \sim k$. If either $i = j$ or $j = k$ it is immediate that $i \sim k$. Otherwise, we must have $(i\ j) \in G$ and $(j\ k) \in G$. As G is a subgroup it follows that $(j\ k)(i\ j)(j\ k) \in G$, but that composite is equal to $(i\ k)$, so we see that $i \sim k$ as required. This means that $\sim$ is an equivalence relation, so we can divide P into equivalence classes. Next, we claim that if $\sigma \in G$ and $i \sim j$ then $\sigma(i) \sim \sigma(j)$. Indeed, this is clear if $i = j$. Moreover, if $i \neq j$ we must have $(i\ j) \in G$, and it follows that $(\sigma(i)\ \sigma(j)) = \sigma(i\ j)\sigma^{-1} \in G$, so $\sigma(i) \sim \sigma(j)$ as claimed. We can also apply the same argument using σ^{-1} to deduce that converse implication, that if $\sigma(i) \sim \sigma(j)$ then $i \sim j$. Using this we see that the equivalence class of i has the same size as the equivalence class of $\sigma(i)$. By transitivity, for any $j \in P$ we can choose $\sigma \in G$ with $\sigma(i) = j$, and using this we see *all* the equivalence classes have the same size, say m. If there are n equivalence classes this means that $mn = p$. As G contains a transposition we see that there is at least one equivalence class of size larger than one, so $m > 1$. As p is prime we must thus have $m = p$ and $n = 1$. This means that the whole of P is a single equivalence class, so for all $i \neq j$ in P we have $(i\ j) \in G$. On the other hand, it is well known that every permutation can be written as a product of transpositions, so G is all of Σ_p as claimed. □

Corollary 7.8. [cor-all-perms]
Let p be a prime, and let $f(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$ that has precisely $p - 2$ real roots. Then the Galois group of the splitting field is all of Σ_p.

Proof. As $f(x)$ is irreducible it has no repeated roots, so there are precisely p distinct roots altogether. We can number them as $\alpha_1, \dots, \alpha_p$ with α_1 and α_2 being non-real and $\alpha_3, \dots, \alpha_p$ being real. We can take the complex conjugate of the equation $f(\alpha_1) = 0$ to see that $f(\overline{\alpha_1}) = 0$, so $\overline{\alpha_1}$ is a non-real root different from α_1, so it must be α_2. It follows from this that complex conjugation gives an automorphism of the splitting field $K = \mathbb{Q}(\alpha_1, \dots, \alpha_p)$, which exchanges α_1 and α_2, and fixes α_k for $k > 2$. This means that the Galois group G contains the transposition $(1\ 2)$, and it is transitive by Proposition 6.17(c). The claim now follows from Lemma 7.7. □

Example 7.9. [eg-generic-quintic]
Consider the quintic $f(x) = x^5 - 6x + 3$, which is irreducible by Eisenstein's criterion at the prime three. Using Maple or a graphing calculator we see that there are precisely three real roots, at approximately $x \simeq -1.67$, $x \simeq 0.51$ and $x \simeq 1.40$. For a more rigorous argument, we note that $f(-2) = -17 < 0$ and $f(0) = 3 > 0$ and $f(1) = -2 < 0$ and $f(2) = 23 > 0$, so the Intermediate Value Theorem tells us that there is at least one root between -2 and 0, and another between 0 and 1, and another between 1 and 2. Moreover, Rolle's theorem tells us that between any two roots of $f(x)$ there is at least one root of $f'(x) = 5x^4 - 6$, but $f'(x)$ has only two real roots (namely $x = \pm(6/5)^{1/4} \simeq \pm 1.0466$), so $f(x)$ can only have three real roots. This verifies the hypotheses of Corollary 7.8, so we see that the Galois group of the splitting field of $f(x)$ is all of Σ_5.

Exercises

Exercise 7.1. [ex-two-roots-basis]
Give a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. Express the element $1/(2 + \sqrt{2} + \sqrt{3})$ as a linear combination of your basis elements.

Exercise 7.2. [ex-three-five]
Show directly that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Exercise 7.3. [ex-biquadratic]
Let p and q be primes with $p < q$. You may assume (as shown in the notes) that the list $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$ is

linearly independent over $\mathbb{Q}$. Put

$$\begin{aligned} f(x) &= x^4 - 2(p+q)x^2 + (p-q)^2 \\ g(x) &= x^4 - (p+q)x^2 + pq. \end{aligned}$$

Show that $f(x)$ is the minimal polynomial of $\sqrt{p} + \sqrt{q}$ over $\mathbb{Q}$ (so in particular it is irreducible). Find all the roots of $f(x)$. Show that $g(x)$ is reducible, and has the same splitting field as $f(x)$.

Exercise 7.4. [`ex-galois-i`]
Put $L = \mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})$. Prove that this is normal over $\mathbb{Q}$, and describe the group $G(L/\mathbb{Q})$.

Exercise 7.5. [`ex-galois-ii`]
Find all automorphisms of the field $L = \mathbb{Q}(\sqrt[3]{3}, i)$. Deduce that L is normal over $\mathbb{Q}(\sqrt[3]{3})$, but not over $\mathbb{Q}$.

Exercise 7.6. [`ex-galois-iii`]
Put $L = \mathbb{Q}(\sqrt[4]{3}, i)$. Find all the automorphisms of L, and show that L is normal over $\mathbb{Q}$.

Exercise 7.7. [`ex-galois-iv`]
Consider the polynomial $f(x) = x^4 + x^2 + 4$. This is irreducible over $\mathbb{Q}$; you can either prove that, or just assume it and continue with the rest of the question. Put

$$\alpha = \sqrt{-\frac{1}{2} + \frac{1}{2}\sqrt{-15}}.$$

(a) Show that the roots of $f(x)$ are $\pm\alpha$ and $\pm\frac{2}{\alpha}$, so $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$.
(b) Compute $G(\mathbb{Q}(\alpha)/\mathbb{Q})$. What well-known group is it?

Exercise 7.8. [`ex-galois-v`]
Put $f(x) = x^4 + 8x^2 - 2 \in \mathbb{Q}[x]$, and $\alpha = \sqrt{3\sqrt{2} - 4}$, and $M = \mathbb{Q}(\alpha, \sqrt{-2})$.
(a) Show that $f(x)$ is irreducible over $\mathbb{Q}$.
(b) Show that $f(x)$ has roots $\pm\alpha, \pm\sqrt{-2}/\alpha$, so that M is a splitting field for $f(x)$.
(c) Show that $\mathbb{Q}(\alpha) = M \cap \mathbb{R} \neq M$, and deduce that $[M : \mathbb{Q}] = 8$.
(d) Show that there exist automorphisms $\phi, \psi \in G(M/\mathbb{Q})$ such that ϕ has order 4, ψ has order 2, and $G(M/\mathbb{Q}) = \langle \phi, \psi \rangle$.
(e) Write $\psi\phi\psi^{-1}$ in the form $\phi^i\psi^j$. To what well-known group is $G(M/\mathbb{Q})$ isomorphic?

8. Cyclotomic extensions

Definition 8.1. [`defn-cyclotomic`]
For any $n > 0$ we put

$$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\exp(2\pi i k/n) \mid k = 0, 1, \ldots, n-1\}.$$

If $z \in \mu_n$ for some n, then the *order* of z is the smallest $d > 0$ for which $z^d = 1$; this is a divisor of n. We write $\mu_n^\times$ for the subset of μ_n consisting of numbers of order precisely d. We also define

$$\varphi_n(t) = \prod_{z \in \mu_n^\times} (t - z) \in \mathbb{C}[t],$$

and call this the *n'th cyclotomic polynomial.* We write $\mathbb{Q}(\mu_n)$ for the subfield of $\mathbb{C}$ generated by $\mu_n^\times$, and call this the *n'th cyclotomic field.* This is evidently a splitting field for $\varphi_n(t)$.

Remark 8.2. [rem-cyclotomic]
If $\xi = \exp(2\pi ik/n) \in \mu_n$, then $\xi = \zeta_1^k$, where $\zeta_1 = \exp(2\pi i/n) \in \mu_n^\times$. By definition we have $\zeta_1 \in \mathbb{Q}(\mu_n)$ and $\mathbb{Q}(\mu_n)$ is a subfield so it is closed under multiplication, so $\zeta_1^k = \xi \in \mathbb{Q}(\mu_n)$. This shows that $\mathbb{Q}(\mu_n)$ does indeed contain μ_n as suggested by the notation.

Proposition 8.3. [prop-cyclotomic-product]
The polynomial $\varphi_n(t)$ is actually in $\mathbb{Z}[t]$, and satisfies

$$t^n - 1 = \prod_{d|n} \varphi_d(t).$$

Proof. Firstly, for each divisor d of n, we note that $\mu_d^\times \subseteq \mu_d \subseteq \mu_n$. Every element $z \in \mu_n$ lies in precisely one of the sets $\mu_d^\times$, so we see that

$$\prod_{z\in\mu_n} (t-z) = \prod_{d|n} \prod_{z\in\mu_d^\times} (t-z) = \prod_{d|n} \varphi_d(t).$$

On the other hand, the elements of μ_n are precisely the roots of $x^n - 1$, and there are n of them, so we see from Proposition 4.29 that $t^n - 1 = \prod_{z\in\mu_n}(t-z) = \prod_{d|n} \varphi_d(t)$ as claimed.

We will now prove by induction that $\varphi_n(t) \in \mathbb{Z}[t]$ for all n. To start the induction, note that $\mu_1^\times = \{1\}$ so $\varphi_1(t) = t - 1 \in \mathbb{Z}[t]$. Now suppose that $\varphi_d(t) \in \mathbb{Z}[t]$ for all $d < n$. Let $f(t)$ be the product of all the polynomials $\varphi_d(t)$ where $d|n$ and $d < n$. From the above we then see that $t^n - 1 = f(t)\varphi_n(t)$. Moreover, the induction hypothesis implies that $f(t) \in \mathbb{Z}[t] \subseteq \mathbb{Q}[t]$, and it is visible that $t^n - 1 \in \mathbb{Z}[t] \subseteq \mathbb{Q}[t]$. We therefore see from Corollary 4.6 that $\varphi_n(t) \in \mathbb{Q}[t]$. As $f(t)$ and $\varphi_n(t)$ are monic and $f(t)\varphi_n(t) \in \mathbb{Z}[t]$ it then follows from Proposition 4.21 that $\varphi_n(t) \in \mathbb{Z}[t]$. □

Example 8.4. [eg-cyclotomic-p]
We claim that when p is prime we have $\varphi_p(t) = 1 + t + \cdots + t^{p-1}$. Indeed, as the only divisors of p are 1 and p, the proposition tells us that $t^p - 1 = \varphi_1(t)\varphi_p(t)$. It is clear from the definitions that $\varphi_1(t) = t - 1$, so $\varphi_p(t) = (t^p - 1)/(t-1)$, which is $1 + t + \cdots + t^{p-1}$ by the standard geometric progression formula.

Example 8.5. [eg-cyclotomic]
One can also check that

$$\begin{aligned}
\varphi_1(t) &= t - 1 \\
\varphi_2(t) &= t + 1 \\
\varphi_3(t) &= t^2 + t + 1 \\
\varphi_4(t) &= t^2 + 1 \\
\varphi_5(t) &= t^4 + t^3 + t^2 + t + 1 \\
\varphi_6(t) &= t^2 - t + 1 \\
\varphi_7(t) &= t^6 + t^5 + t^4 + t^3 + t^2 + t + 1 \\
\varphi_8(t) &= t^4 + 1 \\
\varphi_9(t) &= t^6 + t^3 + 1 \\
\varphi_{10}(t) &= t^4 - t^3 + t^2 - t + 1.
\end{aligned}$$

To see this, let $\psi_1(t), \dots, \psi_{10}(t)$ be the polynomials listed above, so the claim is that $\varphi_n(t) = \psi_n(t)$ for $n = 1, \dots, 10$. One can check directly that for these n we have $t^n - 1 = \prod_{d|n} \psi_d(t)$, and for all n we have $t^n - 1 = \prod_{d|n} \varphi_d(t)$. If we know that $\varphi_d(t) = \psi_d(t)$ for all $d < n$, one can easily deduce from this that $\varphi_n(t) = \psi_n(t)$. It therefore follows inductively that $\varphi_n(t) = \psi_n(t)$ for $n \leq 10$ as claimed.

To explain the case $n = 6$ in more detail, note that

$$\begin{aligned}
\psi_1(t)\psi_2(t)\psi_3(t)\psi_6(t) &= (t-1)(t+1)(t^2+t+1)(t^2-t+1) \\
&= (t^2-1)(t^4+t^2+1) = t^6 - 1.
\end{aligned}$$

On the other hand, Proposition 8.3 tells us that $\varphi_1(t)\varphi_2(t)\varphi_3(t)\varphi_6(t) = t^6 - 1$. It is clear that $\varphi_1(t) = t - 1 = \psi_1(t)$, and using Example 8.4 we see that $\varphi_2(t) = \psi_2(t)$ and $\varphi_3(t) = \psi_3(t)$. We can therefore cancel the factor $\varphi_1(t)\varphi_2(t)\varphi_3(t) = \psi_1(t)\psi_2(t)\psi_3(t)$ in the equation

$$\varphi_1(t)\varphi_2(t)\varphi_3(t)\varphi_4(t) = t^6 - 1 = \psi_1(t)\psi_2(t)\psi_3(t)\psi_4(t)$$

to see that $\varphi_4(t) = \psi_4(t)$ as claimed.

Proposition 8.6. [prop-phi-irreducible]
The polynomial $\varphi_n(t)$ is irreducible over $\mathbb{Q}$.

The proof will follow after some preliminary results.

Lemma 8.7. [lem-F-additive]
If p is prime then $(x+y)^p = x^p + y^p \pmod{p}$, and $n^p = n \pmod{p}$ for all $n \in \mathbb{Z}$.

Proof. First, we have the binomial expansion

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}.$$

It will therefore be enough to show that $\binom{p}{k} = 0 \pmod{p}$ for $0 < k < p$. From the definitions we have $k!(p-k)!\binom{p}{k} = p!$, which is divisible by p. This means that p must divide $k!$ or $(p-k)!$ or $\binom{p}{k}$. However, as $k < p$ and $k! = 1.2.3\cdots k$ we see that $k!$ is not divisible by p. Moreover, $(p-k)!$ is also not divisible by p, for the same reason. It follows that p must divide $\binom{p}{k}$, and we deduce that $(x+y)^p = x^p + y^p \pmod{p}$ as claimed.

Now suppose that $n^p = n \pmod{p}$. By taking $x = n$ and $y = 1$ in our previous congruence we obtain $(n+1)^p = n^p + 1^p = n + 1 \pmod{p}$. It follows by induction that $n^p = n \pmod{p}$ for all $n \in \mathbb{N}$. We also have $n^p + (-n)^p = (n + (-n))^p = 0^p = 0 \pmod{p}$, so $(-n)^p = -(n^p) = -n \pmod{p}$ for all $n \in \mathbb{N}$. It follows that $m^p = m \pmod{p}$ for all $m \in \mathbb{Z}$. □

Corollary 8.8. [cor-F-additive]
If $g(t) \in \mathbb{Z}[t]$ then $g(t^p) = g(t)^p \pmod{p}$.

Proof. We can write $g(t) = \sum_{i=0}^{d} a_i t^i$ with $a_i \in \mathbb{Z}$. The lemma tells us that the p'th power operation commutes with addition modulo p, so $g(t)^p = \sum_{i=0}^{d} a_i^p t^{ip} \pmod{p}$. The lemma also tells us that $a_i^p = a_i \pmod{p}$, so $g(t)^p = \sum_{i=0}^{d} a_i t^{ip} \pmod{p}$, and this is just the same as $g(t^p)$. □

Lemma 8.9. [lem-zeta-p]
Let ζ be an element of $\mu_n^{\times}$, and put $f(t) = \min(\zeta, \mathbb{Q})$. Let p be a prime that does not divide n. Then $f(\zeta^p) = 0$.

Proof. As ζ is a root of $t^n - 1$ we see that $f(t)$ divides $t^n - 1$, say $t^n - 1 = f(t)g(t)$ for some (necessarily monic) polynomial $g(t) \in \mathbb{Q}[t]$. We see from Proposition 4.21 that in fact $f(t), g(t) \in \mathbb{Z}[t]$.

Next, we can use the equation $\zeta^n = 1$ to see that $(\zeta^p)^n - 1 = 0$, or equivalently $f(\zeta^p)g(\zeta^p) = 0$. If we can show that $g(\zeta^p) \neq 0$ then we conclude that $f(\zeta^p) = 0$ as required.

We therefore assume that $g(\zeta^p) = 0$, and try to derive a contradiction. Note that $g(t^p)$ is a polynomial in $\mathbb{Z}[t]$ that is zero when $t = \zeta$. It therefore follows from the definition of $f(t) = \min(\zeta, \mathbb{Q})$ that $g(t^p)$ is divisible by $f(t)$, say $g(t^p) = f(t)h(t)$. We can again use Proposition 4.21 to see that $h(t) \in \mathbb{Z}[t]$.

We next need to work temporarily modulo p. For any polynomial $m(t) \in \mathbb{Z}[t]$, we will write $\overline{m}(t)$ for the image of $m(t)$ in $\mathbb{F}_p[t]$. The equation $g(t^p) = f(t)h(t)$ in conjunction with Corollary 8.8 tells us that $\overline{g}(t)^p = \overline{f}(t)\overline{h}(t)$. Now let $\overline{k}(t)$ be any monic irreducible factor of $\overline{f}(t)$ in $\mathbb{F}_p[t]$. We then see that $\overline{k}(t)$ divides $\overline{g}(t)^p$, so (by irreducibility) it must divide $\overline{g}(t)$. It follows that $\overline{k}(t)^2$ divides $\overline{f}(t)\overline{g}(t) = t^n - 1$, say $t^n - 1 = \overline{k}(t)^2\overline{m}(t)$ for some $\overline{m}(t) \in \mathbb{F}_p[t]$. We then take the algebraic derivative to see that

$$n\,t^{n-1} = 2\overline{k}(t)\overline{k}'(t)\overline{m}(t) + \overline{k}(t)^2\overline{m}'(t) = (2\overline{k}'(t)\overline{m}(t) + \overline{k}(t)\overline{m}'(t))\overline{k}(t)$$

so in particular $\overline{k}(t)$ divides $n\,t^{n-1}$. Note here that $n \neq 0$ in $\mathbb{F}_p$ (because we assumed that p does not divide n) and that $\overline{k}(t)$ was assumed to be monic and irreducible. It is clear from this that we must have $\overline{k}(t) = t$, so $\overline{k}(0) = 0$. We can thus put $t = 0$ in the equation $t^n - 1 = \overline{k}(t)^2\overline{m}(t)$ to get $-1 = 0 \pmod{p}$, which is the required contradiction. □

Corollary 8.10. [`cor-cyclotomic-roots`]
Let ζ be an element of $\mu_n^\times$, and put $f(t) = \min(\zeta, \mathbb{Q})$. Let k be any integer that is coprime to n. Then $f(t) = \min(\zeta^k, \mathbb{Q})$ (and so $f(\zeta^k) = 0$).

Proof. If k is prime, then the lemma tells us that $f(\zeta^k) = 0$. It follows that $\min(\zeta^k, \mathbb{Q})$ is a non-constant monic divisor of the irreducible polynomial $f(t)$, so it must just be equal to $f(t)$ as required.

Now suppose that $k = pq$ for some primes p and q (which cannot divide n, because k is coprime to n). By the prime case (applied to ζ and p) we see that $f(t) = \min(\zeta^p, \mathbb{Q})$. We can therefore apply the prime case again to ζ^p and q to see that $f(t) = \min(\zeta^{pq}, \mathbb{Q}) = \min(\zeta^k, \mathbb{Q})$. In general, if $k > 0$ and k is coprime to n then we can write $k = p_1p_2\cdots p_r$ for some primes $p_1, \ldots, p_r$ (not necessarily distinct) that do not divide n. We then see that $f(t) = \min(\zeta^k, \mathbb{Q})$ by an obvious extension of the argument for the case $k = pq$. Finally, if $k < 0$ and $(k, n) = 1$ then we can choose j such that the number $k' = k + jn$ is positive (and still coprime to n). We then see that $f(t) = \min(\zeta^{k'}, \mathbb{Q})$ but $\zeta^{k'} = (\zeta^n)^j\zeta^k = \zeta^k$ so $f(t) = \min(\zeta^k, \mathbb{Q})$ as claimed. □

Proof of Proposition 8.6. Put $\zeta = \exp(2\pi i/n) \in \mu_n^\times$, and $f(t) = \min(\zeta, \mathbb{Q})$. As $\varphi_n(\zeta) = 0$ we see that $f(t)$ divides $\varphi_n(t)$. On the other hand, the roots of $\varphi_n(t)$ are precisely the elements of $\mu_n^\times$, or in other words the powers ζ^k with $0 \leq k < n$ and $(k, n) = 1$. Corollary 8.10 tells us that these are also roots of $f(t)$, so $\varphi_n(t)$ divides $f(t)$ by Proposition 4.29. As $f(t)$ and $\varphi_n(t)$ are monic polynomials that divide each other, we must have $\varphi_n(t) = f(t)$. As $f(t)$ is irreducible by definition, we see that $\varphi_n(t)$ is irreducible as claimed. □

Proposition 8.11. [`prop-cyclotomic-galois`]
For each $k \in \mathbb{Z}$ that is coprime to n there is a unique automorphism σ_k of $\mathbb{Q}(\mu_n)$ such that $\sigma_k(\zeta) = \zeta^k$ for all $\zeta \in \mu_n$. Moreover, the rule $k + n\mathbb{Z} \mapsto \sigma_k$ gives an isomorphism of groups $(\mathbb{Z}/n\mathbb{Z})^\times \to G(\mathbb{Q}(\mu_n)/\mathbb{Q})$.

Proof. Put $\zeta_1 = \exp(2\pi i/n) \in \mu_n^\times$; we have seen that $\varphi_n(x) = \min(\zeta_1, \mathbb{Q})$. Now suppose we have $k \in \mathbb{Z}$ such that $(k, n) = 1$. Then $\zeta_1^k \in \mu_n^\times$, so $\varphi_n(\zeta_1) = 0$. It then follows from Proposition 6.17(c) that there is an automorphism $\sigma_k \in G(\mathbb{Q}(\mu_n)/\mathbb{Q})$ with $\sigma_k(\zeta_1) = \zeta_1^k$. Any other element $\zeta \in \mu_n$ has the form $\zeta = \zeta_1^m$ for some m, and as σ_k is a homomorphism we deduce that

$$\sigma_k(\zeta) = \sigma_k(\zeta_1^m) = \sigma_k(\zeta_1)^m = (\zeta_1^k)^m = (\zeta_1^m)^k = \zeta^k.$$

Next, part (b) of Proposition 6.17 tells us that any automorphism of $\mathbb{Q}(\mu_n)$ is determined by its effect on the set $\mu_n^\times$ of roots of $\varphi_n(t)$. It follows that σ_k is the *unique* automorphism such that $\sigma_k(\zeta) = \zeta^k$ for all $\zeta \in \mu_n$. In particular, if j is another element of $\mathbb{Z}$ that is coprime to n, we see that

$$\sigma_j(\sigma_k(\zeta)) = \sigma_j(\zeta^k) = \sigma_j(\zeta)^k = \zeta^{jk} = \sigma_{jk}(\zeta).$$

It therefore follows from the above uniqueness statement that $\sigma_j\sigma_k = \sigma_{jk}$. Similarly, if $j = k \pmod{n}$ then $\zeta^j = \zeta^k$ for all $\zeta \in \mu_n$ so σ_j and σ_k give the same permutation of roots, so $\sigma_j = \sigma_k$. We now see that there is a well-defined map $S\colon (\mathbb{Z}/n\mathbb{Z})^\times \to G(\mathbb{Q}(\mu_n)/\mathbb{Q})$ given by $S(k) = \sigma_k$. If σ_k is the identity then we must have $\zeta_1^k = \zeta_1$, so $\zeta_1^{k-1} = 1$, so $k = 1 \pmod{n}$. It follows that $\ker(S) = \{1\}$ and so S is injective. Finally, suppose that $\tau \in G(\mathbb{Q}(\mu_n)/\mathbb{Q})$. We then see that $\tau(\zeta_1)$ must be a root of $\varphi_n(t)$, and so $\tau(\zeta_1) = \zeta_1^k$ for some k that is coprime to n. Just as above we deduce that $\tau(\zeta) = \zeta^k$ for all $\zeta \in \mu_n$, and so $\tau = \sigma_k$. This proves that S is surjective and so is an isomorphism. □

We will state without proof the following result of Kronecker and Weber:

Theorem 8.12. [`thm-kronecker-weber`]
Let K be a subfield of $\mathbb{C}$ that is normal and of finite degree over $\mathbb{Q}$, such that $G(K/\mathbb{Q})$ is abelian. Then $K \subseteq \mathbb{Q}(\mu_n)$ for some n.

The proof uses ideas far beyond the scope of these notes. However, we will prove an interesting special case.

Proposition 8.13. [prop-root-p]
For any prime $p > 2$ we have $\sqrt{p} \in \mathbb{Q}(\mu_{4p})$. More precisely, if $\xi = \exp(\pi i/(2p))$ is the standard generator of μ_{4p} then

$$\sqrt{p} = \prod_{k=1}^{(p-1)/2} (\xi^{p-2k} - \xi^{p+2k}) = \xi^{(p-1)^2/4} \prod_{k=1}^{(p-1)/2} (1 - \xi^{4k}).$$

(Note here that $(p-1)/2$ and $(p-1)^2/4$ are integers, because p is odd.)

Example 8.14. [eg-five]
Before discussing the general case we will look at the example where $p = 5$. There we have $\xi = \exp(\pi i/10)$ and the claim is that

$$\sqrt{5} = (\xi^3 - \xi^7)(\xi - \xi^9) = \xi^4(1 - \xi^4)(1 - \xi^8).$$

Put

$$\begin{aligned} \lambda &= (\xi^3 - \xi^7)(\xi - \xi^9) \\ \mu &= \xi^4(1 - \xi^4)(1 - \xi^8), \end{aligned}$$

so the claim is that $\lambda = \mu = \sqrt{p}$. If we start with λ and extract a factor of ξ^3 from the first bracket and a factor of ξ from the second bracket then we end up with μ, so $\lambda = \mu$ as claimed. It will be convenient to rewrite μ in terms of $\zeta = \xi^4 = \exp(2\pi i/5)$, which is a primitive 5th root of unity. This satisfies

$$(1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4)(1 - \zeta) = 1 - \zeta^5 = 0$$

and $1 - \zeta \neq 0$ so we must have $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$.

Note that

$$\mu = \zeta(1 - \zeta)(1 - \zeta^2) = \zeta - \zeta^2 - \zeta^3 + \zeta^4.$$

If we square this and collect terms in the most obvious way, we get

$$\begin{aligned} \mu^2 &= \zeta^2 + \zeta^4 + \zeta^6 + \zeta^8 - 2\zeta^3 - 2\zeta^4 + 2\zeta^5 + 2\zeta^5 - 2\zeta^6 - 2\zeta^7 \\ &= \zeta^2 - 2\zeta^3 - \zeta^4 + 4\zeta^5 - \zeta^6 - 2\zeta^7 + \zeta^8. \end{aligned}$$

If we now use the identity $\zeta^5 = 1$ (so $\zeta^6 = \zeta$ and so on) we get

$$\begin{aligned} \mu^2 &= \zeta^2 - 2\zeta^3 - \zeta^4 + 4 - \zeta - 2\zeta^2 + \zeta^3 \\ &= 4 - \zeta - \zeta^2 - \zeta^3 - \zeta^4. \end{aligned}$$

Finally, we can combine this with the identity $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$ to get $\mu^2 = 5$, so $\mu = \pm\sqrt{5}$. It is not hard to check that the factors $\xi^3 - \xi^7$ and $\xi - \xi^9$ are positive real numbers, so $\mu > 0$, so $\mu = \sqrt{5}$; we will explain this in more detail when we discuss the general case.

Lemma 8.15. [lem-root-p-xi]
With p and ξ as above we have $\prod_{k=1}^{p-1}(1 - \xi^{4k}) = p$.

Proof. The powers ξ^{4k} for $k = 0, \dots, p-1$ are precisely the p'th roots of unity, so we have

$$t^p - 1 = \prod_{k=0}^{p-1} (t - \xi^{4k}).$$

The $k = 0$ term on the right hand side is just $t - 1$. We can move this to the left hand side and use the standard geometric progression formula to get

$$1 + t + \cdots + t^{p-1} = \frac{t^p - 1}{t - 1} = \prod_{k=1}^{p-1} (t - \xi^{4k}).$$

Now set $t = 1$. On the left hand side we have p terms which all become 1, and on the right we have $\prod_{k=1}^{p-1}(1 - \xi^{4k})$ so $\prod_{k=1}^{p-1}(1 - \xi^{4k}) = p$ as claimed. □

Corollary 8.16. [cor-norm]
We have $|\prod_{k=1}^{(p-1)/2}(1 - \xi^{4k})| = \sqrt{p}$.

Proof. Put $\kappa = \prod_{k=1}^{(p-1)/2}(1-\xi^{4k})$. We then have $\overline{\kappa} = \prod_{k=1}^{(p-1)/2}(1-\xi^{-4k})$, and $\xi^{4p}=1$ so we can rewrite ξ^{-4k} as ξ^{4p-4k} or as $\xi^{4(p-k)}$. Now, as k runs from 1 to $(p-1)/2$ we find that $p-k$ runs through the numbers from $(p+1)/2$ to $p-1$ (in reverse order), so the numbers k and $p-k$ together cover all the numbers from 1 to $p-1$ (each number exactly once). Thus

$$\kappa\overline{\kappa} = \prod_{k=1}^{(p-1)/2}(1-\xi^{4k})\prod_{k=1}^{(p-1)/2}(1-\xi^{4(p-k)}) = \prod_{j=1}^{p-1}(1-\xi^{4j}) = p.$$

(The last step here is just the previous lemma.) On the other hand, we have $\kappa\overline{\kappa} = |\kappa|^2$, so $|\kappa| = \sqrt{p}$ as claimed. □

Proof of Proposition 8.13. Put

$$\lambda = \prod_{k=1}^{(p-1)/2}(\xi^{p-2k} - \xi^{p+2k})$$
$$\mu = \xi^{(p-1)^2/4}\prod_{k=1}^{(p-1)/2}(1-\xi^{4k}),$$

so the claim is that $\lambda = \mu = \sqrt{p}$. First, combine Corollary 8.16 with the fact that $|\xi|=1$ to get

$$|\mu| = |\xi|^{(p-1)^2/4}\left|\prod_{k=1}^{(p-1)/2}(1-\xi^{4k})\right| = 1^{(p-1)^2/4}\sqrt{p} = \sqrt{p}.$$

Next, note that

$$\xi^{p-2k}(1-\xi^{4k}) = \xi^{p-2k} - \xi^{p+2k}.$$

Take the product for $k=1,\dots,(p-1)/2$ to get

$$\xi^N\prod_{k=1}^{(p-1)/2}(1-\xi^{4k}) = \lambda,$$

where $N = \sum_{k=1}^{(p-1)/2}(p-2k)$. This is the sum of $(p-1)/2$ equally spaced terms from $p-2$ down to 1, so the average term is $\frac{1}{2}((p-2)+1) = (p-1)/2$ and the total is the number of terms times the average, which gives $N = (p-1)^2/4$. Given this, the displayed equation tells us that $\mu = \lambda$, so $|\lambda| = |\mu| = \sqrt{p}$.

Next, note that $\xi^p = i$ and

$$\xi^{2k} = \exp(k\pi i/p) = \cos(k\pi/p) + i\sin(k\pi/p)$$
$$\xi^{-2k} = \exp(-k\pi i/p) = \cos(k\pi/p) - i\sin(k\pi/p)$$

so

$$\xi^{p-2k} - \xi^{p+2k} = i(\cos(k\pi/p) - i\sin(k\pi/p)) - i(\cos(k\pi/p) + i\sin(k\pi/p)) = 2\sin(k\pi/p).$$

Moreover, when $1 \le k \le (p-1)/2$ we have $0 < k\pi/p < \pi/2$ so $\sin(k\pi/p) > 0$. It follows that λ is a positive real number, so $\lambda = |\lambda| = \sqrt{p}$. □

Corollary 8.17. [cor-mquad-cyclotomic]
For any field of the form $K = \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_m})$ (where the p_i are odd primes) there exists N such that $K \subseteq \mathbb{Q}(\mu_N)$.

Proof. Put $N = 4\prod_i p_i$. For each i we see that $4p_i$ divides N and so $\sqrt{p_i} \in \mathbb{Q}(\mu_{4p_i}) \subseteq \mathbb{Q}(\mu_N)$. It follows that $K \subseteq \mathbb{Q}(\mu_N)$ as claimed. □

Exercises

Exercise 8.1. [ex-cyclotomic-twenty]
Find the cyclotomic polynomial $\varphi_{20}(x)$.

Exercise 8.2. [ex-phi-CC]
What is $\varphi_{200}(x)$?

Exercise 8.3. [ex-mu-seven]
Explicitly compute a polynomial $f(t) \in \mathbb{Q}[t]$ of degree six with $e^{3\pi i/7}+1$ as a root. Prove that this polynomial is irreducible over $\mathbb{Q}$, using Eisenstein's criterion.

Exercise 8.4. [ex-mu-fifteen]
Describe the automorphisms of $\mathbb{Q}(\mu_{15})$. Find two cyclic subgroups A and B such that $G(\mathbb{Q}(\mu_{15})/\mathbb{Q}) = A \times B$.

Exercise 8.5. [ex-cyclotomic-real]
Let ζ be a primitive nth root of unity, where $n \geq 3$, and write $\beta = \zeta + \zeta^{-1}$.

(a) Show that ζ satisfies a quadratic equation over $\mathbb{Q}(\beta)$ and deduce that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\beta)] \leq 2$.
(b) Show that $\mathbb{Q}(\beta) \subset \mathbb{R}$, and deduce that $\zeta \notin \mathbb{Q}(\beta)$. Deduce that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\beta)] = 2$.
(c) Prove by induction that for all m, $\zeta^m + \zeta^{-m} \in \mathbb{Q}(\beta)$.
(d) Express $\zeta^5 + \zeta^{-5}$ as a polynomial in β.

[*Hint for (c) and (d): if* $\zeta^m + \zeta^{-m} = p_m(\beta)$, *show that* $\zeta^{m+1} + \zeta^{-m-1} = \beta p_m(\beta) - p_{m-1}(\beta)$.]

Exercise 8.6. [ex-shift-irr]
Show that if $f(t) \in K[t]$ and $a \in K$ and the polynomial $g(t) = f(t+a)$ is irreducible, then $f(t)$ itself is also irreducible. Apply this together with Eisenstein's criterion to give an alternative proof that $\varphi_p(t)$ is irreducible (for any prime p).

Exercise 8.7. [ex-phi-two-power]
Prove that $\varphi_{2^{k+1}}(t) = t^{2^k} + 1$.

Exercise 8.8. [ex-phi-families]

(a) Prove that ζ is a primitive mth root of unity if and only if $\overline{\zeta}$ is a primitive mth root of unity. Deduce that if $m > 2$ then $\varphi_n(x)$ has even degree.
(b) Let $n \geq 6$ be even, but not divisible by 4. Prove that ζ is a primitive nth root of 1 if and only if $-\zeta$ is a primitive $(n/2)$th root of 1. Deduce that $\varphi_n(x) = \varphi_{n/2}(-x)$.
(c) Suppose that n is divisible by p^2 for some prime p. Show that ζ is a primitive nth root of 1 if and only if ζ^p is a primitive (n/p)th root of 1. Deduce that $\varphi_n(x) = \varphi_{n/p}(x^p)$.
(d) Recall that $\varphi_1(x) = x-1$, and that $\varphi_p(x) = 1+x+\cdots+x^{p-1}$ when p is prime. How many cyclotomic polynomials can you calculate using these facts together with (b) and (c)?
(e) For small n one observes that all coefficients in $\varphi_n(x)$ are 0, 1 or -1, but this pattern does not persist for ever. Let N be the smallest number such that $\varphi_N(x)$ has a coefficient not in $\{0, 1, -1\}$. What do (b) and (c) tell you about N?
(f) Use (e) to find N, with help from Maple if necessary. (Start by entering `with(numtheory):`; then you can use the notation `cyclotomic(n,x)` for $\varphi_n(x)$.)

Exercise 8.9. [ex-phi-pq]
Let p and q be distinct odd primes, and consider the power series

$$f(x) = \sum_{i=0}^{q-1}\sum_{j=0}^{p-1}\sum_{k=0}^{\infty}(x^{ip+jq+kpq} - x^{1+ip+jq+kpq}).$$

Prove that $f(x) = \varphi_{pq}(x)$ (so in particular, enough terms must cancel to make $f(x)$ a polynomial).

Exercise 8.10. [ex-fifth-root]
Let ζ be a primitive 5th root of unity, and let α denote the real 5th root of 2. You are given that $\mathbb{Q}(\zeta,\alpha)$ is the splitting field of x^5-2 over $\mathbb{Q}$ and that $[\mathbb{Q}(\zeta,\alpha):\mathbb{Q}]=20$.

- Specify the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta,\alpha)/\mathbb{Q})$ by writing down how they act on ζ and on α.
- Show that there exist automorphisms ϕ, $\psi\in\mathrm{Gal}(\mathbb{Q}(\zeta,\alpha)/\mathbb{Q})$ such that ϕ has order 4, ψ has order 5, and $\mathrm{Gal}(\mathbb{Q}(\zeta,\alpha)/\mathbb{Q})=\langle\phi,\psi\rangle$.
- Write $\phi\psi\phi^{-1}$ in the form $\phi^i\psi^j$.
- Recall that if $\beta=\zeta+\frac{1}{\zeta}$, then $\mathbb{Q}(\beta)=\mathbb{Q}(\sqrt{5})$. Under the Galois correspondence, what should be the order of the corresponding subgroup $\mathrm{Gal}(\mathbb{Q}(\zeta,\alpha)/\mathbb{Q}(\beta))$?
- Show that the group $\mathrm{Gal}(\mathbb{Q}(\zeta,\alpha)/\mathbb{Q}(\beta))$ is $\langle\phi^2,\psi\rangle$.

Exercise 8.11. [ex-forty-two]
Let L be the splitting field of x^7-3 over $\mathbb{Q}$. You know that $[L:\mathbb{Q}]=42$. Calculate the elements of $\mathrm{Gal}(L/\mathbb{Q})$. Find ψ, $\phi\in\mathrm{Gal}(L/\mathbb{Q})$ which satisfy:

- ψ has order 7, ϕ has order 6
- $\phi\psi\phi^{-1}=\psi^3$
- $\mathrm{Gal}(L/\mathbb{Q})=\langle\phi,\psi\rangle$

9. Finite fields

We now divert temporarily from our main focus on fields of characteristic zero, and instead discuss finite fields. It turns out that the relevant theory is quite closely related to that of cyclotomic fields.

Theorem 9.1. [thm-finite-fields]

(a) *There is a finite field of order n if and only if $n=p^r$ for some prime p and $r>0$.*
(b) *If K is a field of order p^r then K has characteristic p, and $K^\times\simeq C_{p^r-1}$. Moreover, the function $\sigma(a)=a^p$ defines an automorphism of K, called the* Frobenius automorphism*.*
(c) *If K and L are fields of the same order then they are isomorphic.*
(d) *If $|L|=p^{rs}$ then the set $K=\{a\in L\mid a^{p^r}=a\}$ is a subfield of L, and is the unique subfield of order p^r. Moreover, this procedure gives all the subfields of L.*
(e) *If K and L are as above, then L is normal over K, and $G(L/K)$ is cyclic of order s, generated by σ^r.*

The proof will be given at the end of this section; it will consist of collecting together a number of smaller results that we will prove separately.

We first discuss a few examples.

Example 9.2. [eg-finite-misc]
We have already seen the fields $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ for p prime, and Example 1.11 exhibited a field $\mathbb{F}_4$ of order four. Now suppose that $p>2$, and consider the ring $\mathbb{F}_p[i]$ of "mod p complex numbers", as discussed in Exercise 1.2. The elements of $\mathbb{F}_p[i]$ have the form $a+bi$, with $a,b\in\mathbb{F}_p$, and the multiplication rule is

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

We saw in Exercise 1.2 that $\mathbb{F}_3[i]$ is a field (of order 9) but that $\mathbb{F}_2[i]$ and $\mathbb{F}_5[i]$ are not fields. More generally, we will see in Proposition 9.14 that $\mathbb{F}_p[i]$ is a field (of order p^2) if and only if $p=3 \pmod 4$.

Lemma 9.3. [lem-finite-field-order]
Let K be a finite field. Then K has characteristic $p>0$ for some prime p, and $|K|=p^r$ for some $r>0$.

Proof. As K is finite, the elements $n.1$ (for $n\in\mathbb{N}$) cannot all be different. It follows that there exist integers $n<m$ with $n.1=m.1$, so $(m-n).1=0$. It follows (see Definition 1.9) that $\mathrm{char}(K)>0$, and so $\mathrm{char}(K)$ is a prime p by Proposition 1.10. It therefore follows from Proposition 1.32 that K contains a copy of $\mathbb{F}_p$. Note that the whole of K is certainly a finite spanning set for K over $\mathbb{F}_p$, so K is finite-dimensional over $\mathbb{F}_p$, with dimension r say. This means that $K \simeq \mathbb{F}_p^r$ and so $|K| = p^r$. As $1 \neq 0$ in K (by one of the field axioms) we have $|K| > 1$ and so $r > 0$. □

Lemma 9.4. [prop-frobenius-exists]
Let K be a finite field of order p^r. Then the function $\sigma(a) = a^p$ defines an automorphism of K.

Proof. It is clear that $\sigma(0) = 0$ and $\sigma(1) = 1$ and $\sigma(ab) = \sigma(a)\sigma(b)$. We also see from Lemma 8.7 that $\sigma(a + b) = \sigma(a) + \sigma(b)$. This means that σ is a homomorphism from K to K. Now suppose that $K = \{a_1, \dots, a_{p^r}\}$. We see from Proposition 1.29 that σ is injective, so the p^r elements $\sigma(a_1), \dots, \sigma(a_{p^r})$ are all different, so between them they must cover all the p^r elements of K. This means that σ is also surjective, so it is an isomorphism as required. □

Remark 9.5. [rem-frobenius-powers]
We observe that

$$\begin{aligned}
\sigma(a) &= a^p \\
\sigma^2(a) &= \sigma(\sigma(a)) = (a^p)^p = a^{p\times p} = a^{p^2} \\
\sigma^3(a) &= \sigma(\sigma^2(a)) = (a^{p^2})^p = a^{p^2\times p} = a^{p^3} \\
\sigma^4(a) &= \sigma(\sigma^3(a)) = (a^{p^3})^p = a^{p^3\times p} = a^{p^4}
\end{aligned}$$

and so on; in general, $\sigma^r(a) = a^{p^r}$.

Lemma 9.6. [lem-cyclotomic-coprime]
Suppose that p is prime and $r > 0$ and put $q = p^r$. If $f(x), g(x) \in \mathbb{F}_p[x]$ and $x^q - x$ is divisible by $f(x)g(x)$, then $f(x)$ and $g(x)$ are coprime.

Proof. We have $x - x^q = f(x)g(x)h(x)$ for some h. Taking derivatives gives

$$1 - qx^{q-1} = f'(x)g(x)h(x) + f(x)g'(x)h(x) + f(x)g(x)h'(x).$$

The left hand side is just 1, because we are working mod p. We can rewrite the right hand side in terms of the polynomials $a(x) = g'(x)h(x) + g(x)h'(x)$ and $b(x) = f'(x)h(x)$ to get

$$1 = a(x)f(x) + b(x)g(x),$$

showing that $f(x)$ and $g(x)$ are coprime. □

Lemma 9.7. [lem-Fq-exists]
Suppose again that p is prime and $r > 0$ and $q = p^r$. Let $f(x) \in \mathbb{F}_p[x]$ be an irreducible factor of the mod p reduction of $\varphi_{q-1}(x)$, and put $K = \mathbb{F}_p[x]/f(x)$. Then K is a field with $|K| = q$, and $K^\times$ is cyclic of order $q - 1$.

Proof. We write α for the image of x in K, so $f(\alpha) = 0$. As $f(x)$ is irreducible, we see from Corollary 4.25 that K is a field and $K = \mathbb{F}_p(\alpha)$. If $f(x)$ has degree s we also see from Proposition 5.2 that $K \simeq \mathbb{F}_p^s$ as vector spaces over $\mathbb{F}_p$, so in particular $|K| = p^s$. As $f(x) \mid \varphi_{q-1}(x) \mid x^{q-1} - 1 \mid x^q - x$, we see that $\alpha^q = \alpha$. Here $q = p^r$ and so one checks that $\sigma^r(t) = t^{p^r} = t^q$, so we see that $\sigma^r(\alpha) = \alpha$. Now put $K' = \{a \in K \mid \sigma^r(a) = a\}$. We see from Proposition 1.31 that K' is a subfield of $K = \mathbb{F}_p(\alpha)$, and it contains α so it must be all of K. This means that every element in K is a root of the polynomial $g(x) = x^q - x$. However, $g(x)$ has degree q and so cannot have more than q roots in any field. We must therefore have $|K| \leq q$.

We next consider the order of α in $K^\times$. As explained above we have $f(x) \mid x^{q-1} - 1$ and so $\alpha^{q-1} = 1$, so the order of α divides $q - 1$. Write r for this order, and suppose (for a contradiction) that $r < q - 1$. It then follows from Proposition 8.3 that $x^{q-1} - 1$ is divisible by $(x^r - 1)f(x)$, so Lemma 9.6 tells us that $x^r - 1$ and $f(x)$ are coprime mod p. This means that there exist polynomials $a(x), b(x) \in \mathbb{F}_p[x]$ with $a(x)(x^r - 1) + b(x)f(x) = 1$. We now put $x = \alpha$, remembering that $f(\alpha) = 0 = \alpha^r - 1$, to get $0 = 1$, which is impossible. We must therefore have $r = q - 1$ instead, so the subgroup of $K^\times$ generated by α is isomorphic to C_{q-1}. On the other hand, we have shown that $|K| \leq q$ so $|K^\times| \leq q - 1$. This can only be consistent if $K^\times = \langle\alpha\rangle \simeq C_{q-1}$ as claimed. □

Example 9.8. [`eg-F-eight`]
Put $f(t) = 1 + t + t^3$ and $g(t) = 1 + t^2 + t^3$, considered as elements of $\mathbb{F}_2[t]$. By direct expansion and Example 8.4 we see that

$$f(t)g(t) = 1 + t + t^2 + t^3 + t^4 + t^5 + t^6 = \varphi_7(t) \text{ in } \mathbb{F}_2[t].$$

We also claim that $f(t)$ is irreducible over $\mathbb{F}_2$. Indeed, any nontrivial factorisation of $f(t)$ would involve a factor of degree one, which would give a root of $f(t)$ in $\mathbb{F}_2 = \{0, 1\}$. However, we have $f(0) = f(1) = 1$ so there is no such root. By the same argument we see that $g(t)$ is also irreducible. It follows that there are fields $K = \mathbb{F}_2[\alpha]/f(\alpha)$ and $L = \mathbb{F}_2[\beta]/g(\beta)$ of order 8.

We next claim that in K we have $g(\alpha^3) = 0$. Indeed, by construction we have $f(\alpha) = 0$, and $f(t)$ divides $t^7 - 1$, so $\alpha^7 = 1$, which implies $\alpha^9 = \alpha^2$. The relation $f(\alpha) = 0$ can also be rewritten as $\alpha^3 = 1 + \alpha$, which squares to give $\alpha^6 = 1 + \alpha^2$. It follows that

$$g(\alpha^3) = 1 + \alpha^6 + \alpha^9 = 1 + (1 + \alpha^2) + \alpha^2 = 0$$

as claimed. This means that we can define a homomorphism $\lambda\colon L \to K$ by $\lambda(\beta) = \alpha^3$. One can check that this is actually an isomorphism, with $\lambda^{-1}(\alpha) = \beta^5$.

Proposition 9.9. [`prop-units-cyclic`]
Let K be a field, and let U be a finite subgroup of $K^\times$. Then U is cyclic.

Proof. Put $U[d] = \{x \in U \mid x^d = 1\}$. As a polynomial of degree d can have at most d roots, we see that $|U[d]| \leq d$ for all d. The claim thus follows from Lemma 9.11 below. □

Lemma 9.10. [`lem-cyclic-test-aux`]
Let U be a finite abelian group of order n such that $|U[d]| \leq d$ for all d. Then $|U[d]| = d$ whenever d divides n.

Proof. We can define a group homomorphism $\alpha\colon U \to U$ by $\alpha(x) = x^{n/d}$. We note that $\alpha(x)^d = x^n = 1$, so $\alpha(x) \in U[d]$, so $|U[d]| \geq |\operatorname{image}(\alpha)|$. On the other hand, the First Isomorphism Theorem tells us $|\operatorname{image}(\alpha)| = |U|/|\ker(\alpha)|$. Here $|U| = n$, and it is clear from the definitions that $\ker(\alpha) = U[n/d]$, so $|\ker(\alpha)| \leq n/d$, so $|\operatorname{image}(\alpha)| \geq n/(n/d) = d$. Putting this together gives $|U[d]| \geq d$, but also $|U[d]| \leq d$ by assumption, so $|U[d]| = d$ as claimed. The groups and homomorphisms considered can be displayed in the following diagram:

$$\begin{tikzcd}
U[n/d] \arrow[r, tail] \arrow[d] & U \arrow[rr, two heads] \arrow[d, "\alpha"'] & & U/U[n/d] \arrow[d, "\simeq"', "\overline{\alpha}"] \\
1 \arrow[r, tail] & U & U[d] \arrow[l, tail] & \operatorname{image}(\alpha) \arrow[l, tail]
\end{tikzcd}$$

□

Lemma 9.11. [`lem-cyclic-test`]
Let U be a finite abelian group such that $|U[d]| \leq d$ for all d. Then U is cyclic.

Proof. Put $n = |U|$ and let C be a cyclic group of order n; we will compare U with C. Put

$$U\langle d\rangle = \{x \in U \mid x \text{ has exact order } d\}.$$

Note that $x^d = 1$ if and only if the exact order of x is a divisor of d. Using this together with Lemma 9.10 we see that $d = |U[d]| = \sum_{e|d} |U\langle e\rangle|$, so

$$|U\langle d\rangle| = d - \sum_{e|d, e<d} |U\langle e\rangle|.$$

Similarly, we have

$$|C\langle d\rangle| = d - \sum_{e|d, e<d} |C\langle e\rangle|.$$

Note that $|U\langle 1\rangle| = 1 = |C\langle 1\rangle|$. If we know that $|U\langle e\rangle| = |C\langle e\rangle|$ for all $e < d$, we can use the above two displayed equations to see that $|U\langle d\rangle| = |C\langle d\rangle|$ as well. It therefore follows by induction that $|U\langle d\rangle| = |C\langle d\rangle|$ for all d dividing n, and in particular that $|U\langle n\rangle| = |C\langle n\rangle|$. Now, any generator of C lies in $C\langle n\rangle$, so

$|C\langle n\rangle| > 0$, so $|U\langle n\rangle| > 0$. If x is any element of $U\langle n\rangle$ then x generates a cyclic subgroup of U of order n, which must therefore be U itself. Thus U is cyclic as claimed. □

Remark 9.12. [rem-classify]
We have chosen to give a proof that does not depend on the classification of finite abelian groups. Readers who are familiar with that classification may prefer to proceed as follows. The general theory implies that there is a unique sequence $d_1, \dots, d_r$ of integers with $d_k > 0$ and $d_1|d_2|\cdots|d_r$, such that U is isomorphic to $\prod_{k=1}^r C_{d_k}$. In particular, U is cyclic if and only if $r = 1$, so we must show that this is the case. As d_1 divides d_k for all k, we see that each cyclic factor C_{d_k} contains a copy of C_{d_1}, and thus $U[d_1] \simeq C_{d_1}^r$ and $|U[d_1]| = d_1^r$. By assumption we have $|U[d_1]| \leq d_1$, so we must have $r = 1$ as required.

Corollary 9.13. [cor-units-cyclic]
If K is a finite field of order q then $K^\times$ is cyclic of order $q - 1$.

Proof. This is immediate from Proposition 9.9. □

We now pause to justify the claims made in Example 9.2.

Proposition 9.14. [prop-Fpi]
Let p be a prime. Then $\mathbb{F}_p[i]$ is a field if and only if $p = 3 \pmod 4$.

Proof. We first dispose of the case $p = 2$. There $p \neq 3 \pmod 4$, and the ring $\mathbb{F}_2[i] = \{0, 1, i, 1 + i\}$ is not a field because the element $1 + i$ has no inverse. From now on we assume that p is odd, so either $p = 1 \pmod 4$ or $p = 3 \pmod 4$. We will say that p is *bad* if $\mathbb{F}_p[i]$ is not a field. We must show that p is bad if and only if $p = 1 \pmod 4$.

We next claim that p is bad if and only if there is an element $a \in \mathbb{F}_p$ with $a^2 = -1$. Indeed, if there exists such an a then we have $a + i, a - i \neq 0$ but $(a + i)(a - i) = a^2 - i^2 = (-1) - (-1) = 0$ so $\mathbb{F}_p[i]$ is not a field, so p is bad. On the other hand, if there is no such a then the polynomial $f(x) = x^2 + 1$ has no roots in $\mathbb{F}_p[x]$ and so is irreducible (because any nontrivial factor would have to have degree one). It therefore follows that $\mathbb{F}_p[x]/f(x)$ is a field, which is easily seen to be isomorphic to $\mathbb{F}_p[i]$; so p is good.

Next, Corollary 9.13 tells us that $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$. If p is bad then there is an element a with $a^2 = -1$ so the subgroup generated by a is $\{1, a, -1, -a\}$, which has order 4. It follows by Lagrange's theorem that $p - 1$ is divisible by 4, so $p = 1 \pmod 4$. Conversely, suppose that $p = 1 \pmod 4$, so $(p - 1)/4$ is an integer. Choose a generator b for the cyclic group $\mathbb{F}_p^\times$, and put $a = b^{(p-1)/4}$. The powers $1, b, \dots, b^{p-2}$ are then distinct, so we see that $a^2 = b^{(p-1)/2} \neq 1$ but $a^4 = b^{p-1} = 1$. This means that $(a^2 + 1)(a^2 - 1) = a^4 - 1 = 0$ but $a^2 - 1 \neq 0$ so $a^2 + 1 = 0$, which implies that p is bad. □

Proposition 9.15. [prop-factor]
Let K be a finite field of order $q = p^r$. Then $\prod_{\alpha \in K}(x - \alpha) = x^q - x$.

Proof. We have $|K^\times| = q - 1$, so for all $\alpha \in K^\times$ we have $\alpha^{q-1} = 1$. It follows that for all $\alpha \in K$ we have $\alpha^q - \alpha = 0$. Thus the elements of K give q distinct roots of $x^q - x$, and it follows that $x^q - x = \prod_\alpha (x - \alpha)$. □

Proposition 9.16. [prop-unique]
Let K and L be fields of order $q = p^n$. Then $K \simeq L$.

Proof. We have seen that $K^\times$ is cyclic, generated by some element α, say. We then have a surjective homomorphism $\epsilon\colon \mathbb{F}_p[x] \to K$ given by $x \mapsto \alpha$. Let $f(x)$ be the minimal polynomial of α over $\mathbb{F}_p$, or in other words, the monic generator of $\ker(\epsilon)$. Then α induces an isomorphism $\overline{\epsilon}\colon \mathbb{F}_p[x]/f(x) \to K$. Moreover, $f(x)$ is non-constant and divides $x^q - x$, which factors in $L[x]$ as $\prod_{\beta \in L}(x - \beta)$. It follows that $f(\beta) = 0$ for some $\beta \in L$. We can therefore define $\phi\colon \mathbb{F}_p[x]/f(x) \to L$ by $\phi(x) = \beta$. Now the map $\psi = \phi \circ \overline{\epsilon}^{-1}\colon K \to L$ is a homomorphism of fields, and so is injective. As $|K| = |L| = q$, it follows that ψ must be a bijection, and thus an isomorphism. □

Proposition 9.17. [prop-finite-subfield]
Let L be a field of order p^{rs}. Then the subset $K = \{a \in L \mid a^{p^r} = a\}$ is a subfield of L, and is the unique subfield of order p^r. Moreover, we have $[L : K] = s$.

Proof. Using Remark 9.5 we see that $K = \{a \in L \mid \sigma^r(a) = a\} = L^{\{\sigma^r\}}$, which is a subfield by Proposition 1.31. Next, put $f_k(t) = t^{p^k} - t$, so that K is the set of roots of $f_r(t)$ in L, whereas $f_{rs}(t) = \prod_{\alpha\in L}(t-\alpha)$. We claim that $f_r(t)$ divides $f_{rs}(t)$. To see this, consider the standard identity

$$u^m - 1 = (u-1)(1 + u + \cdots + u^{m-1}) = (u-1)\sum_{i=0}^{m-1} u^i.$$

Put $u = t^{p^r-1}$ and

$$m = \frac{p^{rs}-1}{p^r-1} = 1 + p^s + p^{2s} + \cdots + p^{(r-1)s} \in \mathbb{N}$$

so that $u^m = t^{p^{rs}-1}$; we find that $t^{p^{rs}-1} - 1$ is divisible by $t^{p^r-1} - 1$, and we can multiply by t to see that $f_{rs}(t)$ is divisible by $f_r(t)$ as claimed. As $f_{rs}(t)$ splits in L and has distinct roots, we see from Proposition 5.18 that $f_r(t)$ is also split and has distinct roots. This means that the number of roots of $f_r(t)$ is precisely equal to its degree, so $|K| = p^r$. Now if K' is any other subfield of order p^r we can apply Proposition 9.15 to K' to see that K' is the set of roots of $f_r(t)$, so $K' = K$.

Finally, put $t = [L : K] = \dim_K(L)$, which means that L is isomorphic to K^t as vector spaces over K. We have $|K^t| = |K|^t = p^{rt}$ whereas $|L| = p^{rs}$; it follows that $t = s$ as claimed. □

Corollary 9.18. [cor-finite-galois]
If K and L are as in Proposition 9.17 then L is normal over K and $G(L/K)$ is cyclic of order s, generated by σ^r.

Proof. First, we have seen that L is the set of roots of the polynomial $f_{rs}(t) = t^{p^{rs}} - t \in \mathbb{F}_p[t] \subseteq K[t]$, so it is the splitting field over K of that polynomial, so it is normal over K. It follows as in Lemma 6.9 that $|G(L/K)| = [L : K] = s$. Next, we have seen that $L^\times$ is cyclic, of order $p^{rs} - 1$. Choose an element β that generates $L^\times$, so $L^\times$ consists of the powers β^i for $0 \le i < p^{rs} - 1$ and these are all distinct. In particular, we see that the powers $\sigma^j(\beta) = \beta^{p^j}$ are all distinct for $0 \le j < rs$, so the automorphisms σ^j are all different for j in this range. On the other hand, we have seen that every element $\gamma \in L$ has $\gamma^{p^{rs}} = \gamma$ and so $\sigma^{rs} = 1$. It follows that σ generates a cyclic subgroup of $G(L/\mathbb{F}_p)$ of order precisely rs. Now let H be the set of powers σ^{rk} for $0 \le k < s$, so $|H| = s$. By the definition of K we have $\sigma^r|_K = 1_K$ so every element of H acts as the identity on K, so $H \subseteq G(L/K)$, but $|H| = s = |G(L/K)|$ so we must have $G(L/K) = H$ as claimed. □

Exercises

Exercise 9.1. [ex-cyclic-five]
Show that there exists a finite field K such that $K^\times$ contains a cyclic group of order 5, but that there is no finite field K such that $K^\times$ itself is cyclic of order 5.

Exercise 9.2. [ex-F-nine]
Factorise the polynomial $\varphi_8(t) = t^4 + 1$ in $\mathbb{F}_3[t]$ (by trial and error, if necessary). Use this to construct two different fields of order 9. Show explicitly that they are both isomorphic to $\mathbb{F}_3[i]$ (and thus to each other).

Exercise 9.3. [ex-F-twentyfive]
Let K be the set of all matrices of the form $\left[\begin{smallmatrix} a+b & b \\ 2b & a+b \end{smallmatrix}\right]$ with $a, b \in \mathbb{F}_5$. Prove that K is a field of order 25.

Exercise 9.4. [ex-cyclic-galois]
Let p be a prime. Prove that the Galois group $G(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is cyclic of order $p-1$.

Exercise 9.5. [ex-seven-cubed]
Find a generator for the cyclic group $\mathbb{F}_7^\times$. Deduce that $t^3 - 3$ is irreducible in $\mathbb{F}_7$. This means that we can construct $\mathbb{F}_{7^3}$ as $\mathbb{F}_7[\alpha]/(\alpha^3 - 3)$. Show that although α is a primitive element for $\mathbb{F}_{7^3}$, it does not generate $\mathbb{F}_{7^3}^\times$.

Exercise 9.6. [ex-factor-mod-five]
Show that the polynomial $f(x) = x^6 - 2 \in \mathbb{F}_5[x]$ can be written as $f(x) = g_1(x)g_2(x)g_3(x)$, where each $g_i(x)$ is an irreducible quadratic polynomial. Show that if α is a root of $g_i(x)$ in some field $K \supset \mathbb{F}_5$, then α generates a subgroup of $K^\times$ whose order is either 8 or 24.

Exercise 9.7. [ex-Fpp]
Consider the polynomial $f(x) = x^p - x - 1 \in \mathbb{F}_p[x]$, and suppose we have a finite field $K = \mathbb{F}_p(\alpha)$ with $f(\alpha) = 0$. Prove that $\alpha^{p^k} \neq \alpha$ for $0 < k < p$. Deduce that $|K| = p^p$ and that $f(x)$ is irreducible over $\mathbb{F}_p$.

Exercise 9.8. [ex-closed-infinite]
Prove that every algebraically closed field is infinite.

10. Multiquadratic extensions

We will next discuss another extended example, extending Proposition 7.2 and related to Corollary 8.17.

Let $p_1, \dots, p_n$ be distinct prime numbers. For any subset $T \subseteq \{1, \dots, n\}$, put $r_T = \prod_{i \in T} \sqrt{p_i}$. For the case where T is the empty set, this should be interpreted as $r_\emptyset = 1$. We will allow ourselves to write r_{245} rather than $r_{\{2,4,5\}}$ and so on.

Let $K(m)$ be the $\mathbb{Q}$-linear span of all the numbers r_T for $T \subseteq \{1, \dots, m-1\}$. For example:

- $K(0)$ should be interpreted as $\mathbb{Q}$.
- $K(1)$ is the set of all real numbers that can be written as $a_\emptyset + a_1\sqrt{p_1}$ for some rational numbers $a_\emptyset, a_1 \in \mathbb{Q}$.
- $K(2)$ is the set of all real numbers that can be written as
$$a_\emptyset + a_1\sqrt{p_1} + a_2\sqrt{p_2} + a_{12}\sqrt{p_1p_2}$$
for some rational numbers $a_\emptyset, a_1, a_2, a_{12} \in \mathbb{Q}$.
- In general, $K(m)$ could also be described as $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_m})$.

We will call fields of this type *multiquadratic* extensions of $\mathbb{Q}$.

Our main result in this section is as follows:

Theorem 10.1. [thm-mquad]

(a) *$K(m)$ is a subfield of $\mathbb{R}$.*
(b) *The elements $\{r_T \mid T \subseteq \{1, \dots, m\}\}$ form a basis for $K(m)$ over $\mathbb{Q}$ (so $K(m)$ has degree 2^m over $\mathbb{Q}$).*
(c) *If $u \in K(m)$ and $u^2 \in \mathbb{Q}$ then $u = u_T r_T$ for some $T \subseteq \{1, \dots, m\}$ and $u_T \in \mathbb{Q}$.*

We pause to explore the meaning of this a little. Firstly, you can check that
$$2 - 3\sqrt{2} + 4\sqrt{3} - \sqrt{2}\sqrt{3} - \sqrt{5} = 0.000004822873256233\ldots \simeq 0.$$
Could there be any "coincidental" relationship between square roots that holds *exactly*? Part (b) of the theorem says that this is impossible. Next, suppose we have a nonzero real number a that can be expressed in terms of the square roots of certain primes. The hardest part of part (a) of the Theorem tells us that $1/a$ can also be expressed in terms of the square roots of the same primes. For example, if a is the small number mentioned above,
$$a = 2 - 3\sqrt{2} + 4\sqrt{3} - \sqrt{2}\sqrt{3} - \sqrt{5}$$
it works out that
$$a^{-1} = 25918 + 18327\,\sqrt{2} + 14964\,\sqrt{3} + 10581\,\sqrt{2}\sqrt{3} + 11591\,\sqrt{5} + 8196\,\sqrt{2}\sqrt{5} + 6692\,\sqrt{3}\sqrt{5} + 4732\,\sqrt{2}\sqrt{3}\sqrt{5}.$$

We now prove some preliminary results, which will lead in to the proof of Theorem 10.1.

Lemma 10.2. [lem-prod]
If $T, U \subseteq \{1, \dots, m\}$ then $r_T r_U \in K(m)$. More precisely, if $W = T \cap U$ and $V = (T \cup U) \setminus W$ and $w = \prod_{i \in W} p_i \in \mathbb{Q}$ then $r_T r_U = w r_V$.

Proof. If $i \in W$ then $\sqrt{p_i}$ occurs in both r_T and r_U giving a factor of p_i in $r_T r_U$. If $i \in V$ then $\sqrt{p_i}$ occurs either in r_T or in r_U but not both, giving a factor of $\sqrt{p_i}$ in $r_T r_U$. Thus, we have $r_T r_U = w r_V$. As $K(m)$ was defined to be the $\mathbb{Q}$-linear span of a set of elements including the element r_V, it follows that $r_T r_U \in K(m)$. □

Lemma 10.3. [lem-mquad-subring]
$K(m)$ is a subring of $\mathbb{R}$.

Proof. We must show that $K(m)$ contains 0 and 1 and that it is closed under addition, subtraction and multiplication. Note that $K(m)$ was defined as a span, so it is certainly a $\mathbb{Q}$-linear subspace of $\mathbb{R}$, so it contains 0 and is closed under addition and subtraction and under multiplication by elements of $\mathbb{Q}$. We can think of 1 as $r_\emptyset$, so we also have $1 \in K(m)$. Now consider elements $a, b \in K(m)$. From the definition of $K(m)$, we can write $a = \sum_T a_T r_T$ and $b = \sum_U b_U r_U$ for some numbers $a_T, b_U \in \mathbb{Q}$. It follows that

$$ab = \sum_{T,U} a_T b_U r_T r_U.$$

Here $r_T r_U \in K(m)$ by Lemma 10.2, and $a_T b_U$ is just a rational number, so $a_T b_U r_T r_U \in K(m)$. Moreover, $K(m)$ is closed under addition, so $\sum_{T,U} a_T b_U r_T r_U \in K(m)$, or in other words $ab \in K(m)$. Thus $K(m)$ is closed under multiplication, as required. □

We could now use Proposition 5.11 to show that $K(m)$ is a subfield of $\mathbb{R}$. However, we will instead give a more direct and elementary argument, which might be considered more illuminating.

Lemma 10.4. [lem-not-square]
Suppose that $T \subseteq \{1, \dots, m-1\}$ and $u_T \in \mathbb{Q}$. Then $(u_T r_T)^2 \neq p_m$.

Proof. Suppose that $(u_T r_T)^2 = p_m$; we will derive a contradiction. Clearly we must have $u_T \neq 0$, so we can write $u_T = \pm u/v$, where u and v are positive integers with no common factors. We then have

$$p_m = (u_T r_T)^2 = u^2 r_T^2 / v^2 = u^2 v^{-2} \prod_{i \in T} p_i,$$

so

$$p_m v^2 = u^2 \prod_{i \in T} p_i.$$

This is now an equation in $\mathbb{Z}$; it implies that p_m divides $u^2 \prod_T p_i$. By assumption the primes p_i on the right hand side are all different from p_m, so p_m must divide u instead. We can write $u = p_m w$ and rearrange to get

$$v^2 = p_m w^2 \prod_{i \in T} p_i.$$

Here the right hand side is divisible by p_m, so the left hand side must be divisible by p_m, so v must be divisible by p_m. This contradicts the fact that u and v have no common factors. □

Lemma 10.5. [lem-step]
Suppose that Theorem 10.1 holds for $K(m-1)$, and that $b, c \in K(m-1)$. Put $a = b + c\sqrt{p_m}$ and $a' = b - c\sqrt{p_m}$, so $a, a' \in K(m)$. Then

- *$aa' = b^2 - c^2 p_m \in K(m-1)$*
- *If $aa' = 0$ then $b = c = 0$ and so $a = 0$.*
- *If $aa' \neq 0$ then $1/a \in K(m)$.*

Proof. It is simple algebra to check that $aa' = b^2 - c^2 p_m$. As $b, c \in K(m-1)$ and $p_m \in \mathbb{Z}$ it follows that $aa' \in K(m-1)$. Now suppose that $aa' = 0$, so $b^2 = c^2 p_m$. Suppose that c is nonzero, so $p_m = (b/c)^2$. By assumption $K(m-1)$ is a field, so the element $u = b/c$ lies in $K(m-1)$, and $u^2 = p_m \in \mathbb{Q}$. Part (c) of Theorem 10.1 tells us that $u = u_T r_T$ for some $T \subseteq \{1, \dots, m-1\}$ and $u_T \in \mathbb{Q}$, so $(u_T r_T)^2 = p_m$. Lemma 10.4

tells us that this is impossible. This contradiction means that we must in fact have $c = 0$. We also have $b^2 = c^2 p_m$, so it follows that $b = 0$ as well.

Now suppose instead that the element aa' is nonzero. As $K(m-1)$ is a field and $aa' \in K(m-1)$ it follows that $(aa')^{-1} \in K(m-1) \subseteq K(m)$. As $K(m)$ is a subring of $\mathbb{R}$ and $a', (aa')^{-1} \in K(m)$ it follows that $a'.(aa')^{-1} \in K(m)$; but $a'.(aa')^{-1} = a^{-1}$, so $a^{-1} \in K(m)$ as claimed. □

Proof of Theorem 10.1. We can assume by induction that the theorem holds for $K(m-1)$ (as the initial case of $K(0)$ is trivial).

(b) The elements r_T span $K(m)$ by definition, so we need only show that they are linearly independent. Suppose we have rational numbers a_T for all $T \subseteq \{1, \dots, m\}$, giving an element $a = \sum_T a_T r_T \in K(m)$. We must show that if $a = 0$, then the individual coefficients a_T are all zero. We put

$$b = \sum_{U \subseteq \{1,\dots,m-1\}} a_U r_U \in K(m-1)$$
$$c = \sum_{U \subseteq \{1,\dots,m-1\}} a_{U\cup\{m\}} r_U \in K(m-1)$$

so that $a = b + c\sqrt{p_m}$. We then put $a' = b - c\sqrt{p_m}$ as in Lemma 10.5. If $a = 0$ then certainly $aa' = 0$ so the Lemma tells us that $b = c = 0$. As $b = 0$ we have $\sum_{U\subseteq\{1,\dots,m-1\}} a_U r_U = 0$ but the set $\{r_U \mid U \subseteq \{1, \dots, m-1\}\}$ is linearly independent by our inductive assumption, so we must have $a_U = 0$ for all $U \subseteq \{1, \dots, m-1\}$. By applying the same logic to c, we see that $a_{U\cup\{m\}}$ is also zero for all $U \subseteq \{1, \dots, m-1\}$. These two cases cover all the coefficients a_T, so $a_T = 0$ for all $T \subseteq \{1, \dots, m\}$, as required.

(a) We showed in Lemma 10.3 that $K(m)$ is a subring of $\mathbb{R}$, so all that is left is to show that if $a \in K(m)$ is nonzero then a^{-1} is also in $K(m)$. We can write it as $a = b + c\sqrt{p_m}$ and put $a' = b - c\sqrt{p_m}$, just as before. If $aa' = 0$ then Lemma 10.5 tells us that $a = 0$, contrary to assumption. Thus $aa' \neq 0$ and the other part of Lemma 10.5 tells us that $a^{-1} \in K(m)$, as required.

(c) Suppose that $u \in K(m)$ and $u^2 = q \in \mathbb{Q}$. Just as above, we can write $u = x + y\sqrt{p_m}$ with $x, y \in K(m-1)$. It follows that $(x^2 + p_m y^2 - q) + 2xy\sqrt{p_m} = u^2 - q = 0$. Here $x^2 + p_m y^2 - q$ and $2xy$ are in $K(m-1)$, and it follows easily from part (a) that $\{1, \sqrt{p_m}\}$ is a basis for $K(m)$ over $K(m-1)$. We must therefore have $x^2 + p_m y^2 - q = 0$ and $2xy = 0$, so either $x = 0$ or $y = 0$.

Suppose that $y = 0$, so the equation $x^2 + p_m y^2 - q = 0$ reduces to $u^2 = x^2 = q$. This means that $u \in K(m-1)$ and $u^2 \in \mathbb{Q}$, so part (c) of the theorem for $K(m-1)$ tells us that $u = u_T r_T$ for some $T \subseteq \{1, \dots, m-1\}$ and $u_T \in \mathbb{Q}$, as required.

Suppose instead that $x = 0$, so $y^2 = q/p_m$ with $y \in K(m-1)$ and $y^2 \in \mathbb{Q}$. It follows that $y = y_T r_T$ for some $T \subseteq \{1, \dots, m-1\}$ and $y_T \in \mathbb{Q}$, so $u = y\sqrt{p_m} = y_T r_{T\cup\{m\}}$, which again has the required form.

□

We next examine the Galois groups of multiquadratic extensions.

Proposition 10.6. [prop-mquad-galois]
For $i = 1, \dots, m$ there is an automorphism τ_i of $K(m)$ with $\tau_i(\sqrt{p_1}) = -\sqrt{p_i}$ and $\tau_i(\sqrt{p_j}) = \sqrt{p_j}$ for all $j \neq i$. Moreover, the full Galois group $G(K(m)/\mathbb{Q})$ is the product of all the groups $\{1, \tau_i\} \simeq C_2$, so $G(K(m)/\mathbb{Q}) \simeq C_2^m$.

Proof. As the elements r_T form a basis for $K(m)$, we can certainly define a $\mathbb{Q}$-linear map $\tau_i \colon K(m) \to K(m)$ by

$$\tau_i(r_T) = \begin{cases} -r_T & \text{if } i \in T \\ +r_T & \text{if } i \notin T. \end{cases}$$

Note that $\tau_i(0) = 0$ and $\tau_i(1) = \tau_i(r_\emptyset) = 1$. Now consider a pair of basis elements r_T, r_U with $r_T r_U = w r_V$ as in Lemma 10.2. We claim that $\tau_i(r_T r_U) = \tau_i(r_T)\tau_i(r_U)$. There are four cases to consider, depending on whether $i \in T$ or not, and whether $i \in U$ or not; we leave details to the reader. Now consider arbitrary elements $a, b \in K(m)$, say $a = \sum_T a_T r_T$ and $b = \sum_U b_U r_U$ with $a_T, b_U \in \mathbb{Q}$. We then have

$$\begin{aligned}\tau_i(ab) &= \tau_i\left(\sum_{T,U} a_T b_U r_T r_U\right) = \sum_{T,U} a_T b_U \tau_i(r_T r_U) = \sum_{T,U} a_T b_U \tau_i(r_T)\tau_i(r_U) \\ &= \left(\sum_T a_T \tau_i(r_T)\right)\left(\sum_U b_U \tau_i(r_U)\right) = \tau_i(a)\tau_i(b).\end{aligned}$$

This proves that τ_i is a homomorphism from $K(m)$ to itself. It is clear that $\tau_i^2(r_T) = r_T$ for all T, so $\tau_i^2 = 1$. Now suppose that $i \neq j$. We find that $\tau_i\tau_j(r_T)$ is either $+r_T$ (if $\{i,j\} \subseteq T$ or $\{i,j\} \cap T = \emptyset$) or $-r_T$ (if $|\{i,j\} \cap T| = 1$). From this it is clear that $\tau_i\tau_j = \tau_j\tau_i$, so the elements τ_i generate a commutative subgroup $T \leq G(K(m)/\mathbb{Q})$. For any sequence $\epsilon_1, \dots, \epsilon_m$ in $\{0,1\}$ we have an element $\sigma_\epsilon = \tau_1^{\epsilon_1} \cdots \tau_m^{\epsilon_m} \in T$. Note that $\sigma_\epsilon(\sqrt{p_i})$ is $+\sqrt{p_i}$ if $\epsilon_i = 0$, and $-\sqrt{p_i}$ if $\epsilon_i = 1$. Using this we see that if $\sigma_\epsilon = \sigma_\delta$ then $\epsilon = \delta$. We thus have 2^m different elements of $T \subseteq G(K(m)/\mathbb{Q})$. It follows using Proposition 6.11 that $K(m)$ is normal over $\mathbb{Q}$ and that T is the full Galois group. □

It will be proved as Theorem 11.12 that every field extension of finite degree has a primitive element. It turns out that there is a nice explicit example of this for multiquadratic fields.

Proposition 10.7. [prop-mquad-primitive]
If $\theta_n = \sum_{i=1}^n \sqrt{p_i}$ then $\mathbb{Q}(\theta_n) = K(n)$.

(I thank Jayanta Manoharmayum for this fact and its proof.)

Proof. This is clear for $n = 1$, so we may assume inductively that $K(n-1) = \mathbb{Q}(\theta_{n-1})$. We have seen that $K(n)$ has degree 2^n over $\mathbb{Q}$, and $\mathbb{Q} \leq \mathbb{Q}(\theta_n) \leq K(n)$ so the degree of $\mathbb{Q}(\theta_n)$ over $\mathbb{Q}$ must have the form 2^m for some m with $0 \leq m \leq n$; we must show that $m = n$. Let the minimal polynomial of θ_n over $\mathbb{Q}$ be

$$f(t) = \sum_{i=0}^{2^m} a_i t^i,$$

and put

$$\begin{aligned}g(t) &= \sum_{i=0}^{2^m}\left(\sum_{2j \leq 2^m - i}\binom{i+2j}{2j} p_n^j a_{i+2j}\right) t^i \\ h(t) &= \sum_{i=0}^{2^m-1}\left(\sum_{2j < 2^m - i}\binom{i+2j+1}{2j+1} p_n^j a_{i+2j+1}\right) t^i.\end{aligned}$$

By expanding out the relation $f(\theta_{n-1} + \sqrt{p_n}) = f(\theta_n) = 0$ we obtain $g(\theta_{n-1}) + h(\theta_{n-1})\sqrt{p_n} = 0$, with $g(\theta_{n-1}), h(\theta_{n-1}) \in K(n-1)$. We have seen that $\{1, \sqrt{p_n}\}$ is a basis for $K(n)$ over $K(n-1)$, so $g(\theta_{n-1}) = h(\theta_{n-1}) = 0$. The coefficient of t^{2^m-1} in $h(t)$ is 2^m, so h is nonzero and has degree precisely $2^m - 1$. It follows that $2^m - 1$ must be at least as large as the degree of θ_{n-1} over $\mathbb{Q}$, which is 2^{n-1} by inductive assumption. This gives $m > n - 1$ but we also had $0 \leq m \leq n$, so $m = n$ as required. □

11. The Galois correspondence

The following theorem is the main result of Galois theory.

Theorem 11.1. [thm-correspondence]
Let M be a normal extension of K, with Galois group $G = G(M/K)$.

(a) *For any subgroup $H \leq G$, the set*

$$L = M^H = \{a \in M \mid \sigma(a) = a \text{ for all } \sigma \in H\}$$

is a subfield of M containing K, and M is normal over L with $G(M/L) = H$.

(b) *For any subfield $L \subseteq M$ containing K, the Galois group $H = G(M/L)$ is a subgroup of G and we have $M^H = L$.*

(c) *If L and H are as above, then L is a normal extension of K if and only if H is a normal subgroup of G, and if so, then $G(L/K) = G/H$.*

This will be proved in three parts, as Corollary 11.7, Proposition 11.8 and Proposition 11.11 below.

Remark 11.2. [`rem-correspondence`]
Let $\mathcal{L}$ be the set of all subfields L with $K \subseteq L \subseteq M$. Let $\mathcal{H}$ be the set of all subgroups of G. We can define $\Phi\colon \mathcal{L} \to \mathcal{H}$ by $\Phi(L) = G(M/L)$, and we can define $\Psi\colon \mathcal{H} \to \mathcal{L}$ by $\Psi(H) = M^H$. Parts (a) and (b) of the theorem can be rephrased as saying that Φ and Ψ are inverse to each other, so both are bijections.

Remark 11.3. [`rem-finite-galois`]
Suppose that $K = \mathbb{F}_p$, so that M is also finite, of order p^n say. Then $G = G(M/K)$ is cyclic of order n, generated by the Frobenius automorphism $\sigma\colon a \mapsto a^p$. For each divisor d of n we have a cyclic subgroup of G of order d generated by $\sigma^{n/d}$, and these are all the subgroups of G. Given this, all the claims in Theorem 11.1 follow easily from Theorem 9.1. The same is true with just a little more work if M is finite and K is any subfield of M.

Example 11.4. [`eg-even-quartic-galois`]
Consider again the field $K = \mathbb{Q}(\alpha, \beta)$, where $\alpha = \sqrt{3+\sqrt{7}}$ and $\beta = \sqrt{3-\sqrt{7}}$, as in Example 7.6. We will make the Galois correspondence explicit in this case. First note that $\alpha^2 - 3 = 3 - \beta^2 = \sqrt{7}$ and $\alpha\beta = \sqrt{2}$. It follows using this that $(\alpha+\beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta = 6 + 2\sqrt{2}$, and $\alpha + \beta > 0$ so $\alpha + \beta = \sqrt{6+2\sqrt{2}}$. In the same way we also see that $\alpha - \beta = \sqrt{6 - 2\sqrt{2}}$. We also note that $\alpha^2 - \beta^2 = 2\sqrt{7}$, and we can divide this by the equation $\alpha\beta = \sqrt{2}$ to get $\alpha/\beta - \beta/\alpha = \sqrt{14}$.

The subgroups of D_8 (other than $\{1\}$ and D_8 itself) can be listed as follows:

$$\begin{aligned}
A_0 &= \{1, \quad (\alpha\ -\beta)(-\alpha\ \beta)\} \\
A_1 &= \{1, \quad (\alpha\ -\alpha)\} \\
A_2 &= \{1, \quad (\alpha\ \beta)(-\alpha\ -\beta)\} \\
A_3 &= \{1, \quad (\beta\ -\beta)\} \\
Z &= \{1, \quad (\alpha\ -\alpha)(\beta\ -\beta)\} \\
B_0 &= A_0 A_2 \simeq C_2^2 \\
B_1 &= A_1 A_3 \simeq C_2^2 \\
C_4 &= \text{ subgroup generated by } (\alpha\ -\beta\ -\alpha\ \beta).
\end{aligned}$$

We can display the subgroups and subfields in the following diagram:

$$\begin{tikzcd}
1 & & & \{1\} \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
2 & A_0 \arrow[dr] & A_2 \arrow[d] & Z \arrow[dl] \arrow[d] \arrow[dr] & A_1 \arrow[d] & A_3 \arrow[dl] \\
4 & & B_0 \arrow[dr] & C_4 \arrow[d] & B_1 \arrow[dl] & \\
8 & & & D_8 & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & K & & \\
\mathbb{Q}(\alpha-\beta) \arrow[urr] & \mathbb{Q}(\alpha+\beta) \arrow[ur] & \mathbb{Q}(\sqrt{2},\sqrt{7}) \arrow[u] & \mathbb{Q}(\beta) \arrow[ul] & \mathbb{Q}(\alpha) \arrow[ull] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[ul] \arrow[u] \arrow[ur] & \mathbb{Q}(\sqrt{14}) \arrow[u] & \mathbb{Q}(\sqrt{7}) \arrow[ul] \arrow[u] \arrow[ur] & \\
 & & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}$$

The first lattice shows all the subgroups, with the smaller groups towards the top. The orders of the groups are shown at the left. Arrows indicate inclusions between subgroups, so they point downwards. For each subgroup H shown on the left, we display the field K^H in the corresponding place on the right. As the

Galois correspondence is order-reversing, the largest fields appear at the top and the inclusion arrows point upwards.

For example, consider the group C_4. We observed above that $\sqrt{14} = \alpha/\beta - \beta/\alpha$. Let ρ be the generator of C_4. This sends α to $-\beta$ and β to α. It therefore sends $\alpha/\beta - \beta/\alpha$ to $(-\beta)/\alpha - \alpha/(-\beta)$, which is the same as $\alpha/\beta - \beta/\alpha$. In other words, we have $\rho(\sqrt{14}) = \sqrt{14}$, so $\sqrt{14} \in K^{C_4}$. On the other hand, we always have $[K : K^H] = |H|$ and so $[K^H : \mathbb{Q}] = 8/|H|$, so in particular $[K^{C_4} : \mathbb{Q}] = 2$. Similarly, it is clear that α is fixed by A_3, so $\mathbb{Q}(\alpha) \subseteq K^{A_3}$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [K^{A_3} : \mathbb{Q}]$, so we must have $K^{A_3} = \mathbb{Q}(\alpha)$. All the other subgroups can be handled in the same way.

Lemma 11.5. [lem-correspondence-a]
Let H be any subgroup of G; then $H \leq G(M/M^H)$ and $|G(M/M^H)| = [M : M^H] \geq |H|$.

Proof. By definition we have

$$M^H = \{a \in M \mid \sigma(a) = a \text{ for all } \sigma \in H\}$$
$$G(M/M^H) = \{\sigma\colon M \to M \mid \sigma(a) = a \text{ for all } a \in M^H\}.$$

If $\sigma \in H$ then $\sigma(a) = a$ for all $a \in M^H$ by the very definition of M^H, so $\sigma \in G(M/M^H)$. This shows that $H \leq G(M/M^H)$, and so $|H| \leq |G(M/M^H)|$. Next, as M is normal over K we see from Proposition 6.14 that it is normal over any intermediate field, such as M^H. We therefore see from Proposition 6.11 that $[M : M^H] = |G(M/M^H)| \geq |H|$ as claimed. □

Lemma 11.6. [lem-V-zero]
Let H be any subgroup of G, and let $e_1, \dots, e_n$ be a basis for M over M^H (so $[M : M^H] = n$). Put

$$V = \{b = (b_1, \dots, b_n) \in M^n \mid \sum_{i=1}^{n} b_i \sigma(e_i) = 0 \textit{ for all } \sigma \in H\}.$$

Then $V = 0$.

Proof. We first note some properties of V.

(a) V is clearly a vector subspace of M^n.
(b) If $b \in V$ then we can take $\sigma = 1$ in the definition to see that $\sum_i b_i e_i = 0$.
(c) We next claim that $V \cap (M^H)^n = \{0\}$. Indeed, if $b \in V \cap (M^H)^n$ then the relation $\sum_i b_i e_i = 0$ above is an M^H-linear relation between the elements e_i, which by assumption are linearly independent over M^H; so we must have $b_1 = \dots = b_n = 0$.
(d) Suppose that $(b_1, \dots, b_n) \in V$ and $\tau \in H$; we claim that $(\tau(b_1), \dots, \tau(b_n)) \in V$ also. Indeed, we have $\sum_i b_i \sigma(e_i) = 0$ for all σ, and as σ is arbitrary we can replace it by $\tau^{-1}\sigma$ to see that $\sum_i b_i \tau^{-1}\sigma(e_i) = 0$. We then apply τ to this equation to obtain $\sum_i \tau(b_i)\sigma(e_i) = 0$, which proves the claim.

Next, for any vector $b \in V$, we define the *size* of b to be the number of nonzero entries. We must show that for $r > 0$ there are no elements of size r, which we do by induction on r.

Consider an element $b \in V$ of size one, so there is an index i with $b_i \neq 0$, and all other entries are zero. Fact (b) above therefore reduces to $b_i e_i = 0$. As e_i is a basis element it is nonzero, and $b_i \neq 0$ by assumption, so we have a contradiction. Thus, there are no elements in V of size one, which starts the induction.

Now suppose that $r > 0$, and we have shown already that there are no elements in V of size s for all $0 < s < r$. Consider an element $b \in V$ of size r. We can then choose i such that $b_i \neq 0$, and after replacing b by b/b_i we may assume that $b_i = 1$. Now fix $\tau \in H$ and put $c_k = b_k - \tau(b_k)$, so $c \in V$ by facts (d) and (a). We clearly have $c_i = 0$, and also $c_j = 0$ whenever $b_j = 0$; so the size of c is strictly less than that of b. By our induction hypothesis we must therefore have $c = 0$. This means that $b_k = \tau(b_k)$ for all k, but τ was arbitrary so $b_k \in M^H$. This means that $b \in V \cap (M^H)^n$ so $b = 0$ by fact (c). This contradicts the assumption that b has size r, and so completes the induction step. □

Corollary 11.7. [cor-correspondence-a]
For any subgroup $H \leq G$ we have $[M : M^H] = |H|$ and $G(M/M^H) = H$.

Proof. Choose $e_1, \dots, e_n$ as in the lemma, and list the elements of H as $\tau_1, \dots, \tau_m$. Define $w_i \in M^m$ (for $1 \leq i \leq n$) by $w_i = (\tau_1(e_i), \dots, \tau_m(e_i))$. It is then clear that $V = \{b \in M^n \mid \sum_i b_i w_i = 0\}$, so the lemma tells us that the vectors $w_1, \dots, w_n$ are linearly independent. The length of any linearly independent list is at most the dimension of the containing space, so we have $n \leq m$, or in other words $[M : M^H] \leq |H|$. Lemma 11.5 gives the reverse inequality, so $[M : M^H] = |H|$. The same lemma also tells us that $H \leq G(M/M^H)$ and these two groups have the same order (namely $[M : M^H]$) so $H = G(M/M^H)$. □

Proposition 11.8. [`prop-correspondence-b`]
Let M be a normal extension of K, with Galois group $G = G(M/K)$, and let L be a field with $K \leq L \leq M$. Put $H = G(M/L)$. Then H is a subgroup of G and $[M : L] = |H|$ and $L = M^H$.

Proof. Proposition 6.14 tells us that M is normal over L, and so we see from Proposition 6.11 that $|H| = |G(M/L)| = [M : L]$. Next, recall that by definition we have

$$\begin{aligned} G &= \{\sigma \colon M \to M \mid \sigma(a) = a \text{ for all } a \in K\} \\ H &= \{\sigma \colon M \to M \mid \sigma(a) = a \text{ for all } a \in L \supseteq K\} \\ M^H &= \{a \in M \mid \sigma(a) = a \text{ for all } \sigma \in H\}. \end{aligned}$$

It is clear from this that H is a subgroup of G. It is also tautological that $L \subseteq M^H$: if $a \in L$ then $\sigma(a) = a$ for all $\sigma \in H$ by the very definition of H, so certainly $a \in M^H$. We therefore have $|H| = [M : L] = [M : M^H][M^H : L]$. On the other hand, Lemma 11.5 tells us that $[M : M^H] \geq |H|$. The only way this can be consistent is if $[M : M^H] = |H|$ and $[M^H : L] = 1$, so $M^H = L$. □

Proposition 11.9. [`prop-correspondence-conj`]
Suppose that $K \leq L \leq M$ and $\tau \in G$. Then $K \leq \tau(L) \leq M$ and $G(M/\tau(L)) = \tau G(M/L)\tau^{-1}$.

Proof. As τ is an automorphism of M we have $\tau(M) = M$, and as $\tau|_K = 1_K$ we have $\tau(K) = K$. We can therefore apply τ to the inclusions $K \subseteq L \subseteq M$ to see that $K \subseteq \tau(L) \subseteq M$. We thus have groups $H = G(M/L)$ and $H' = G(M/\tau(L))$. If $\sigma \in H$ and $a' \in \tau(L)$ then $a' = \tau(a)$ for some $a \in L$, which means that $\sigma(a) = a$, so $\tau\sigma\tau^{-1}(a') = \tau\sigma(a) = \tau(a) = a'$. This shows that $\tau\sigma\tau^{-1} \in G(M/\tau(L)) = H'$. As $\sigma \in H$ was arbitrary we have $\tau H \tau^{-1} \subseteq H'$. Conversely, suppose that $\sigma' \in H'$. Put $\sigma = \tau^{-1}\sigma'\tau$, so $\sigma' = \tau\sigma\tau^{-1}$. If $a \in L$ then $\tau(a) \in \tau(L)$, and $\sigma'|_{\tau(L)} = 1$ so $\sigma'\tau(a) = \tau(a)$, so $\sigma(a) = \tau^{-1}\sigma'\tau(a) = \tau^{-1}\tau(a) = a$. This shows that $\sigma \in H$, so $\sigma' = \tau\sigma\tau^{-1} \in \tau H \tau^{-1}$ as required. □

We next study the set $E_K(L, M) = \{\theta \colon L \to M \mid \theta|_K = 1_K\}$ (as in Definition 6.1).

Proposition 11.10. [`prop-correspondence-cosets`]
Let L and H be related as in Theorem 11.1. Then there is a bijection $G/H \to E_K(L, M)$ given by $\sigma H \mapsto \sigma|_L$.

Proof. First, if $\sigma H = \sigma' H$ then $\sigma' = \sigma\tau$ for some $\tau \in H = G(M/L)$, so $\tau|_L = 1_L$, so for $a \in L$ we have $\sigma'(a) = \sigma(\tau(a)) = \sigma(a)$, so $\sigma'|_L = \sigma|_L$. This means that there is a well-defined map $f \colon G/H \to E_K(L, M)$ given by $f(\sigma H) = \sigma|_L$. It follows easily from Corollary 6.16 that this is injective. Moreover, as M is normal over K we have

$$|E_K(L, M)| = [L : K] = \frac{[M : K]}{[M : L]} = \frac{|G|}{|H|} = |G/H|.$$

It follows that f must actually be a bijection. □

Proposition 11.11. [`prop-correspondence-c`]
Let L and H be related as in Theorem 11.1. Then then L is a normal extension of K if and only if H is a normal subgroup of G, and if so, then $G(L/K) = G/H$.

Proof. First suppose that H is a normal subgroup. Consider an element $\zeta \in E_K(L, M)$. By the previous proposition we can choose $\sigma \in G$ such that $\sigma|_L = \zeta$, and so $\zeta(L) = \sigma(L)$. It follows by Proposition 11.9 that $G(M/\zeta(L)) = \sigma H \sigma^{-1}$, which is the same as H because H is normal. Next, Proposition 11.8 (applied to $\zeta(L)$) tells us that $\zeta(L) = M^{G(M/\zeta(L))} = M^H = L$. Thus, we can regard ζ as an element of $G(L/K)$. We deduce that $G(L/K) = E_K(L, M)$. As M is normal over K we have $|E_K(L, M)| = [L : K]$, so $|G(L/K)| = [L : K]$, which implies that L is normal over K (by Proposition 6.11). Proposition 11.10 now also gives us an isomorphism $G/H \to G(L/K)$. □

We conclude this section by proving the following result:

Theorem 11.12 (Theorem of the Primitive Element)**.** [thm-primitive]
Any extension $\phi\colon K \to L$ of finite degree has a primitive element.

Proof. First suppose that K (and therefore L) is finite. We then know that $L^\times$ is cyclic, so we can choose a generator, say α. This is clearly a primitive element for ϕ. For the rest of the proof we may therefore assume that K is infinite.

Corollary 6.13 tells us that there exists a homomorphism $\psi\colon L \to M$ of finite degree such that $\psi\phi$ is normal. After adjusting notation slightly, we can assume that $K \subseteq L \subseteq M$ and that M is normal over K. Now Theorem 11.1 tels us that the fields between K and M biject with the subgroups of the finite group $G(M/K)$, so there are only finitely many such fields.

Now choose $\alpha \in L$ such that $[K(\alpha) : K]$ is as large as possible. We claim that $K(\alpha)$ is actually equal to L. If not, we can choose $\beta \in L$ such that $\beta \notin K(\alpha)$. For each of the infinitely many elements $t \in K$, we have a field $K(\alpha + t\beta)$ with $K \subseteq K(\alpha + t\beta) \subseteq M$. As there are only finitely many fields between K and M, there must exist elements $t \neq u$ with $K(\alpha + t\beta) = K(\alpha + u\beta) = N$ say. We now have $t - u \in K^\times$ and so

$$\beta = \frac{(\alpha + t\beta) - (\alpha + u\beta)}{t - u} \in N,$$

and thus $\alpha = (\alpha + t\beta) - t\beta \in N$. This means that $K(\alpha, \beta) \subseteq N$, so the field $N = K(\alpha + t\beta)$ is strictly larger than $K(\alpha)$. As α was chosen so that $[K(\alpha) : K]$ is as large as possible, this is a contradiction. We must therefore have $K(\alpha) = L$ as claimed. □

Remark 11.13. [rem-mquad-primitive]
We can now revisit Proposition 10.7. There we had a field $K(n)$ and an element $\theta_n = \sum_{i=1}^{n} \sqrt{p_i} \in K(n)$. Part (b) of Theorem 11.1 tells us that $\mathbb{Q}(\theta_n) = K(n)^H$ for some subgroup $H \leq G(K(n)/\mathbb{Q})$. Using Proposition 10.6 we see that θ_n is not fixed by any nontrivial element of $G(K(n)/\mathbb{Q})$, which means that $H = \{1\}$ and so $\mathbb{Q}(\theta_n) = K(n)$, just as we proved more directly before.

Exercises

Exercise 11.1. [ex-H-cap-K]
Let L be a Galois extension of K, with Galois group G, and let H and K be subgroups of G. Prove that $L^H L^K = L^{H \cap K}$.

Exercise 11.2. [ex-vier]
Let K be a field of characteristic zero, and suppose that L is a normal extension of K such that $G(L/K)$ is isomorphic to $C_2 \times C_2$. Show that there exist $\alpha, \beta \in L$ such that $\alpha^2, \beta^2 \in K$ and $\{1, \alpha, \beta, \alpha\beta\}$ is a basis for L over K. Describe the lattice of subgroups of $G(L/K)$, and the corresponding lattice of fields between K and L.

Exercise 11.3. [ex-golden]
Put

$$\begin{aligned} \zeta &= e^{2\pi i/5} \\ \alpha &= \zeta + \zeta^{-1} = 2\cos(2\pi/5) \\ \beta &= \zeta - \zeta^{-1} = 2i\sin(2\pi/5). \end{aligned}$$

Given that $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$, show that $\alpha = (-1 + \sqrt{5})/2$, and deduce that $\sqrt{5} \in \mathbb{Q}(\zeta)$. Then check that $\beta^2 = \alpha^2 - 4$, and thus that $\beta = \sqrt{-(1 + \sqrt{5})/2}$.

Draw the subfield and subgroup lattices for the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$.

Exercise 11.4. [ex-mu-eleven]
Put $\zeta = e^{2\pi i/11}$ and $K = \mathbb{Q}(\zeta) = \mathbb{Q}(\mu_{11})$. Recall that the corresponding cyclotomic polynomial is

$$\varphi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

and that the roots of this are $\zeta, \zeta^2, \dots, \zeta^{10} = \zeta^{-1}$. Define

$$\begin{aligned}\beta &= \zeta + \zeta^{-1} = 2\cos(2\pi/11) \\ \gamma &= \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9.\end{aligned}$$

(a) Explain why β satisfies a quintic equation over $\mathbb{Q}$, and write it down.
(b) Expand γ^2 in powers of ζ, and hence deduce that $\gamma^2 + \gamma + 3 = 0$. Show that $\mathbb{Q}(\sqrt{-11}) \subseteq \mathbb{Q}(\zeta)$.
(c) Use the general theory of cyclotomic extensions to find the structure of $G(K/\mathbb{Q})$, and draw its lattice of subgroups.
(d) Using the earlier parts of the question, draw the subfield lattice.

Exercise 11.5. [ex-two-group]
Let G be a finite group of order 2^r for some r. It is a standard fact from group theory that one can find subgroups

$$\{1\} = H_0 < H_1 < \cdots < H_{r-1} < H_r = G$$

such that $|H_i| = 2^i$ for all i, and H_i is normal in G. Now suppose that G is the Galois group of some normal extension L/K. What can we deduce about the structure of L?

12. Cubics

In this section we will work with cubic polynomials over $\mathbb{Q}$, for convenience. Not much would change if we instead considered cubics over an arbitrary field K (although there would be some special features if the characteristic of K was 2 or 3).

Consider a polynomial $f(x) = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Q}$. If $f(x)$ is reducible then it must factor as $g(x)h(x)$ with $\deg(g(x)) = 1$ and $\deg(h(x)) = 2$. It is then easy to understand the roots of $g(x)$ and $h(x)$, and this determines the roots of $f(x)$. From now on we will ignore this case and assume instead that $f(x)$ is irreducible over $\mathbb{Q}$. We can factor this over $\mathbb{C}$ as $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ say. Moreover, Proposition 4.42 assures us that α, β and γ are all distinct, so the set $R = \{\alpha, \beta, \gamma\}$ has size three. By expanding out the relation

$$x^3 + ax^2 + bx + c = (x-\alpha)(x-\beta)(x-\gamma)$$

we find that

$$\begin{aligned}a &= -(\alpha + \beta + \gamma) \\ b &= \alpha\beta + \beta\gamma + \gamma\alpha \\ c &= -\alpha\beta\gamma.\end{aligned}$$

Now put $K = \mathbb{Q}(\alpha, \beta, \gamma)$, which is the splitting field of $f(x)$. Put $G = G(K/\mathbb{Q})$, which can be considered as a subgroup of $\Sigma_R \simeq \Sigma_3$.

The subgroups of Σ_R can be enumerated as follows.

(a) There is the trivial subgroup, of order one.
(b) There are three different transpositions, namely $(\alpha\ \beta)$, $(\beta\ \gamma)$ and $(\gamma\ \alpha)$. For each transposition τ, the set $\{1, \tau\}$ is a subgroup of Σ_R of order two.
(c) The set $A_R = \{1, (\alpha\ \beta\ \gamma), (\gamma\ \beta\ \alpha)\}$ is a subgroup of order 3, isomorphic to C_3.
(d) The full group Σ_R has order 6.

It is straightforward to check that this gives all possible subgroups of Σ_R. We also know from Proposition 6.17 that the subgroup G acts transitively: for any pair of elements in R, there is an element $\sigma \in G$ that sends one to the other. It is easy to check that the subgroups of order 1 or 2 do not have this property. We must therefore have $G = A_R$ or $G = \Sigma_R$. To distinguish between these cases we introduce the element

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

and the element $\Delta = \delta^2$, which is known as the *discriminant* of $f(x)$.

Proposition 12.1. [prop-cubic]

(a) *If $\sigma \in G$ then $\sigma(\delta) = \operatorname{sgn}(\sigma)\delta$, where $\operatorname{sgn}(\sigma)$ denotes the signature of the corresponding permutation.*
(b) *We also have $\Delta \in \mathbb{Q}$, so $\sigma(\Delta) = \Delta$ for all $\sigma \in G$.*
(c) *If $\delta \in \mathbb{Q}$ (or equivalently, Δ is a square in $\mathbb{Q}$) then $G = A_R \simeq C_3$, and $K = \mathbb{Q}(\alpha)$.*
(d) *Suppose instead that $\delta \notin \mathbb{Q}$. Then $G = \Sigma_R$, and $K = \mathbb{Q}(\delta, \alpha)$, and $K^{A_R} = \mathbb{Q}(\delta)$.*

Proof. (a) Suppose that σ acts on R as the transposition $(\alpha\ \beta)$. We then have

$$\sigma(\delta) = \sigma((\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)) = (\beta-\alpha)(\alpha-\gamma)(\gamma-\beta) = -(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha) = -\delta.$$

Similarly, if $\sigma = (\beta\ \gamma)$ or $\sigma = (\gamma\ \alpha)$ we see that $\sigma(\delta) = -\delta$. Now suppose instead that σ acts as the 3-cycle $(\alpha\ \beta\ \gamma)$. We then have

$$\sigma(\delta) = (\beta-\gamma)(\gamma-\alpha)(\alpha-\beta) = \delta.$$

If $\sigma = (\gamma\ \beta\ \alpha)$ we also have $\sigma(\delta) = \delta$, by a very similar argument. This covers all possible permutations (except for the identity, which is trivial) and so proves claim (a).

(b) For all $\sigma \in G$ we have $\sigma(\delta) = \pm\delta$, and so $\sigma(\Delta) = \sigma(\delta^2) = \sigma(\delta)^2 = (\pm\delta)^2 = \delta^2 = \Delta$. This proves that $\Delta \in K^G$, which is just $\mathbb{Q}$ by Theorem 11.1.

(c) Suppose that $\delta \in \mathbb{Q}$. It follows that for all $\sigma \in G = G(K/\mathbb{Q})$ we must have $\sigma(\delta) = \delta$, which is only consistent with (a) if $G \subseteq A_R$. We also saw previously (using transitivity) that G must either be A_R or Σ_R, so now we see that $G = A_R$. In particular we have $|G| = 3$ and so $[K : \mathbb{Q}] = 3$, but as $f(x)$ is irreducible we also have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, so it must be that $K = \mathbb{Q}(\alpha)$.

(d) Suppose instead that $\delta \notin \mathbb{Q} = K^G$, so there must exist $\sigma \in G$ with $\sigma(\delta) \neq \delta$. We then see from (a) that σ gives an odd permutation of R, and that $\sigma(\delta) = -\delta$. This means that we cannot have $G = A_R$, so we must have $G = \Sigma_R$ instead. This means in particular that $[K : \mathbb{Q}] = |G| = 6$. Consider the field $K' = \mathbb{Q}(\delta, \alpha) \subseteq K$. We then see that $[K' : \mathbb{Q}]$ divides $[K : \mathbb{Q}] = 6$, so $[K' : \mathbb{Q}] \in \{1, 2, 3, 6\}$. On the other hand, as $\mathbb{Q} \subseteq \mathbb{Q}(\delta) \subseteq K'$ and $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K'$ we see that $[K' : \mathbb{Q}]$ is divisible by both $[\mathbb{Q}(\delta) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. It follows that $[K' : \mathbb{Q}] = 6$, and thus that $K' = K$. It is also clear from (a) that $\mathbb{Q}(\delta) \subseteq K^{A_R}$ and $[K^{A_R} : \mathbb{Q}] = |G/A_R| = |\Sigma_R/A_R| = 2 = [\mathbb{Q}(\delta) : \mathbb{Q}]$ so $K^{A_R} = \mathbb{Q}(\delta)$ as claimed.

□

We will now explore the Galois correspondence in the case where $G(K/\mathbb{Q}) = \Sigma_R$. Put

$$A = \{1, (\beta\ \gamma)\} \qquad B = \{1, (\gamma\ \alpha)\} \qquad C = \{1, (\alpha\ \beta)\}$$

The lattice of subgroups is then as shown on the left below, and the corresponding lattice of subfields is as shown on the right.

$$\begin{tikzcd}
1 & & \{1\} \arrow[ddl] \arrow[d] \arrow[dr] \arrow[drr] & & & & K & & \\
2 & & A \arrow[dd] & B \arrow[ddl] & C \arrow[ddll] & & \mathbb{Q}(\alpha) \arrow[u] & \mathbb{Q}(\beta) \arrow[ul] & \mathbb{Q}(\gamma) \arrow[ull] \\
3 & C_3 \arrow[dr] & & & & \mathbb{Q}(\delta) \arrow[uur] & & & \\
6 & & \Sigma_3 & & & & \mathbb{Q} \arrow[ul] \arrow[uu] \arrow[uur] \arrow[uurr] & &
\end{tikzcd}$$

Remark 12.2. [rem-disc-formula]
One can in fact show that

$$\begin{aligned}\Delta(\alpha,\beta,\gamma) &= a^2b^2-4a^3c-4b^3+18abc-27c^2\\ &= -\det\begin{bmatrix}1&0&3&0&0\\ a&1&2a&3&0\\ b&a&b&2a&3\\ c&b&0&b&2a\\ 0&c&0&0&b\end{bmatrix}.\end{aligned}$$

It would be long, but essentially straightforward, to check this by hand. Alternatively, one can just enter the following in Maple:

```
a :=  - alpha - beta - gamma;
b := alpha * beta + beta * gamma + gamma * alpha;
c := - alpha * beta * gamma;
delta := (alpha-beta) * (beta - gamma) * (gamma - alpha);
M := <<1|0|3|0|0>,<a|1|2*a|3|0>,<b|a|b|2*a|3>,<c|b|0|b|2*a>,<0|c|0|0|b>>;
expand(delta^2 - (a^2*b^2-4*a^3*c-4*b^3+18*a*b*c-27*c^2));
expand(LinearAlgebra[Determinant](M) + delta^2);
```

There is also a more conceptual argument using the determinant formula, which we will not explain here, except to mention that the first two columns contain the coefficients of $f(t)$ and the last three columns contain the coefficients of $f'(t)$. The determinant formula can be generalised to cover polynomials of any degree, not just cubics.

Remark 12.3. In the case where $a=0$, the formula reduces to $\Delta=-4b^3-27c^2$. One can always reduce to this case: if $f(x)=x^3+ax^2+bx+c$, then $f(x-a/3)=x^3+Bx+C$, where $B=b-a^2/3$ and $C=2a^3/27-ab/3+c$.

We next explain how to find the roots α, β and γ in terms of the coefficients of $f(x)$. Traditionally this is usually done by starting with some preliminary steps that simplify the algebra but obscure some of the symmetry. Here we will assume that the algebra can be handled by a system such as Maple or Mathematica, so we will bypass these preliminary steps.

First, we define $\Delta=a^2b^2-4a^3c-4b^3+18abc-27c^2$. If this is zero then $f(x)$ must be reducible, and so must have a root in $\mathbb{Q}$. We will ignore this case from now on, and assume that $\Delta\neq 0$. We will also assume for the moment that $b\neq a^2/3$; the significance of this will appear later.

Let δ be one of the square roots of Δ. For definiteness, we choose $\delta>0$ if $\Delta>0$, and we take δ to be a positive multiple of i if $\Delta<0$. Then put

$$\begin{aligned}m&=(9ab-2a^3-27c+3\sqrt{-3}\delta)/2\\ n&=(9ab-2a^3-27c-3\sqrt{-3}\delta)/2.\end{aligned}$$

We find (with computer assistance if necessary) that

$$\begin{aligned}m+n&=9ab-2a^3-27c\\ mn&=((9ab-2a^3-27c)^2+27\Delta)/4=(a^2-3b)^3.\end{aligned}$$

In particular, as we have assumed that $b\neq a^2/3$ we see that $mn\neq 0$ and so $m,n\neq 0$. Now let μ be any cube root of m. (If $\Delta>0$ then m lies in the upper half plane and we can take μ to be the unique cube root with $0<\arg(\mu)<\pi/3$; if $\Delta<0$ then m is real and we can take μ to be the unique real cube root of m.) Now put $\nu=(a^2-3b)/\mu$ and observe (using the above formula for mn) that ν is a cube root of n. We now have

$$\begin{aligned}\mu^3+\nu^3&=9ab-2a^3-27c\\ \mu\nu&=a^2-3b.\end{aligned}$$

Now consider the number $\omega = e^{2\pi i/3} = (\sqrt{3}i - 1)/2$, so that $\omega^3 = 1$ and $\omega^2 = \overline{\omega} = \omega^{-1} = -1 - \omega$. It is easy to check that the above equations will still hold if we replace (μ, ν) by $(\omega\mu, \overline{\omega}\nu)$ or $(\overline{\omega}\mu, \omega\nu)$. Finally, we put

$$\begin{aligned}\alpha &= (\mu + \nu - a)/3 \\ \beta &= (\omega\mu + \overline{\omega}\nu - a)/3 \\ \gamma &= (\overline{\omega}\mu + \omega\nu - a)/3.\end{aligned}$$

We claim that these are the roots of $f(x)$. To see this, we note by direct expansion that

$$f(\alpha) = f((\mu + \nu - a)/3) = (\mu^3 + \nu^3 + 2a^3 - 9ab + 27c)/27 + (\mu\nu + 3b - a^2)(\mu + \nu)/9.$$

However, we saw above that $\mu^3 + \nu^3 + 2a^3 - 9ab + 27c = 0$ and $\mu\nu + 3b - a^2 = 0$, so it follows that $f(\alpha) = 0$. We can now replace (μ, ν) by $(\omega\mu, \overline{\omega}\nu)$ and argue in the same way to see that $f(\beta) = 0$, and similarly $f(\gamma) = 0$. If we can show that α, β and γ are distinct, it will follow from Proposition 4.29 that $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$ as expected.

To check for distinctness, first note that $\mu^3 - \nu^3 = m - n = 3\sqrt{-3}\delta \neq 0$, which implies that $\mu \neq \nu$, so $\mu - \nu \neq 0$. We also have

$$\beta - \gamma = (\omega - \overline{\omega})(\mu - \nu)/3 = \sqrt{-3}(\mu - \nu)/3 \neq 0,$$

so $\beta \neq \gamma$. One can show that $\alpha \neq \beta$ and $\alpha \neq \gamma$ in a similar way.

This completes our discussion of the general case where $b \neq a^2/3$. We conclude by discussing briefly the special case where $b = a^2/3$. Here we find that $\Delta = -(a^3 - 27c)^2/27$, so $\delta = \pm(a^3 - 27c)/(3\sqrt{-3})$. We also have $mn = 0$, so either m or n is zero. On the other hand, we have $m - n = 3\sqrt{-3}\delta \neq 0$, so m and n are not both zero. If $m \neq 0$ then we proceed exactly as before, noting that $\nu = (a^2 - 3b)/\mu = 0$. If $m = 0$ then we instead define ν to be the standard cube root of n and put $\mu = 0$, and then the rest of the argument works as previously.

Exercises

Exercise 12.1. [`ex-classify-cubics`]
Show that the cubics $g_0(x) = x^3 - 3x + 1$ and $g_1(x) = x^3 + 3x + 1$ are irreducible, and find their Galois groups.

Exercise 12.2. [`ex-cyclic-cubic`]
Let q be a rational number, and put $r = 1 + q + q^2$. Consider the polynomials

$$\begin{aligned}f(x) &= x^3 - (3x - 2q - 1)r \\ g(x) &= x^3 + 3qx^2 - 3(q + 1)x - (4q^3 + 6q^2 + 6q + 1) \\ s(x) &= x^2 + qx - 2r.\end{aligned}$$

Check (with assistance from Maple if necessary) that $f(s(x)) = f(x)g(x)$. For the rest of the exercise we will assume that q has been chosen so that $f(x)$ is irreducible.

Now suppose we have a field L and an element $\alpha \in L$ with $f(\alpha) = 0$. Show that $s(\alpha)$ is also a root of $f(x)$ in $\mathbb{Q}(\alpha)$, and is different from α. Deduce that $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$ over $\mathbb{Q}$, and that $G(\mathbb{Q}(\alpha)/\mathbb{Q})$ is cyclic of order 3.

Exercise 12.3. [`ex-inv-sq-sum`]
Suppose that the polynomial $f(x) = x^3 + ux^2 + vx + w$ hs three distinct roots, namely α, β and γ. Give a formula for

$$p = \frac{1}{\alpha^2} + \frac{1}{\beta^2} + \frac{1}{\gamma^2}$$

in terms of u, v and w.

Exercise 12.4. [ex-vandermonde]
Suppose $f(x) = x^3 + ax + b$. If f has roots α, β and γ, then recall that its discriminant $\Delta(f)$ is $(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$. Let M denote the matrix

$$M = \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}.$$

(a) Define $\delta(f) = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$. Show that $\delta(f) = \det(M)$.
(b) Thus $\Delta(f) = \delta(f)^2$. Given that $\det(M) = \det(M^T)$, deduce that $\Delta(f) = \det(MM^T)$.
(c) Write $S_i = \alpha^i + \beta^i + \gamma^i$. Show that

$$MM^T = \begin{pmatrix} S_0 & S_1 & S_2 \\ S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{pmatrix}.$$

(d) Clearly $S_0 = 3$ and $S_1 = 0$ (as S_1 is the sum of the roots, which is zero as the coefficient of x^2 in f is zero). Show that $S_2 = -2a$ by an explicit computation.
(e) As α, β and γ are roots of f, we have

$$\alpha^3 + a\alpha + b = 0$$
$$\beta^3 + a\beta + b = 0$$
$$\gamma^3 + a\gamma + b = 0.$$

By summing these three, find S_3 in terms of S_0 and S_1. Similarly, multiplying these equations by α, β and γ respectively, find S_4 in terms of S_1 and S_2. Compute the values of S_3 and S_4 in terms of a and b.
(f) Combining all the above, show that $\Delta(f) = -(4a^3 + 27b^2)$.

13. Quartics

Let $f(x)$ be an irreducible quartic over $\mathbb{Q}$, with roots $R = \{\alpha, \beta, \gamma, \delta\}$ say. Let $K = \mathbb{Q}(\alpha, \beta, \gamma, \delta)$ be the splitting field, and let $G = G(K/\mathbb{Q})$ be the Galois group. This is then a transitive subgroup of Σ_R. Our first task will be to classify such subgroups.

First note that $|\Sigma_R| = 4! = 24$. The elements can be listed as follows.

- The identity element has order 1.
- There are six transpositions ($(\alpha;\beta)$, $(\alpha\ \gamma)$, $(\alpha\ \delta)$, $(\beta\ \gamma)$, $(\beta\ \delta)$ and $(\gamma\ \delta)$), each of order 2.
- There are three transposition pairs, which again have order 2:

$$\tau_1 = (\alpha\ \beta)(\gamma\ \delta)$$
$$\tau_2 = (\alpha\ \gamma)(\beta\ \delta)$$
$$\tau_3 = (\alpha\ \delta)(\beta\ \gamma).$$

- There are eight three-cycles, each of order three.
- There are six four-cycles, each of order 4.

One crucial fact is as follows:

Proposition 13.1. [prop-vier]
The set $V = \{1, \tau_1, \tau_2, \tau_3\}$ is a normal subgroup of Σ_R, isomorphic to $C_2 \times C_2$. It is also transitive. For each $\sigma \in \Sigma_R$ there is a unique permutation $\overline{\sigma} \in \Sigma_3$ such that $\sigma\tau_i\sigma^{-1} = \tau_{\overline{\sigma}(i)}$ for all i. Moreover, the rule $\pi(\sigma) = \overline{\sigma}$ defines a surjective homomorphism of groups $\pi\colon \Sigma_R \to \Sigma_3$, with kernel V.

Remark 13.2. [rem-resolvent]
This connection between Σ_R and Σ_3 allows us to relate cubics to quartics. More precisely, we will later write down a cubic polynomial $h(x) \in \mathbb{Q}[x]$ (called the *resolvent cubic* of $f(x)$) such that $K^{G\cap V}$ is a splitting field for $h(x)$. The full field K can then be obtained by adjoining at most two square roots to $K^{G\cap V}$.

Before the proof, we will give a sample calculation with π. Consider the three-cycle $\sigma = (\alpha\ \beta\ \gamma)$, so $\sigma^{-1} = (\gamma\ \beta\ \alpha)$. We have

$$\begin{aligned}
\sigma\tau_1\sigma^{-1} &= (\alpha\ \beta\ \gamma)(\alpha\ \beta)(\gamma\ \delta)(\gamma\ \beta\ \alpha) = (\alpha\ \delta)(\beta\ \gamma) = \tau_3 \\
\sigma\tau_2\sigma^{-1} &= (\alpha\ \beta\ \gamma)(\alpha\ \gamma)(\beta\ \delta)(\gamma\ \beta\ \alpha) = (\alpha\ \beta)(\gamma\ \delta) = \tau_1 \\
\sigma\tau_3\sigma^{-1} &= (\alpha\ \beta\ \gamma)(\alpha\ \delta)(\beta\ \gamma)(\gamma\ \beta\ \alpha) = (\alpha\ \gamma)(\beta\ \delta) = \tau_2.
\end{aligned}$$

The first line shows that $\overline{\sigma}(1) = 3$, the second that $\overline{\sigma}(2) = 1$, and the third that $\overline{\sigma}(3) = 2$. It follows that $\overline{\sigma} = (1\ 3\ 2) \in \Sigma_3$.

Proof of Proposition 13.1. One can check directly that $\tau_i^2 = 1$ for all i and

$$\begin{aligned}
\tau_1\tau_2 &= \tau_2\tau_1 = \tau_3 \\
\tau_2\tau_3 &= \tau_3\tau_2 = \tau_1 \\
\tau_3\tau_1 &= \tau_1\tau_3 = \tau_2.
\end{aligned}$$

(More succinctly, the product of any two τ's is the third one.) This shows that V is a subgroup of Σ_R. The subgroups generated by τ_1 and τ_2 are cyclic of order 2, and V is the direct product of these subgroups, so $V \simeq C_2 \times C_2$.

Next, recall that any conjugate of a transposition pair is another transposition pair. More precisely, for any $\sigma \in \Sigma_R$ and any transposition pair $(\kappa\ \lambda)(\mu\ \nu)$ we have

$$\sigma(\kappa\ \lambda)(\mu\ \nu)\sigma^{-1} = (\sigma(\kappa)\ \sigma(\lambda))(\sigma(\mu)\ \sigma(\nu)).$$

As τ_1, τ_2 and τ_3 are the only transposition pairs, we must have $\sigma\tau_i\sigma^{-1} = \tau_j$ for some j. We define $\overline{\sigma}(i)$ to be this j, so $\sigma\tau_i\sigma^{-1} = \tau_{\overline{\sigma}(j)}$. Now if we have another permutation ρ we find that

$$\tau_{\overline{\rho\sigma}(i)} = \rho\sigma\tau_i(\rho\sigma)^{-1} = \rho\sigma\tau_i\sigma^{-1}\rho^{-1} = \rho\tau_{\overline{\sigma}(i)}\rho^{-1} = \tau_{\overline{\rho}(\overline{\sigma}(i))},$$

so $\overline{\rho\sigma} = \overline{\rho}\circ\overline{\sigma}$. In particular, we can take $\rho = \sigma^{-1}$ and we find that $\overline{\rho}$ is an inverse for $\overline{\sigma}$, so $\overline{\sigma}$ is a permutation of $\{1, 2, 3\}$. In particular, we see from this that $\sigma V \sigma^{-1} = V$, so V is a normal subgroup of Σ_R. We can now define $\pi\colon \Sigma_R \to \Sigma_3$ by $\pi(\sigma) = \overline{\sigma}$, and the relation $\overline{\rho\sigma} = \overline{\rho}\circ\overline{\sigma}$ tells us that this is a homomorphism.

Note that V is commutative, so if $\sigma \in V$ then $\sigma\tau_i\sigma^{-1} = \tau_i\sigma\sigma^{-1} = \tau_i$, so $\overline{\sigma}$ is the identity. We therefore have $V \leq \ker(\pi)$.

Next, using the formula above for conjugating transposition pairs, we find that

$$\begin{aligned}
(\beta\ \gamma)\tau_1(\beta\ \gamma)^{-1} &= \tau_2 & \qquad (\gamma\ \delta)\tau_1(\gamma\ \delta)^{-1} &= \tau_1 \\
(\beta\ \gamma)\tau_2(\beta\ \gamma)^{-1} &= \tau_1 & \qquad (\gamma\ \delta)\tau_2(\gamma\ \delta)^{-1} &= \tau_3 \\
(\beta\ \gamma)\tau_3(\beta\ \gamma)^{-1} &= \tau_3 & \qquad (\gamma\ \delta)\tau_3(\gamma\ \delta)^{-1} &= \tau_2,
\end{aligned}$$

so $\pi((\beta\ \gamma)) = (1\ 2)$ and $\pi((\gamma\ \delta)) = (2\ 3)$. Thus, the image of π is a subgroup of Σ_3 containing $(1\ 2)$ and $(2\ 3)$, but it is straightforward to check that the only such subgroup is Σ_3 itself, so π is surjective. The First Isomorphism Theorem for groups then gives $\Sigma_R/\ker(\pi) \simeq \Sigma_3$, so $|\ker(\pi)| = |\Sigma_R|/|\Sigma_3| = 24/6 = 4$. On the other hand, we also have $V \leq \ker(\pi)$ and $|V| = 4$. We must therefore have $\ker(\pi) = V$ as claimed. □

We next explain in more detail the Galois-theoretic significance of V and π. We put

$$\begin{aligned}
\mu_1 &= \tfrac{1}{2}((\alpha+\beta) - (\gamma+\delta)) & \qquad \lambda_1 &= \mu_1^2 \\
\mu_2 &= \tfrac{1}{2}((\alpha+\gamma) - (\beta+\delta)) & \qquad \lambda_2 &= \mu_2^2 \\
\mu_3 &= \tfrac{1}{2}((\alpha+\delta) - (\beta+\gamma)) & \qquad \lambda_3 &= \mu_3^2 \\
K_0 &= \mathbb{Q}(\lambda_1, \lambda_2, \lambda_3) \subseteq K.
\end{aligned}$$

The factor of $1/2$ is included for later convenience. Note that $\mu_1 + \mu_2 = \alpha - \delta$ and $\mu_1 - \mu_2 = \beta - \gamma$. These are nonzero so $\mu_1 \neq \pm\mu_2$, so $\lambda_1 \neq \lambda_2$. We can do the same for $\mu_1 \pm \mu_3$ and $\mu_2 \pm \mu_3$ so we find that all the numbers $\pm\mu_i$ are distinct, and all the numbers λ_i are distinct.

Because the roots are grouped in μ_i the same way that they are in τ_i, we find that

$$\sigma(\mu_i) = \pm\mu_{\overline{\sigma}(i)} \qquad\qquad \sigma(\lambda_i) = \lambda_{\overline{\sigma}(i)}$$

for all $\sigma \in G$ and $i \in \{1,2,3\}$. It follows that $\sigma|_{K_0} = 1_{K_0}$ iff $\overline{\sigma} = 1$ iff $\sigma \in V \cap G$. This means that $V \cap G = G(K/K_0)$ and so (by the Galois Correspondence) $K_0 = K^{V \cap G}$. As $V \cap G$ is normal in G we deduce that K_0 is a Galois extension of $\mathbb{Q}$ with Galois group $G/(V \cap G) \simeq \pi(G) \leq \Sigma_3$, and also K is Galois over K_0 with Galois group $V \cap G$.

To understand the extension $K_0/\mathbb{Q}$ in more detail, consider the polynomial

$$\begin{aligned} g(x) &= (x-\lambda_1)(x-\lambda_2)(x-\lambda_3) \\ &= x^3 - (\lambda_1+\lambda_2+\lambda_3)x^2 + (\lambda_1\lambda_2+\lambda_2\lambda_3+\lambda_3\lambda_1)x - \lambda_1\lambda_2\lambda_3. \end{aligned}$$

As G permutes the elements λ_i and the coefficients of g are symmetric in these elements, we see that these coefficients lie in $K^G = \mathbb{Q}$, so $g(x) \in \mathbb{Q}[x]$. Thus $g(x)$ is a cubic over $\mathbb{Q}$ (called the *resolvent cubic* for $f(x)$) and K_0 is a splitting field for $g(x)$. Later we will give formulae for the coefficients of $g(x)$ in terms of the coefficients of $f(x)$. Once we know $g(x)$ we can find the roots λ_i by the methods of Section 12. We can then find $\mu_i = \pm\sqrt{\lambda_i}$. We also note that the element $a = -(\alpha+\beta+\gamma+\delta)$ is just the coefficient of x^3 in $f(x)$, so we can find the roots of $f(x)$ by the formulae

$$\begin{aligned} \alpha &= (+\mu_1+\mu_2+\mu_3)/2 - a/4 \\ \beta &= (+\mu_1-\mu_2-\mu_3)/2 - a/4 \\ \gamma &= (-\mu_1+\mu_2-\mu_3)/2 - a/4 \\ \delta &= (-\mu_1-\mu_2+\mu_3)/2 - a/4. \end{aligned}$$

The only issue here is to control the signs of the elements $\mu_i = \pm\sqrt{\lambda_i}$. Suppose that

$$f(x) = (x-\alpha)(x-\beta)(x-\gamma)(x-\delta) = x^4 + ax^3 + bx^2 + cx + d,$$

so that

$$\begin{aligned} a &= -(\alpha+\beta+\gamma+\delta) \\ b &= \alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta \\ c &= -(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta) \\ d &= \alpha\beta\gamma\delta. \end{aligned}$$

One can check directly (perhaps with assistance from Maple) that

$$\mu_1\mu_2\mu_3 = (4ab - a^3 - 8c)/8.$$

When solving the quartic, one can choose the signs of μ_1 and μ_2 arbitrarily, but one should then define μ_3 to be $(4ab - a^3 - 8c)/(8\mu_1\mu_2)$ so that the above identity holds. It then works out that μ_3 is a square root of λ_3, and the roots of $f(x)$ can be found by the formulae displayed above.

The formulae simplify considerably if we assume that $f(x)$ has no term in x^3, so $\alpha+\beta+\gamma+\delta = 0$. This does not really lose any generality: if $f(x) = x^4 + ax^3 + bx^2 + cx + d$ then one can check that the polynomial $f(x - a/4)$ has no term in x^3, and if we know the roots of $f(x - a/4)$ we can just subtract $a/3$ to get the roots of $f(x)$.

If $\alpha+\beta+\gamma+\delta = 0$ then we find that

$$\begin{aligned} \mu_1 &= \alpha+\beta & -\mu_1 &= \gamma+\delta & \lambda_1 &= (\alpha+\beta)^2 = (\gamma+\delta)^2 \\ \mu_2 &= \alpha+\gamma & -\mu_2 &= \beta+\delta & \lambda_2 &= (\alpha+\gamma)^2 = (\beta+\delta)^2 \\ \mu_3 &= \alpha+\delta & -\mu_3 &= \beta+\gamma & \lambda_3 &= (\alpha+\delta)^2 = (\beta+\gamma)^2 \end{aligned}$$

It follows that $\mu_1\mu_2\mu_3 = -c$. We can now expand out the definition of $g(x)$ to obtain the following result:

Proposition 13.3. [prop-resolvent]
For a quartic polynomial of the form $f(x) = x^4 + bx^2 + cx + d$, the resolvent cubic is given by

$$g(x) = x^3 + 2bx^2 + b^2x - 4dx - c^2. \quad \square$$

We now continue our investigation of which subgroups of Σ_R can appear as Galois groups.

Proposition 13.4. [prop-vier-converse]
Suppose that H is a transitive subgroup of Σ_R such that $|H| = 4$, and that H contains no elements of order 4. Then $H = V$.

Proof. Suppose that $\sigma \in H$ with $\sigma \neq 1$. By Lagrange's Theorem the order of σ must divide $|H| = 4$, but by assumption the order is not equal to 4, so the order must be two. This means that σ is either a transposition or a transposition pair. Suppose that σ is a transposition; then there exists a root λ with $\sigma(\lambda) = \lambda$. Put $K = \mathrm{stab}_H(\lambda) = \{\rho \in H \mid \rho(\lambda) = \lambda\}$, so $\{1, \sigma\} \subseteq K$, so $|K| > 1$, so $|H|/|K| < 4$. However, the Orbit-Stabiliser Theorem tells us that $|H\lambda| = |H|/|K|$, so $|H\lambda| < 4$, so $H\lambda \neq R$. This contradicts the assumption that H is transitive. It follows that all nontrivial elements of H must actually be transposition pairs, but there are only three transposition pairs in Σ_R, so all of them must be in H, so $H = V$. $\square$

Definition 13.5. [defn-Qi]
For $i \in \{1, 2, 3\}$ we put $Q_i = \{\sigma \in \Sigma_R \mid \overline{\sigma}(i) = i\}$.

Proposition 13.6. [prop-dihedral]
Q_i is a dihedral group of order 8, and is transitive. Moreover, these are the only subgroups of order 8 in Σ_R.

Proof. We first consider Q_2. Let ρ be the four-cycle $(\alpha\ \beta\ \gamma\ \delta)$. Note that $\rho^2 = (\alpha\ \gamma)(\beta\ \delta) = \tau_2$, so $\rho\tau_2\rho^{-1} = \tau_2$, so $\overline{\rho}(2) = 2$, so $\rho \in Q_2$. On the other hand, we have

$$\rho\tau_1\rho^{-1} = (\rho(\alpha)\ \rho(\beta))(\rho(\gamma)\ \rho(\delta)) = (\beta\ \gamma)(\delta\ \alpha) = \tau_3$$
$$\rho\tau_3\rho^{-1} = (\rho(\alpha)\ \rho(\delta))(\rho(\beta)\ \rho(\gamma)) = (\beta\ \alpha)(\gamma\ \delta) = \tau_1,$$

so $\overline{\rho} = (1\ 3)$. If $\sigma \in Q_2$ then $\overline{\sigma}$ must either be the identity or $(1\ 3)$. If $\overline{\sigma} = 1$ then $\sigma \in \ker(\pi) = V$. If $\overline{\sigma} = (1\ 3) = \overline{\rho}$ then we find that $\sigma\rho^{-1} \in \ker(\pi) = V$, so $\sigma \in V\rho$. It follows that $Q_2 = V \amalg V\rho$, which has order 8. One can also check that $\tau_1\rho\tau_1^{-1} = \rho^{-1}$, which mean that τ_1 and ρ generate a group isomorphic to D_8, which must be all of Q_2. As V is transitive and $V \leq Q_2$ we also see that Q_2 is transitive. One can show in the same way that Q_1 and Q_3 are also transitive and isomorphic to D_8.

Now let H be an arbitrary subgroup of Σ_R with $|H| = 8$. We then have subgroups $\pi(H) \leq \Sigma_3$ and $H \cap V = \ker(\pi\colon H \to \pi(H)) \leq V$, and the First Isomorphism Theorem tells us that $|H \cap V||\pi(H)| = |H| = 8$. Here $|H \cap V|$ must divide $|V| = 4$ and $|\pi(H)|$ must divide $|\Sigma_3| = 6$. The only possibility is $|\pi(H)| = 2$ and $|H \cap V| = 4 = |V|$. This means that $H \cap V = V$ (or in other words, that $V \leq H$) and that $\pi(H) = \{1, \sigma\}$ for some transposition $\sigma \in \Sigma_3$. If $\sigma = (1\ 2)$ we see that $H \leq Q_3$, but $|H| = 8 = |Q_3|$ so $H = Q_3$. Similarly, if $\sigma = (1\ 3)$ then $H = Q_2$, and if $\sigma = (2\ 3)$ then $H = Q_1$. $\square$

One can check directly that in any group isomorphic to D_8 there is a unique cyclic subgroup of order 4. We can thus do the following:

Definition 13.7. [defn-Pi]
We write P_i for the unique cyclic subgroup of order 4 in Q_i.

Proposition 13.8. [prop-C-four]
The groups P_i are all different, and they are the only cyclic subgroups of order 4 in Σ_R.

Proof. First, we have $Q_i = P_iV$, and the subgroups Q_i are all different, so the subgroups P_i are all different. Each P_i contains precisely two elements of order 4 (each inverse to the other). The elements of order 4 are the four-cycles, and there are only six of them in Σ_R. Thus, there cannot be any further cyclic subgroups of order 4. $\square$

Lemma 13.9. [lem-half-normal]
Let G be a finite group, and let H be a subgroup such that $|G| = 2|H|$. Then H is normal in G.

Proof. Put $C = G \setminus H$, so $|C| = |G| - |H| = |H|$. Suppose that $g \in G$; we must show that $gHg^{-1} = H$. If $g \in H$ then this is clear. If $g \notin H$, then the left coset gH is disjoint from H and so is contained in C, but $|gH| = |H| = |C|$ so $gH = C$. Similarly, the right coset Hg is disjoint from H and has the same size as C so it is equal to C. We now have $gH = Hg$ and we can multiply on the right by g^{-1} to get $gHg^{-1} = H$ as required. $\square$

Proposition 13.10. [prop-alternating]
The only subgroup of Σ_R of order 12 is the group A_R of even permutations of R.

Proof. Suppose that $|H| = 12$. By the lemma, we see that H is normal so we have a quotient group $G/H \simeq C_2$ and a quotient homomorphism $q\colon G \to G/H$ with kernel H. Let x denote the nontrivial element of G/H. Recall that all the transpositions in Σ_R are conjugate to each other. Thus, if H contains any transposition then it must contain all of them, but the transpositions generate Σ_R, so $H = \Sigma_R$, contradicting the fact that $|H| = 12$. It follows that for all transpositions σ we have $q(\sigma) = x$. Now if ρ is an even permutation then it can bew written as a product of $2m$ transpositions, say, which gives $q(\rho) = x^{2m} = 1$, so $\rho \in H$. This shows that $A_R \leq H$ but $|A_R| = 12 = |H|$ so $H = A_R$. □

Proposition 13.11. [prop-transitive]
The transitive subgroups of Σ_R are as follows: $V, P_1, P_2, P_3, Q_1, Q_2, Q_3, A_R$ and Σ_R. Thus, the Galois group G must be one of these groups.

Proof. Let H be a transitive subgroup of Σ_R. As H is transitive, the orbit $H\alpha$ is all of R, so $|H\alpha| = 4$. Put $K = \operatorname{stab}_H(\alpha) = \{\sigma \in H \mid \sigma(\alpha) = \alpha\}$. The Orbit-Stabiliser Theorem tells us that $|H\alpha| = |H|/|K|$, so $|H| = 4|K|$, which is divisible by 4. On the other hand, Lagrange's Theorem tells us that $|H|$ divides $|\Sigma_R| = 24$. It follows that $|H| \in \{4, 8, 12, 24\}$. If $|H| = 24$ then clearly $H = \Sigma_R$. If $|H| = 12$ then Proposition 13.10 tells us that $H = A_R$. If $|H| = 8$ then Proposition 13.6 tells us that $H = Q_i$ for some i. If $|H| = 4$ and H contains an element of order 4 then H must be cyclic and Proposition 13.8 tells us that $H = P_i$ for some i. This just leaves the case where $|H| = 4$ but H has no element of order 4, in which case Proposition 13.4 tells us that $H = V$. □

Remark 13.12. [rem-transitive]
The subgroups P_i are all conjugate to each other, so we can convert between them by just renaming the roots. As the naming of the roots is arbitrary, it is not very meaningful to distingush between these subgroups. The same applies to the subgroups Q_i. Thus, we can say that the Galois group is always V, C_4, D_8, A_4 or Σ_4. The inclusions between these subgroups can be displayed as follows:

$$\begin{tikzcd}
 & & \Sigma_4 & \\
 & D_8 \arrow[ur] & & A_4 \arrow[ul] \\
C_4 \arrow[ur] & & V \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Remark 13.13. [rem-irr-resolvent]
Consider a quartic $f(x)$ with resolvent $g(x)$. If the Galois group of $f(x)$ is $H \leq \Sigma_4$, then the Galois group of $g(x)$ is the image of H in $\Sigma_4/V \simeq \Sigma_3$, which we will call $\overline{H}$. If $g(x)$ is irreducible then $\overline{H}$ must be transitive, and so must have order divisible by 3. It follows that $|H|$ must be divisible by 3, and by inspecting the above list of possibilities we see that either $H = A_4$ and $\overline{H} = A_3$, or $H = \Sigma_4$ and $\overline{H} = \Sigma_3$.

Exercises

Exercise 13.1. [ex-classify-quartics]
What are the Galois groups of the quartics $f_0(x) = x^4 + 8x + 12$ and $f_1(x) = x^4 + 8x - 12$?
[*Hint: You may assume that these are irreducible. Exercise 12.1 is relevant.*]

Exercise 13.2. [ex-biquad-quartic]
You are given that a quartic polynomial $f(x)$ has roots as follows:

$$\alpha_0 = \sqrt{2} + \sqrt{5} \qquad \alpha_1 = \sqrt{2} - \sqrt{5} \qquad \alpha_2 = -\sqrt{2} + \sqrt{5} \qquad \alpha_3 = -\sqrt{2} - \sqrt{5}.$$

What is its discriminant? What is the Galois group?

Exercise 13.3. [ex-quartic-discriminant]
Consider an irreducible quartic of the form $f(x) = x^4 + px + q$, with roots $\alpha, \beta, \gamma, \delta$ say. You may assume that the discriminant is $\det(MM^T)$, where M is the 4×4 matrix analogous to the one in Exercise 12.4. Show that this gives $\Delta(f(x)) = 256q^3 - 27p^4$.

14. Cyclic extensions

In this section we will study normal extensions L/K for which the Galois group is cyclic.

Proposition 14.1. [prop-cyclic-ext]
Let K be a field of characteristic zero, and suppose that the polynomial $x^n - 1$ is split in K.

(a) *If L is a normal extension of K and $G(L/K)$ is cyclic of order n, then there exists $\alpha \in K$ and $\beta \in L$ such that $min(\beta, K) = x^n - \alpha$ and $L = K(\beta)$. In other words, we have $L = K(\alpha^{1/n})$.*

(b) *Conversely, if $L = K(\beta)$ for some β with $\beta^n = \alpha \in K$, then L is normal over K and the Galois group $G(L/K)$ is cyclic, with order dividing n. If the polynomial $x^n - \alpha \in K[x]$ is irreducible, then the order is precisely n.*

The proof will follow after some preparatory results.

For K as in the proposition, we see that the group

$$\mu_n = \{a \in K \mid a^n = 1\}$$

has order n. It is also cyclic by Proposition 9.9. We can thus choose a generator $\zeta \in \mu_n$. For $r = 0, 1, \dots, n-1$ we define a K-linear map $\epsilon_r \colon L \to L$ by

$$\epsilon_r(a) = \tfrac{1}{n} \sum_{i=0}^{n-1} \zeta^{-ir} \sigma^i(a).$$

Lemma 14.2. [lem-sg-ep]
For all $a \in L$ we have $\sigma(\epsilon_r(a)) = \zeta^r\, \epsilon_r(a)$.

Proof. We have $\sigma|_K = 1_K$ by assumption and $\zeta \in K$ so $\sigma(\epsilon_r(a)) = n^{-1} \sum_{i=0}^{n-1} \zeta^{-ir} \sigma^{i+1}(a)$. We can rewrite this in terms of the index $j = i + 1$ as

$$\sigma(\epsilon_r(a)) = n^{-1} \sum_{j=1}^{n} \zeta^{r-jr} \sigma^j = \zeta^r \sum_{j=1}^{n} \zeta^{-jr} \sigma^j.$$

Here $\zeta^{rn} = 1 = \zeta^0$ and $\sigma^n = 1 = \sigma^0$ so we can replace the $j = n$ term by the $j = 0$ term to get $\sigma(\epsilon_r(a)) = \zeta^r \sum_{j=0}^{n-1} \zeta^{-rj} \sigma^j(a) = \zeta \epsilon_r(a)$ as claimed. □

Lemma 14.3. [lem-circle-powers]
For any $t \in \mathbb{Z}$ we have

$$\tfrac{1}{n} \sum_{i=0}^{n-1} \zeta^{it} = \begin{cases} 1 & \textit{if } t = 0 \pmod{n} \\ 0 & \textit{if } t \neq 0 \pmod{n}. \end{cases}$$

Proof. If $t = 0 \pmod{n}$ then $\zeta^{it} = 1$ for all i so we just have $n^{-1} \sum_{i=0}^{n-1} 1 = 1$ as claimed. In general, the standard geometric progression argument shows that

$$(\zeta^t - 1) \sum_{i=0}^{n-1} \zeta^{it} = (\zeta^t + \zeta^{2t} + \cdots + \zeta^{nt}) - (1 + \zeta^t + \cdots + \zeta^{(n-1)t}) = \zeta^{nt} - 1 = 0.$$

If $t \neq 0 \pmod{n}$ thn $\zeta^t - 1 \neq 0$ so we can divide by it (and then by n) to see that $n^{-1} \sum_{i=0}^{n-1} \zeta^{it} = 0$ as claimed. □

Proof of Proposition 14.1. (a) L be an extension with cyclic Galois group $G = \{1, \sigma, \dots, \sigma^{n-1}\} \simeq C_n$ as in the last two lemmas. Proposition 6.5 tells us that the map $\epsilon_1 \colon L \to L$ is nonzero. Choose $\lambda \in L$ such that $\phi(\lambda) \neq 0$, and put $\beta = \epsilon_1(\lambda) \in L^\times$. By Lemma 14.2 we have $\sigma(\beta) = \zeta\beta$, so $\sigma(\beta^j) = \sigma(\beta)^j = \zeta^j\beta^j$. From this it follows that

$$\sigma^2(\beta^j) = \sigma(\sigma(\beta^j)) = \sigma(\zeta^j\beta^j) = \zeta^j\sigma(\beta^j) = \zeta^{2j}\beta^j.$$

By continuing in the same way (or, more formally, by induction) we see that $\sigma^i(\beta^j) = \zeta^{ij}\beta^j$ for all $i, j \in \mathbb{Z}$. As $\zeta^n = 1$, it follows that the element $\alpha = \beta^n$ has $\sigma^i(\alpha) = \alpha$ for all i. This means that $\alpha \in L^G$, but $L^G = K$ by the Galois Correspondence, so $\alpha \in K$. We can now put $f(x) = x^n - \alpha \in K[x]$, and we see that $f(\beta) = 0$.

Next, we claim that

$$\epsilon_r(\beta^j) = \begin{cases} \beta^j & \text{if } r = j \pmod{n} \\ 0 & \text{otherwise.} \end{cases}$$

Indeed, from the definition and the fact that $\sigma^i(\beta^j) = \zeta^{ij}\beta^j$ we get

$$\epsilon_r(\beta^j) = n^{-1}\sum_{i=0}^{n-1}\zeta^{-ri}\sigma^i(\beta^j) = \beta^j n^{-1}\sum_{i=0}^{n-1}\zeta^{(j-r)i},$$

so the claim follows from Lemma 14.3.

Next, we claim that the elements $1, \beta, \dots, \beta^{n-1}$ are linearly independent over K. To see this, consider a linear relation $\sum_{i=0}^{n-1} a_i\beta^i = 0$, with $a_i \in K$. We can apply ϵ_r to both sides of this equation. On the right hand side we get zero, and on the left hand side most terms become zero, but we have $\epsilon_r(a_r\beta^r) = a_r\beta^r$. As $\beta \neq 0$ this gives $a_r = 0$, but r was arbitrary so our linear relation is the trivial one. We conclude that the list $1, \beta, \dots, \beta^{n-1}$ is indeed linearly independent, or equivalently that β is not a root of any polynomial in $K[x]$ of degree less than n. Thus, the polynomial $f(x) = x^n - \alpha$ must actually be the minimal polynomial of β over K.

(b) Conversely, suppose we have an extension $L = K(\beta)$ such that the element $\alpha = \beta^n$ lies in K. To avoid trivialities we may assume that $\beta \neq 0$. Choose a generator ζ of the group $\mu_n = \{a \in K \mid a^n = 1\}$. We then see from the cyclotomic theory that $x^n - 1 = \prod_{k=0}^{n-1}(x - \zeta^k)$ and thus that $x^n - \alpha = x^n - \beta^n = \prod_{k=0}^{n-1}(x - \zeta^k\beta)$. In particular we see that L is a splitting field for $x^n - \alpha$ over K, so it is normal over K. Next, for any $\sigma \in G(L/K)$ we put $\lambda(\sigma) = \sigma(\beta)/\beta$. We can then apply σ to the equation $\beta^n = \alpha$ to see that $\sigma(\beta)^n = \alpha$, which implies that $\lambda(\sigma)^n = 1$, so $\lambda(\sigma) \in \mu_n \subseteq K^\times$. We claim that the map $\lambda \colon G(L/K) \to \mu_n$ is actually a group homomorphism. Indeed, if τ is another element of $G(L/K)$ we have $\tau(\lambda(\sigma)) = \lambda(\sigma)$, because $\lambda(\sigma) \in K$. We can therefore apply τ to the equation $\sigma(\beta) = \lambda(\sigma)\beta$ to get $\tau(\sigma(\beta)) = \lambda(\sigma)\tau(\beta) = \lambda(\sigma)\lambda(\tau)\beta$, which rearranges to give $\lambda(\tau\sigma) = \lambda(\tau)\lambda(\sigma)$ as required. Next, we claim that λ is injective. Indeed, if $\lambda(\sigma) = 1$ then $\sigma(\beta)/\beta = 1$ so $\sigma(\beta) = \beta$, so σ acts as the identity on $K(\beta)$, but $K(\beta) = L$, so $\sigma = 1$ as required. It follows that λ gives an isomorphism from $G(L/K)$ to a subgroup of μ_n. We know from Proposition 9.9 that μ_n is cyclic, and it follows that $G(L/K)$ is cyclic as claimed. If $x^n - \alpha$ is irreducible then $G(L/K)$ acts transitively on the set of roots, so for each $\xi \in \mu_n$ we can choose $\sigma \in G(L/K)$ with $\sigma(\beta) = \xi\beta$, so $\lambda(\sigma) = \xi$. In this case we see that λ is also surjective, so it is an isomorphism and therefore $|G(L/K)| = n$.

□

15. Extension by radicals

The roots of a quadratic polynomial $f(x) = x^2 + bx + c$ are of course given by $(-b \pm \sqrt{b^2 - 4c})/2$. To evaluate these, we need the ordinary algebraic operations of addition, subtraction, multiplication and division, and we also need to find a square root. Similarly, to solve a cubic by the method described in Section 12 we need algebraic operations, and we need to extract some square roots and some cube roots. For quartics, we use the same type of operations to solve the resolvent cubic, and then we take some further square roots as part of the process of finding roots of the original equation. More generally, we say that a polynomial $f(x)$ is *solvable by radicals* if all the roots can be found using only algebraic operations and extraction of roots. It turns out that most quintics are *not* solvable by radicals, so there cannot be any general for solving quintics similar to that for quadratics, cubics and quartics. In this section we will develop the theory necessary to prove this.

The main idea is as follows. We will define a property called *solvability* for finite groups. Roughly speaking, a group is solvable if it can be broken up into cyclic groups. Proposition 14.1 tells us that cyclic groups correspond to field extensions generated by taking an n'th root. It follows that for a polynomial $f(x)$, we can find the roots of $f(x)$ by extracting roots if and only if the Galois group of the splitting field is solvable. For a typical polynomial of degree d the Galois group will be Σ_d, and Σ_d is only solvable if $d \leq 4$. Thus, all polynomials of degree less than or equal to four are solvable by radicals, but most polynomials of higher degree are not.

Definition 15.1. [`defn-solvable`]
Let G be a finite group. We say that G is *solvable* if there is a chain of subgroups $\{1\} = G_0 \leq G_1 \leq \cdots \leq G_r = G$ such that G_{i-1} is normal in G_i, and the quotient groups G_i/G_{i-1} are all cyclic. Any such chain is called a *solvable series* for G.

Remark 15.2. [`rem-solvable-defn`]
It is more standard to say that G is solvable if it has a chain as above in which the quotients G_i/G_{i-1} are abelian (not necessarily cyclic). We will see in Corollary 15.13 below that this is equivalent to our definition.

Definition 15.3. [`defn-radical-extension`]
Let K be a field, and let L be an extension of K of finite degree. We say that L is a *radical extension* if there exist elements $\alpha_1, \dots, \alpha_r \in L$ and integers $n_1, \dots, n_r > 0$ such that $L = K(\alpha_1, \dots, \alpha_r)$ and $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$ for all i.

Definition 15.4. [`defn-solvable-poly`]
Let K be a field, and let $f(x)$ be a monic polynomial in $K[x]$. We say that $f(x)$ is *solvable by radicals* if there exists a radical extension L/K such that $f(x)$ splits in $K[x]$.

Theorem 15.5. [`thm-solvable-poly`]
Suppose that K has characteristic zero. Let $f(x)$ be a monic polynomial in $f(x)$, and let N be a splitting field for $f(x)$. Then $f(x)$ is solvable by radicals if and only if the Galois group $G(N/K)$ is solvable.

One half of this will be proved as Proposition 15.15 below, and the converse half as Corollary 15.18. First, however, we will give some examples and preliminary results about solvable groups.

Example 15.6. [`eg-solvable-three`]
Consider the group Σ_3. The alternating subgroup A_3 is cyclic of order 3, and the quotient Σ_3/A_3 is cyclic of order 2. We thus have a series $\{1\} < A_3 < \Sigma_3$ proving that Σ_3 is solvable.

Example 15.7. [`eg-solvable-four`]
Consider the group Σ_4. Put $C = \{1, (1\ 2)(3\ 4)\}$, which is cyclic of order 2. In the notation of Section 13 we then have a series

$$\{1\} < C < V < A_4 < \Sigma_4$$

with $C/\{1\} \simeq V/C \simeq \Sigma_4/A_4 \simeq C_2$ and $A_4/V \simeq C_3$, which shows that Σ_4 is solvable.

Example 15.8. [`eg-An-unsolvable`]
We will show later that Σ_n and A_n are not solvable if $n > 4$.

Example 15.9. [`eg-order-solvable`]
Let G be a group of order n. If n is prime then G is cyclic and therefore solvable. If n is a power of a prime, then G is still solvable. We will not give the proof here but it is a standard exercise in the theory of groups of prime power order. If n involves only two primes, then G is still solvable by a theorem of Burnside which is often covered in advanced undergraduate courses on Representation Theory. More strikingly, if n is odd then G is automatically solvable. This is a famous theorem of Feit and Thompson; the proof takes hundreds of pages and is only accessible to specialists in finite group theory.

Proposition 15.10. [`prop-abelian-solvable`]
Any finite abelian group is solvable.

Proof. Let G be a finite abelian group. Put $G_0 = \{1\} \leq G$. If $G \neq G_0$, we choose an element $a_1 \in G \setminus G_0$, and let G_1 be the subgroup generated by G_0 together with a_1. If $G \neq G_1$, we choose an element $a_2 \in G \setminus G_1$, and let G_2 be the subgroup generated by G_1 together with a_2. Continuing in this way, we get a chain of subgroups

$$\{1\} = G_0 < G_1 < G_2 < \cdots \leq G.$$

As G is finite and G_i is strictly bigger than G_{i-1}, we must eventually reach a stage where $G_r = G$. As everything is abelian, all subgroups are normal, so we can form quotient groups G_i/G_{i-1}. As G_i is generated by G_{i-1} together with a_i, we see that G_i/G_{i-1} is generated by the coset a_iG_{i-1} and so is cyclic. We therefore have a solvable series for G. □

Proposition 15.11. [`prop-subquotient`]
Let G be a finite group, and let H be a normal subgroup. Put $\overline{G} = G/H$ and let $\pi\colon G \to \overline{G}$ be the quotient homomorphism, so $\pi(g) = gH$.

(a) *If K is any subgroup of G such that $H \subseteq K$, then the set $\overline{K} = \pi(K)$ is a subgroup of $\overline{G}$ and is the same as K/H. Moreover, we have $K = \{x \in G \mid \pi(x) \in \overline{K}\}$.*
(b) *Conversely, if $\overline{K}$ is any subgroup of $\overline{G}$ then the set $K = \{x \in G \mid \pi(x) \in \overline{K}\}$ is a subgroup of G containing H, and we have $\overline{K} = \pi(K) = K/H$.*
(c) *If K and $\overline{K}$ are related as above, then K is normal in G if and only if $\overline{K}$ is normal in $\overline{G}$. If so, then there is an isomorphism $G/K \to \overline{G}/\overline{K}$ given by $gK \mapsto \pi(g)\overline{K}$.*

Proof. (a) The identity element 1_G lies in K, so the identity element $1_{\overline{G}} = \pi(1_G)$ lies in $\overline{K}$. Suppose we have elements $\overline{a}, \overline{b} \in \overline{K}$. By the definition of $\overline{K}$, we can choose $a, b \in K$ with $\overline{a} = \pi(a)$ and $\overline{b} = \pi(b)$. As K is a subgroup, we have $ab \in K$ and $a^{-1} \in K$. It follows that $\pi(ab), \pi(a^{-1}) \in \overline{K}$ but $\pi(ab) = \overline{a}\,\overline{b}$ and $\pi(a^{-1}) = \overline{a}^{-1}$, so $\overline{a}\,\overline{b} \in \overline{K}$ and $\overline{a}^{-1} \in \overline{K}$. This proves that $\overline{K}$ is a subgroup of $\overline{G}$. The elements are just the cosets xH for $x \in K$, which are the same as the elements of K/H; so $\overline{K} = K/H$. Now consider the set $K' = \{x \in G \mid \pi(x) \in \overline{K}\}$; we claim that this is the same as K. If $x \in K$ then $\pi(x) \in \overline{K}$ by the definition of $\overline{K}$, so $x \in K'$ by the definition of K'. Thus $K \subseteq K'$. Conversely, suppose that $x \in K'$. Then $\pi(x) \in \overline{K} = \pi(K)$, so $\pi(x) = \pi(y)$ for some $y \in K$. This means that $xH = yH$, so $x = yz$ for some $z \in H$. However, we have $H \subseteq K$ by assumption, so y and z both lie in K, so $x \in K$. This shows that $K' \subseteq K$, so in fact $K' = K$ as claimed.

(b) Now let $\overline{K}$ be an arbitrary subgroup of $\overline{G}$, and put $K = \{x \in G \mid \pi(x) \in \overline{K}\}$. Clearly, if $x \in H$ then $\pi(x) = 1_{\overline{G}} \in \overline{K}$, so $x \in K$. This proves that $H \subseteq K$, so in particular $1 \in K$. Now suppose we have alements $a, b \in K$. This means that the elements $\pi(a)$ and $\pi(b)$ lie in $\overline{K}$, but $\overline{K}$ is a subgroup, so we have $\pi(a)\pi(b) \in \overline{K}$ and $\pi(a)^{-1} \in \overline{K}$. As π is a homomorphism we have $\pi(ab) = \pi(a)\pi(b)$, which lies in $\overline{K}$, so $ab \in K$. Similarly we have $\pi(a^{-1}) = \pi(a)^{-1}$, which lies in $\overline{K}$, so $a^{-1} \in K$. This shows that K is a subgroup of G containing H. From the very definition of K we have $\pi(K) \subseteq \overline{K}$. Conversely, if $u \in \overline{K} \subseteq \overline{G} = G/H$ then we must have $u = xH = \pi(x)$ for some $x \in G$. Now $\pi(x) \in \overline{K}$ so by the definition of K we have $x \in K$. This means that $u \in \pi(K)$. We thus have $\overline{K} \subseteq \pi(K)$, and so $\overline{K} = \pi(K)$ as claimed.

(c) Let K and $\overline{K}$ be related as discussed above. Suppose that K is normal in G. For any $\overline{a} \in \overline{G}$ we can choose $a \in G$ with $\pi(a) = \overline{a}$, and we note that $aKa^{-1} = K$ because K is normal. We thus have

$$\overline{a}\overline{K}\overline{a}^{-1} = \pi(a)\pi(K)\pi(a)^{-1} = \pi(aKa^{-1}) = \pi(K) = \overline{K},$$

which proves that $\overline{K}$ is normal in $\overline{G}$. Conversely, suppose that $\overline{K}$ is normal in $\overline{G}$. Consider an element $a \in G$, and the corresponding subgroup $K' = aKa^{-1} \leq G$. Note that K' contains aHa^{-1}, but $aHa^{-1} = H$ as H is normal. We can thus apply part (a) to K' as well as to K. The last claim in (a) says that $K' = \{x \mid \pi(x) \in \pi(K')\}$, whereas $K = \{x \mid \pi(x) \in \pi(K)\}$. Now $\pi(K') = \pi(a)\overline{K}\pi(a)^{-1}$, but this is just the same as $\overline{K}$, because $\overline{K}$ is assumed to be normal. We thus have $K = K'$, which means that K is normal.

Finally, suppose that K (and thus $\overline{K}$) is normal, and define a homomorphism $\phi\colon G \to \overline{G}/\overline{K}$ by $\phi(x) = \pi(x)\overline{K}$. This is clearly surjective, and we have

$$\begin{aligned}\ker(\phi) &= \{x \in G \mid \pi(x)\overline{K} = \overline{K}\}\\ &= \{x \in G \mid \pi(x) \in \overline{K}\} = K\end{aligned}$$

(where we have again used the last part of (a)). The First Isomorphism Theorem therefore gives us an induced isomorphism $\overline{\phi}\colon G/K = G/\ker(\phi) \to \overline{G}/\overline{K}$, as claimed.

□

Proposition 15.12. [prop-solvable-layers]
Let G be a finite group.

(a) *If G is solvable then every subgroup of G is solvable.*
(b) *If G is solvable, then for every normal subgroup $H \leq G$, the quotient G/H is also solvable.*
(c) *If G has a normal subgroup H such that both H and G/H are solvable, then G is solvable.*

Proof. (a) Suppose that G is solvable, so we have a solvable series $G_0 \leq \cdots \leq G_r$ as in the definition. Let H be a subgroup of G. Put $H_i = H \cap G_i$, which is a subgroup of H. Note that $H_0 = H \cap \{1\} = \{1\}$ and $H_r = H \cap G = H$. We can define a homomorphism $\pi_i\colon H_i \to G_i/G_{i-1}$ by $\pi_i(x) = xG_{i-1}$. The kernel of this is the set of elements in H_i that also lie in G_{i-1}, so

$$\ker(\pi_i) = H_i \cap G_{i-1} = H \cap G_i \cap G_{i-1} = H \cap G_{i-1} = H_{i-1}.$$

Thus, the First Isomorphism Theorem tells us that H_{i-1} is normal in H_i and that H_i/H_{i-1} is isomorphic to $\pi_i(H_i)$. This is a subgroup of the cyclic group G_i/G_{i-1}, so is itself cyclic. Thus, the subgroups H_i form a solvable series for H.

(b) Now suppose that H is normal, so we have a quotient group $\overline{G} = G/H$ and a quotient homomorphism $\pi\colon G \to \overline{G}$ given by $\pi(g) = gH$. Put $\overline{G}_i = \pi(G_i)$, which is a subgroup of $\overline{G}$. Note that $\overline{G}_0 = \pi(\{1\}) = \{1\}$ and $\overline{G}_r = \pi(G) = \overline{G}$. As $G_{i-1} \subseteq G_i$ we have $\overline{G}_{i-1} \subseteq \overline{G}_i$. We next claim that $\overline{G}_{i-1}$ is normal in $\overline{G}_i$. Indeed, if $a \in \overline{G}_i$ and $b \in \overline{G}_{i-1}$ then we must have $a = \pi(x)$ and $b = \pi(y)$ for some $x \in G_i$ and $y \in G_{i-1}$. This means that $aba^{-1} = \pi(xyx^{-1})$, but G_{i-1} is normal in G_i, so $xyx^{-1} \in G_{i-1}$, so $aba^{-1} \in \pi(G_{i-1}) = \overline{G}_{i-1}$ as claimed. Finally, we claim that $\overline{G}_i/\overline{G}_{i-1}$ is cyclic. To see this, choose $x \in H_i$ such that xH_{i-1} generates the cyclic group H_i/H_{i-1}, and put $a = \pi(x)\overline{G}_{i-1} \in \overline{G}_i/\overline{G}_{i-1}$. Any other element $b \in \overline{G}_i/\overline{G}_{i-1}$ has the form $b = \pi(y)\overline{G}_{i-1}$ for some $y \in H_i$. By our choice of x we have $y = x^i z$ for some $i \in \mathbb{Z}$ and $z \in H_{i-1}$, and it follows that $b = a^i$, as required. We have thus constructed a solvable series for $\overline{G}$.

(c) Now suppose instead that G is a finite group with a normal subgroup H, and that both H and the quotient group $\overline{G} = G/H$ are solvable. Let $\pi\colon G \to \overline{G}$ be the quotient map. Choose solvable series

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

$$\{1\} = \overline{G}_0 \leq \overline{G}_1 \leq \cdots \leq \overline{G}_s = \overline{G}.$$

For $1 \leq j \leq s$ we put $H_{r+j} = \{x \in G \mid \pi(x) \in \overline{G}_j\}$. (For $j = 0$ the group H_{r+j} is already defined and is equal to H, and in this case it is still true that $H_{r+j} = \{x \in G \mid \pi(x) \in \overline{G}_j\}$.) This defines a chain

$$\{1\} = H_0 \leq \cdots \leq H_r = H \leq H_{r+1} \leq \cdots H_{r+s} = G,$$

and with the help of Proposition 15.11 we see that this is a solvable series for G.

□

Corollary 15.13. [cor-solvable-defn]
Let G be a finite group, and suppose that there is a chain

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_r = G$$

such that G_{i-1} is normal in G_i and G_i/G_{i-1} is abelian for all i. Then G is solvable.

Proof. Recall from Proposition 15.10 that all abelian groups are solvable, so G_i/G_{i-1} is solvable for all i. This means that G_1 and G_2/G_1 are solvable, so G_2 is solvable by Proposition 15.12(c). Now G_2 and G_3/G_2 are solvable, so G_3 is solvable by Proposition 15.12(c). Continuing in this way, we see that G_i is solvable for all i. In particular, the group $G = G_r$ is solvable as claimed. □

In Section 8 we analysed cyclotomic extensions of $\mathbb{Q}$. In fact, most of what we said there can be adapted to cover cyclotomic extensions of any field of characteristic zero. Our next result is one instance of that.

Proposition 15.14. [prop-cyclotomic-abelian]
Suppose we have a field K of characteristic zero and an extension $L = K(\zeta)$, where $\zeta^n = 1$. Then L is normal over K and $G(L/K)$ is abelian.

Proof. Let d be the smallest positive integer such that $\zeta^d = 1$. We then find that $1, \zeta, \dots, \zeta^{d-1}$ are d distinct roots of the polynomial $x^d - 1$, so we have $x^d - 1 = \prod_{i=0}^{d-1}(x - \zeta^i)$ in $L[x]$. This proves that L is a splitting field for $x^d - 1$ over K, so it is a normal extension of K. Next, for each $\sigma \in G(L/K)$ we see that $\sigma(\zeta)$ is a root of $x^d - 1$, so $\sigma(\zeta) = \zeta^{\lambda(\sigma)}$ say. Here $\lambda(\sigma)$ is an integer that is well-defined modulo d, so we can regard λ as a function $G(L/K) \to \mathbb{Z}/d\mathbb{Z}$. Note that

$$\tau(\sigma(\zeta)) = \tau(\zeta^{\lambda(\sigma)}) = \tau(\zeta)^{\lambda(\sigma)} = \zeta^{\lambda(\tau)\lambda(\sigma)},$$

which means that $\lambda(\tau\sigma) = \lambda(\tau)\lambda(\sigma)$. In particular, we have $\lambda(\sigma^{-1})\lambda(\sigma) = \lambda(1_L) = 1$, so $\lambda(\sigma)$ is invertible in $\mathbb{Z}/n\mathbb{Z}$, and we can regard λ as a group homomorphism $G(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$. We claim that this is injective. Indeed, if $\lambda(\sigma) = 1$ then $\sigma(\zeta) = \zeta$, so σ acts as the identity on $K(\zeta)$, but $K(\zeta) = L$, so $\sigma = 1$ as required. We now see that $G(L/K)$ is isomorphic to a subgroup of the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$, so $G(L/K)$ is abelian. □

Proposition 15.15. [prop-radicals-a]
Let K be a field of characteristic zero. Let L be a splitting field for a polynomial $f(x) \in K[x]$, and suppose that $G(L/K)$ is solvable. Then $f(x)$ is solvable by radicals.

Proof. Put $n = [L : K]$, and let N be a splitting field for $x^n - 1$ over L. This is also a splitting field for $(x^n - 1)f(x)$ over K, so it is normal over K. Next, consider the composite

$$\phi = (G(N/K(\zeta)) \xrightarrow{\text{include}} G(N/K) \xrightarrow{\text{restrict}} G(L/K)).$$

If σ is in the kernel then it acts as the identity on $K(\zeta)$ (because $\sigma \in G(L/K)$) and on L (as $\phi(\sigma) = 1$) so it acts as the identity on $L(\zeta) = N$, so $\sigma = 1$. This means that ϕ is injective, so $G(N/K(\zeta))$ is isomorphic to a subgroup of $G(L/K)$. This means that $|G(N/K(\zeta))|$ divides n, and also that $G(N/K(\zeta))$ is solvable. We can thus find a solvable series

$$\{1\} = H_0 \leq H_1 \leq \cdots \leq H_r = G(N/K(\zeta)).$$

We put $N_i = N^{H_i}$, so that

$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_r = K(\zeta).$$

As H_{i-1} is normal in H_i we see that N_{i-1} is normal over N_i. The Galois group $G(N_{i-1}/N_i)$ is isomorphic to H_i/H_{i-1}, so it is cyclic, of order n_i say. Here n_i divides $|H_r|$ which divides n, so $x^{n_i} - 1$ splits in $K(\zeta) \subseteq N_i$. We can thus use Proposition 14.1 to find $\alpha_{i-1} \in N_{i-1}$ such that $N_{i-1} = N_i(\alpha_{i-1})$ and $\alpha_{i-1}^{n_i} \in N_i$. This proves that N is a radical extension of $K(\zeta)$, which is clearly a radical extension of K. Thus L is contained in a radical extension of K, as required. □

Lemma 15.16. [lem-normal-radical]
Let N be a radical extension of K. Then there is another extension $M \supseteq N$, an integer $n > 0$, and a chain of subfields $K \subseteq M_0 \subseteq \cdots \subseteq M_t = M$ such that:

(a) *M is normal over K.*
(b) *$M_0 = K(\zeta)$ for some ζ such that $x^n - 1 = \prod_{i=0}^{n-1}(x - \zeta^i)$ in $M_0[x]$.*
(c) *For $0 < k \leq t$ we have $M_k = M_{k-1}(\beta_k)$ for some β_k such that $\beta_k^n \in M_{k-1}$.*

(In particular, M is again a radical extension of K.)

Proof. As N is a radical extension of K, we can choose elements $\alpha_1, \dots, \alpha_r$ and integers $n_1, \dots, n_r$ as in Definition 15.3. Put $n = n_1 n_2 \cdots n_r$, so α_i^n is a power of $\alpha_i^{n_i}$ and therefore lies in $K(\alpha_1, \dots, \alpha_{i-1})$. Put $f_i(t) = \min(\alpha_i, K)$ and $f(t) = (t^n - 1)\prod_{i=1}^r f_i(t) \in K[t]$. Let M be a splitting field for $f(t)$ over N, so $K \subseteq N \subseteq M$. Put $\mu_n = \{a \in M \mid a^n = 1\}$. This is a subgroup of $M^\times$, and it has order n because $x^n - 1$ splits in $M[t]$. It is also cyclic by Proposition 9.9. We choose a generator and call it ζ. Next, let P_i be the subfield of M generated by the roots of $x^n - 1, f_1(t), \dots, f_i(t)$, so

$$K \subseteq K(\zeta) = P_0 \subseteq P_1 \subseteq \cdots \subseteq P_r = M.$$

Let the roots of $f_i(t)$ be $\gamma_1, \dots, \gamma_s$, so $P_i = P_{i-1}(\gamma_1, \dots, \gamma_s)$. We claim that $\gamma_j^n \in P_{i-1}$. Indeed, α_i and γ_j are both roots in M of the irreducible polynomial $f_i(t) \in K[t]$, so Proposition 6.17(c) tells us that there is an automorphism $\sigma \in G(M/K)$ with $\sigma(\alpha_i) = \gamma_j$. As $\alpha_i^n \in K(\alpha_1, \dots, \alpha_{i-1}) \subseteq P_{i-1}$, we deduce that $\gamma_j^n = \sigma(\alpha_i^n) \in \sigma(P_{i-1})$. As P_{i-1} is normal over K we have $\sigma(P_{i-1}) = P_{i-1}$, so $\gamma_j^n \in P_{i-1}$ as required.

Now let the list $\beta_1, \dots, \beta_t$ consist of the roots of $f_1(t)$, followed by the roots of $f_2(t)$, and so on. Put $M_k = K(\zeta, \beta_1, \dots, \beta_k)$. It is now clear that these have the stated properties. □

Lemma 15.17. [lem-radicals-b]
In the situation of Lemma 15.16, the group $G(M/K)$ is solvable.

Proof. By the Galois Correspondence, there are subgroups

$$G(M/K) \geq H_0 \geq H_1 \geq \cdots \geq H_t = \{1\}$$

such that $M_k = M^{H_k}$ for all k. As $\zeta \in M_0$ we see that the polynomial $t^n - \beta_k^n \in M_{k-1}[t]$ actually splits as $\prod_{i=0}^{n-1}(t - \zeta^i \beta_k)$ in $M_k[t]$, so M_k is normal over M_{k-1}. It follows that H_k is normal in H_{k-1}, and the quotient H_{k-1}/H_k can be identified with $G(M_k/M_{k-1})$, which is cyclic by Proposition 14.1. Similarly, as M_0 is a splitting field for $t^n - 1$ over K we see that H_0 is normal in $G(M/K)$, and the quotient $G(M/K)/H_0$ can be identified with $G(K(\zeta)/K)$, which is abelian by Proposition 15.14. We can thus apply Corollary 15.13 to see that $G(M/K)$ is solvable, as claimed. □

Corollary 15.18. [cor-radicals-b]
Let K be a field of characteristic zero, and let $f(x)$ be a monic polynomial over K. Suppose we have fields $K \subseteq L \subseteq N$ such L is a splitting field for K, and N is a radical extension of K. Then $G(L/K)$ is solvable.

Proof. Choose M as in Lemma 15.16, so $G(M/K)$ is solvable by the lemma. As L and M are both normal over K, we have $G(L/K) \simeq G(M/K)/G(M/L)$, which is solvable by Proposition 15.12(b). □

Proposition 15.19. [prop-An-simple]
If $n \geq 5$ then the only normal subgroups of A_n are $\{1\}$ and A_n itself.

The proof will be given after some preliminaries.

Lemma 15.20. [lem-commutator]
Let G be a group, and let H be a normal subgroup. Then for all $g \in G$ and $h \in H$, the commutator $[g,h] = ghg^{-1}h^{-1}$ lies in H.

Proof. As H is normal we see that $ghg^{-1} \in H$, and also $h^{-1} \in H$ and H is closed under multiplication so $ghg^{-1}h^{-1} \in H$. □

Lemma 15.21. [lem-cycle-type]
Let σ and σ' be permutations in A_n with the same cycle type, and suppose that there is an odd permutation τ that commutes with σ. Then σ is conjugate to σ' in A_n.

Proof. It is standard that the cycle type determines the conjugacy class in Σ_n, so there is a permutation $\lambda \in \Sigma_n$ with $\lambda\sigma\lambda^{-1} = \sigma'$. If λ is even then we are done. Otherwise, the permutation $\mu = \lambda\tau$ is even and we have

$$\mu\sigma\mu^{-1} = \lambda\tau\sigma\tau^{-1}\lambda^{-1} = \lambda\sigma\tau\tau^{-1}\lambda^{-1} = \lambda\sigma\lambda^{-1} = \sigma',$$

so again σ' is conjugate in A_n to σ. □

Corollary 15.22. [cor-An-conjugacy]
If $n \geq 5$ then all 3-cycles are conjugate in A_n, and all transposition pairs are conjugate in A_n.

Proof. Any transposition pair $\sigma = (a\ b)(c\ d)$ comutes with the odd permutation $(a\ b)$. If $\rho = (a\ b\ c)$ is a 3-cycle, then (as $n \geq 5$) we can find a transposition $(d\ e)$ that is disjoint from ρ, so again this gives an odd permutation that commutes with ρ. □

Lemma 15.23. [lem-An-simple]
Let H be a normal subgroup of A_n (where $n \geq 5$) and suppose that H contains either a 3-cycle or a transposition pair. Then $H = A_n$.

Proof. If H contains one 3-cycle it contains all of them (by Corollary 15.22). One can then check that $[(1\ 2)(3\ 4), (1\ 2\ 3)] = (1\ 3)(2\ 4)$, so H also contains a transposition pair, and therefore (by the same corollary) contains all transposition pairs.

Suppose instead we start by assuming that H contains a transposition pair, and thus contains all transposition pairs. One can then check that $[(1\,2\,5), (1\,2)(3\,4)] = (1\,5\,2)$, so H contains a 3-cycle, and so contains all 3-cycles.

Now let α and β be any two transpositions. Then $\alpha\beta$ is either the identity (if $\alpha = \beta$) or a 3-cycle (if α and β overlap) or a transposition pair. In all cases, we have $\alpha\beta \in H$. Now let σ be any even permutation. Then we can write σ as the product of an even number of transposition, and by grouping them in pairs, we see that $\sigma \in H$. Thus $H = A_n$ as claimed. □

Proof of Proposition 15.19. Let H be a nontrivial normal subgroup of A_n. Choose an element $\sigma \in H$ with $\sigma \neq 1$. We will consider various different cases depending on the cycle type of σ.

(a) Suppose that σ involves an r-cycle $\rho = (a_1\ \cdots\ a_r)$ for some $r > 3$. Put $\tau = (a_1\ a_2\ a_3)$. This commutes with all the other cycles in σ, and it follows that $[\tau, \sigma] = [\tau, \rho]$. One can check directly that $[\tau, \rho] = (a_1\ a_2\ a_4)$, so H contains a 3-cycle, so $H = A_n$ by Lemma 15.23.

(b) Now suppose that (a) does not hold, so σ involves only 3-cycles and transpositions. Suppose that there is at least one transposition. As σ is even and 3-cycles are even, there must be an even number of transpositions. We can thus write $\sigma = \rho\omega$, where $\rho = (a\ b)(c\ d)$ and ω is disjoint from ρ. Put $\tau = (a\ b\ c)$; we then find that $[\tau, \sigma] = [\tau, \rho] = (a\ b)(c\ d)$, so H contains a transposition pair. It follows by Lemma 15.23 that $H = A_n$.

(c) Now suppose that neither (a) nor (b) holds, so σ is a product of 3-cycles. If σ is a single 3-cycle then we can immediately use Lemma 15.23 to see that $H = A_n$. If there are at least two 3-cycles then we can write $\sigma = \rho\omega$, where $\rho = (a\ b\ c)(d\ e\ f)$ and ω is disjoint from ρ. We then put $\tau = (a\ b\ d)$ and check that
$$[\tau, \sigma] = [\tau, \rho] = (a\ b\ e\ c\ d).$$
We can thus apply case (a) to this 5-cycle to see that $H = A_n$ again.

□

Corollary 15.24. [cor-not-solvable]
For $n \geq 5$ the groups Σ_n and A_n are not solvable.

Proof. Suppose we have a solvable series $1 = H_0 \leq H_1 \leq \cdots \leq H_{r-1} \leq H_r = A_n$. After eliminating any repetitions, we may assume that these inclusions are strict, so $1 < H_1 < \cdots < H_{r-1} < H_r = A_n$. By the definition of a solvable series, the group H_{r-1} must be normal in A_n, and also $H_{r-1} < A_n$, so we must have $H_{r-1} = 1$. This means that $A_n = H_r/H_{r-1}$, but H_r/H_{r-1} is cyclic, so this is impossible. This means that A_n is not solvable. As every subgroup of a solvable group is solvable, it follows that Σ_n is also not solvable. □

We now see, as claimed previously, that polynomials of degree at least 5 are typically not solvable by radicals.

Exercises

Exercise 15.1. [ex-check-solvable]
Which of the following polynomials are solvable by radicals over $\mathbb{Q}$?

$$\begin{aligned}
f_0(x) &= 2x^5 - 10x^2 - 5x \\
f_1(x) &= 2x^5 - 10x - 5 \\
f_2(x) &= 2x^6 - 10x^2 - 5 \\
f_3(x) &= 5x^5 + 10x^4 - 2 \\
f_4(x) &= x^5 - 405x + 3 \\
f_5(x) &= 4x^{10} - 40x^6 - 20x^5 + 100x^2 + 100x + 25.
\end{aligned}$$

Three of these polynomials have the same splitting field. Which are they?

Exercise 15.2. [ex-septic]
Prove that the polynomial $f(x) = 30x^7 - 70x^6 - 42x^5 + 105x^4 - 21$ is not solvable by radicals.

Exercise 15.3. [ex-affine-five]
In this question it will be convenient to think Σ_5 as the group of permutations of the set $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. For $a \in \mathbb{F}_5^\times$ and $b \in \mathbb{F}_5$ we define $\rho_{ab} \colon \mathbb{F}_5 \to \mathbb{F}_5$ by $\rho_{ab}(u) = au + b$. We then put

$$U = \{\rho_{ab} \mid a \in \mathbb{F}_5^\times, b \in \mathbb{F}_5.$$

(a) Prove that U is a subgroup of Σ_5, which contains a normal cyclic subgroup of order 5, whose quotient is cyclic of order 4.
(b) Suppose that H is some other subgroup of Σ_5, and there is a cyclic subgroup C of order 5 that is normal in H. Prove that H is conjugate to a subgroup of A.
(c) Prove that any transitive subgroup of Σ_5 is either equal to Σ_5, or equal to A_5, or conjugate to a subgroup of A.

Exercise 15.4. [ex-special-sextic]
Find an irreducible polynomial of degree 6 over $\mathbb{Q}$ with 4 real roots, but whose Galois group over $\mathbb{Q}$ is not Σ_6.

Solutions

Exercise 1.1: The set K_0 is not a field, because the element $1 \in K_0$ has no additive inverse in K_0. The set K_1 is a commutative ring but not a field, because the nonzero element $2 \in K_1$ has no multiplicative inverse in K_1.

The set K_2 (otherwise known as $\mathbb{Q}(\sqrt{2})$) is a field. Indeed, it is clearly closed under addition and contains 0 and 1. It is also closed under multiplication because for all $a, b, c, d \in \mathbb{Q}$ we have

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

(and $ac + 2bd, ad + bc \in \mathbb{Q}$). Finally, any nonzero element $x \in \mathbb{Q}(\sqrt{2})$ has the form $x = a + b\sqrt{2}$ where at least one of a and b are nonzero. A standard lemma tells us that $\sqrt{2}$ is irrational, and thus that $a^2 - 2b^2$ cannot be zero. It follows that the expression $y = (a - b\sqrt{2})/(a^2 - 2b^2)$ gives a well-defined element of K_2, and one checks directly that $xy = 1$, so y is a multiplicative inverse for x. This proves that K_2 is a subfield of $\mathbb{C}$.

Next, K_3 is just equal to $\mathbb{R}$, so it is a field. The set K_4 contains the element $\alpha = 2^{1/3}$ but it does not contain α^2, so it is not closed under multiplication, so it is not a field (or even a ring). The set K_4 is a commutative ring, with the pair $(1, 1)$ as the multiplicative identity. However, it is not a field. Indeed, the element $e = (1, 0)$ is nonzero but for any $(a, b) \in K_4$ we have $e.(a, b) = (a, 0) \neq (1, 1)$; this shows that e has no multiplicative inverse. The set $K_6 = \mathbb{Z}/6\mathbb{Z}$ is a commutative ring but not a field, because the nonzero element $\overline{2}$ has no inverse, as we see from the multiplication table modulo 6:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

On the other hand, the ring $\mathbb{Z}/7Z$ is a field. Indeed, we have

$$1^2 = 2 \times 4 = 3 \times 5 = 6^2 = 1 \pmod{7},$$

so in $\mathbb{Z}/7\mathbb{Z}$ we have

$$1^{-1} = 1 \qquad 2^{-1} = 4 \qquad 3^{-1} = 5 \qquad 4^{-1} = 2 \qquad 5^{-1} = 3 \qquad 6^{-1} = 6,$$

so every nonzero element has an inverse. (The real reason for the difference between K_6 and K_7 is that 7 is prime and 6 is not.)

Exercise 1.2: We have $\mathbb{F}_2[i] = \{0, 1, i, 1 + i\}$ and one can check directly that none of these elements is an inverse for $1 + i$, so $\mathbb{F}_2[i]$ is not a field. Alternatively $(1 + i)^2 = 2i = 0$ which would contradict Lemma 1.5 if $\mathbb{F}_2[i]$ were a field.

Similarly, in $\mathbb{F}_5[i]$ we find that $2 + i$ and $2 - i$ are nonzero but $(2 + i)(2 - i) = 5 = 0$, so again $\mathbb{F}_5[i]$ is not a field.

Now consider $\mathbb{F}_3[i]$, and put $\alpha = 1 + i$. We find that

$$\begin{array}{ll}
\alpha^0 = 1 & \alpha^1 = 1 + i \\
\alpha^2 = -i & \alpha^3 = 1 - i \\
\alpha^4 = -1 & \alpha^5 = -1 - i \\
\alpha^6 = i & \alpha^7 = -1 + i \\
\alpha^8 = 1. &
\end{array}$$

From this we see that every nonzero element of $\mathbb{F}_3[i]$ is α^k for some $k \in \{0, \dots, 7\}$, and that this has inverse α^{8-k}. This shows that $\mathbb{F}_3[i]$ is a field.

Exercise 1.3: Let K be a subfield of $\mathbb{Q}(\sqrt{p})$. This contains 1 and is closed under addition and subtraction, so it must contain $\mathbb{Z}$. For integers $b > 0$ we then deduce that $b^{-1} \in K$, and so $a/b \in K$ for all $a \in \mathbb{Z}$; this shows that K contains $\mathbb{Q}$. Suppose that K is not equal to $\mathbb{Q}$; then K must contain some element $\alpha = u+v\sqrt{p}$ with $u, v \in \mathbb{Q}$ and $v \neq 0$. As $u \in \mathbb{Q} \subseteq K$ and $\alpha \in K$ we see that the number $v\sqrt{p} = \alpha - u$ is also in K. Similarly, we have $v^{-1} \in K$ and so $\sqrt{p} = v^{-1}.(v\sqrt{p}) \in K$. Finally, let x and y be arbitrary rational numbers; then $x, y, \sqrt{p} \in K$, so $x + y\sqrt{p} \in K$. This proves that K is all of $\mathbb{Q}(\sqrt{p})$, as required.

Exercise 1.4: Put $\alpha = a^{1/n}$, so the field in question is $K = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Let $\sigma \colon K \to K$ be an automorphism, and put $\zeta = \sigma(\alpha)/\alpha \in K \subseteq \mathbb{R}$. We can apply σ to the equation $\alpha^n = a$ to get $\sigma(\alpha)^n = a$, and then divide by the original equation to get $\zeta^n = 1$. As ζ is real and n is odd, we see that ζ has the same sign as ζ^n, but $\zeta^n = 1 > 0$, so $\zeta > 0$. We also have $(\zeta - 1)(1 + \zeta + \dots + \zeta^{n-1}) = \zeta^n - 1 = 0$, but all terms in the sum $1 + \zeta + \dots + \zeta^{n-1}$ are strictly positive, so $\zeta = 1$. This means that $\sigma(\alpha) = \alpha$, so σ acts as the identity on $\mathbb{Q}(\alpha) = K$.

Exercise 1.5: We have $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ with $\alpha^2 = \alpha^{-1} = 1 + \alpha$. Any automorphism $\phi \colon \mathbb{F}_4 \to \mathbb{F}_4$ must be a bijection and must satisfy $\phi(0) = 0$ and $\phi(1) = 1$, so either

(a) $\phi(\alpha) = \alpha$ and $\phi(\alpha^2) = \alpha^2$; or
(b) $\phi(\alpha) = \alpha^2$ and $\phi(\alpha^2) = \alpha$.

In case (a) we see that ϕ is the identity. All that is left is to check that case (b) really does define an automorphism, or equivalently that $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathbb{F}_4$. One way to do this would be to just work through the sixteen possible pairs (x, y). More efficiently, we can note that $\phi(x) = x^2$ for all $x \in \mathbb{F}_4$. (This is clear for $x = 0$ or $x = 1$ or $x = \alpha$; for the case $x = \alpha^2$ we recall that $\alpha^3 = 1$ so $(\alpha^2)^2 = \alpha^4 = \alpha^3.\alpha = \alpha = \phi(\alpha^2)$.) Given this, it is clear that $\phi(xy) = x^2y^2 = \phi(x)\phi(y)$ for all x and y. We also have $\phi(x+y) = (x+y)^2 = x^2 + y^2 + 2xy = \phi(x) + \phi(y) + 2xy$, but we are working in characteristic two so $2xy = 0$ and so $\phi(x+y) = \phi(x) + \phi(y)$ as required.

Exercise 1.6: This is very similar to Proposition 1.31. We have $\phi(0_L) = 0_M = \psi(0_L)$, so $0_L \in K$. Similarly, we have $\phi(1_L) = 1_M = \psi(1_L)$, so $1_L \in K$. If $a, b \in K$ then $\phi(a) = \psi(a)$ and $\phi(b) = \psi(b)$ so

$$\begin{aligned}
\phi(a+b) &= \phi(a) + \phi(b) = \psi(a) + \psi(b) = \psi(a+b) \\
\phi(a-b) &= \phi(a) - \phi(b) = \psi(a) - \psi(b) = \psi(a-b) \\
\phi(ab) &= \phi(a)\phi(b) = \psi(a)\psi(b) = \psi(ab),
\end{aligned}$$

which shows that $a+b, a-b, ab \in K$. Finally, if $a \in K^\times$ then we can apply Proposition 1.29(a) to both ϕ and ψ to get

$$\phi(a^{-1}) = \phi(a)^{-1} = \psi(a)^{-1} = \psi(a^{-1}),$$

which shows that $a^{-1} \in K$. Thus, K is a subfield as claimed.

Exercise 1.7: Put $R = K_0 \times K_1$. We recall that this is the set of all pairs (a_0, a_1), where $a_0 \in K_0$ and $a_1 \in K_1$. By hypothesis we are given an addition rule and a multiplication rule for elements of K_0, and an addition rule and a multiplication rule for elements of K_1. We combine these in the obvious way to define addition and multiplication in R:

$$\begin{aligned}
(a_0, a_1) + (b_0, b_1) &= (a_0 + b_0, a_1 + b_1) \\
(a_0, a_1)(b_0, b_1) &= (a_0 b_0, a_1 b_1).
\end{aligned}$$

The zero element of R is the pair $(0,0)$, and the unit element is $(1,1)$. Suppose we have three elements $a,b,c \in R$, say $a=(a_0,a_1)$ and $b=(b_0,b_1)$ and $c=(c_0,c_1)$. By the associativity rule in K_0 we have $a_0+(b_0+c_0)=(a_0+b_0)+c_0$. By the associativity rule in K_1 we have $a_1+(b_1+c_1)=(a_1+b_1)+c_1$. It follows that in R we have

$$\begin{aligned}
a+(b+c) &= (a_0,a_1)+((b_0,b_1)+(c_0,c_1)) \\
&= (a_0,a_1)+(b_0+c_0,b_1+c_1) \\
&= (a_0+(b_0+c_0),a_1+(b_1+c_1)) \\
&= ((a_0+b_0)+c_0,(a_1+b_1)+c_1) \\
&= (a_0+b_0,a_1+b_1)+(c_0,c_1) \\
&= ((a_0,a_1)+(b_0,b_1))+(c_0,c_1)=(a+b)+c.
\end{aligned}$$

(The first, second, fourth and fifth steps here are just instances of the definition of addition in R; the third step uses the associativity rules in K_0 and K_1.) Thus, addition in R is associative.

Similarly, the distributivity rule in K_0 tells us that $a_0(b_0+c_0)=a_0b_0+a_0c_0$. The distributivity rule in K_1 tells us that $a_1(b_1+c_1)=a_1b_1+a_1c_1$. It follows that in R we have

$$\begin{aligned}
a(b+c) &= (a_0,a_1)(b_0+c_0,b_1+c_1) \\
&= (a_0(b_0+c_0),a_1(b_1+c_1)) \\
&= (a_0b_0+a_0c_0,a_1b_1+a_1c_1) \\
&= (a_0b_0,a_1b_1)+(a_0c_0,a_1c_1)=ab+ac.
\end{aligned}$$

The other commutative ring axioms can be checked in the same way.

As $1\neq 0$ in K_0, we see that the element $e=(1,0)\in R$ is nonzero. For any element $a=(a_0,a_1)\in R$ we have $ea=(a_0,0)\neq(1,1)=1_R$, so a is not inverse to e. Thus e is a nonzero element with no inverse, proving that R is not a field.

Exercise 2.1:

- ϕ_0 is not linear because $\phi_0(-I)=(-I)^2=I\neq-\phi(I)$.
- ϕ_1 is linear because

$$\phi_1(sA+tB)=sA+tB-(sA+tB)^T=sA+tB-sA^T-tB^T=s(A-A^T)+t(B-B^T)=s\phi_1(A)+t\phi_1(B).$$

  (This is enough by Remark 2.10.)
- ϕ_2 is also linear, because

$$\phi_2\left(s\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]+t\left[\begin{smallmatrix}c\\d\end{smallmatrix}\right]\right)=\phi_2\left[\begin{smallmatrix}sa+tc\\sb+td\end{smallmatrix}\right]=(sa+tc)x+(sb+td)x^2=s(ax+bx^2)+t(cx+dx^2)=s\phi_2\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]+t\phi_2\left[\begin{smallmatrix}c\\d\end{smallmatrix}\right].$$

- ϕ_3 is not linear, because

$$\phi_3\left(-\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]\right)=\phi_3\left[\begin{smallmatrix}0\\-1\end{smallmatrix}\right]=(-x)^2\neq-x^2=-\phi_3\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right].$$

- ϕ_4 is linear, because if $h(x)=s\,f(x)+t\,g(x)$ then $h(2)=s\,f(2)+t\,g(2)$ and $h(-2)=s\,f(-2)+t\,g(-2)$ so

$$\phi_4(s\,f(x)+t\,g(x))=\begin{bmatrix}h(2)\\h(-2)\end{bmatrix}=s\begin{bmatrix}f(2)\\f(-2)\end{bmatrix}+t\begin{bmatrix}g(2)\\g(-2)\end{bmatrix}=s\phi_4(f(x))+t\phi_4(g(x)).$$

- ϕ_5 is not linear. Indeed, for constant polynomials we just have $\phi_5(c)=c^3$, so $\phi_5(1+1)=8\neq 2=\phi_5(1)+\phi_5(1)$.

Exercise 2.2: No. We would have

$$\begin{aligned}
[M:\mathbb{Q}] &= [M:K][K:\mathbb{Q}]=7\times 3=21 \\
[M:\mathbb{Q}] &= [M:L][L:\mathbb{Q}]=5\times 4=20,
\end{aligned}$$

which is obviously not possible.

Exercise 2.3: Put $a = [L : K]$ and $b = [M : L]$ and $c = [N : M]$. As K, L, M and N are all different we must have $a, b, c > 1$. We also have

$$\begin{aligned} ab &= [M : L][L : K] = [M : K] = 6 \\ bc &= [N : M][M : L] = [N : L] = 15. \end{aligned}$$

As $ab = 6$ with $a, b > 1$ we must have $(a, b) = (2, 3)$ or $(a, b) = (3, 2)$. As $bc = 15$ with $b, c > 1$ we must have $(b, c) = (3, 5)$ or $(b, c) = (5, 3)$. The only way these can both be satisfied is if $(a, b, c) = (2, 3, 5)$.

Exercise 2.4: The general form for elements of V is

$$M = \left[\begin{smallmatrix} a & b & c \\ b & d & e \\ c & e & -a-d \end{smallmatrix}\right] = aA + bB + cC + dD + eE,$$

where

$$A = \left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right] B = \left[\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right] C = \left[\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right] D = \left[\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right] E = \left[\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right].$$

It follows easily from this that the list A, B, C, D, E is a basis for V.

Exercise 2.5:

- Put $A = iI = \left[\begin{smallmatrix} i & 0 \\ 0 & i \end{smallmatrix}\right]$. As $\bar{i} = -i$ we see that $A^\dagger = -A$, so $A \in V$. On the other hand, we have $-iA = I$ and $I + I^\dagger = 2I$ so $-iA \notin V$. This means that V is not closed under multiplication by the complex number $-i$, so it is not a subspace over $\mathbb{C}$ of $M_2(\mathbb{C})$.
- If $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ then $A + A^\dagger = \left[\begin{smallmatrix} a+\overline{a} & b+\overline{c} \\ c+\overline{b} & d\overline{d} \end{smallmatrix}\right]$. For this to be zero, we need $a + \overline{a} = d + \overline{d} = 0$ (so a and d are purely imaginary) and $c = -\overline{b}$. Equivalently, A must have the form

  $$A = \left[\begin{smallmatrix} iw & x+iy \\ -x+iy & iz \end{smallmatrix}\right] = w \left[\begin{smallmatrix} i & 0 \\ 0 & 0 \end{smallmatrix}\right] + x \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] + y \left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right] + z \left[\begin{smallmatrix} 0 & 0 \\ 0 & i \end{smallmatrix}\right]$$

  for some $w, x, y, z \in \mathbb{R}$. It follows that V is a subspace over $\mathbb{R}$ of $M_2(\mathbb{C})$, with basis given by the matrices

  $$\left[\begin{smallmatrix} i & 0 \\ 0 & 0 \end{smallmatrix}\right] \qquad \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] \qquad \left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right] \qquad \left[\begin{smallmatrix} 0 & 0 \\ 0 & i \end{smallmatrix}\right].$$

  In particular, this basis has size four, so $\dim_{\mathbb{R}}(V) = 4$ as required.

Exercise 2.6: As L is generated over $\mathbb{C}$ by x, it is certainly generated over the larger field K by x. Put $f(t) = t^n - x^n \in K[t]$. Clearly $f(x) = 0$, so x is algebraic over K. Let $g(t)$ be the minimal polynomial of x over K, so $g(t)$ divides $f(t)$, and $L = K(x) \simeq K[t]/g(t)$, so $m = [L : K]$ is the degree of $g(t)$. As $g(t)$ divides $f(t)$ we see that $m \leq n$. We will suppose that $m < n$ and derive a contradiction; this will complete the proof.

The coefficients of $g(t)$ are elements of $K = \mathbb{Q}(x^n)$, so they can be written as $a_i(x^n)/b_i(x^n)$ for certain polynomials $a_i(s)$ and $b_i(s) \neq 0$. If we let $d(s)$ be the product of all the terms $b_i(s)$ we obtain an expression $d(x^n)g(t) = \sum_{i=0}^{m} c_i(x^n)t^i$, with $c_i(s), d(s) \in \mathbb{C}[s]$. By assumption $g(x) = 0$, so $\sum_{i=0}^{m} c_i(x^n)x^i = 0$. As $m < n$ we can compare coefficient of x^{nj+i} (for $0 \leq i \leq m$) to see that $c_i(x) = 0$. It follows that $g(t) = 0$, which contradicts the fact that $g(t)$ divides $f(t)$, as required.

Exercise 3.1: Recall that $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ with $\alpha^2 = \alpha^{-1} = 1 + \alpha$. Define $\phi\colon \mathbb{Z}[x] \to \mathbb{F}_4$ by

$$\phi(a_0 + a_1x + \cdots + a_dx^d) = \overline{a_0} + \overline{a_1}\alpha + \cdots + \overline{a_d}\alpha^d.$$

This is clearly a homomorphism. It satisfies $\phi(0) = 0$ and $\phi(1) = 1$ and $\phi(x) = \alpha$ and $\phi(x^2) = \alpha^2$, so every element of $\mathbb{F}_4$ is in the image of ϕ, so ϕ is surjective. Let I be the kernel of ϕ. Proposition 3.10 then gives us an induced isomorphism $\overline{\phi}\colon \mathbb{Z}[x]/I \to \mathbb{F}_4$. One can check that I can be described more explicitly as

$$I = \{f(x) \in \mathbb{Z}[x] \mid f(x) = 2g(x) + (x^2 + x + 1)h(x) \text{ for some } g(x), h(x) \in \mathbb{Z}[x]\}.$$

Exercise 3.2: Write

$$R = \mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

The principal ideals are as follows:

$$\begin{aligned}
R.0 &= \{0\} \\
R.1 &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = R.5 = R.7 = R.11 \\
R.2 &= \{0, 2, 4, 6, 8, 10\} = R.10 \\
R.3 &= \{0, 3, 6, 9\} = R.9 \\
R.4 &= \{0, 4, 8\} = R.8 \\
R.6 &= \{0, 6\}.
\end{aligned}$$

In fact, it can be shown that every ideal in $\mathbb{Z}/n\mathbb{Z}$ is principal, so the above list actually contains all ideals in R.

Exercise 4.1: We first recall Eisenstein's criterion. Suppose we have a monic polynomial

$$a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + x^d$$

and a prime number p such that

(a) the coefficients $a_0, \ldots, a_{d-1}$ are all integers divisible by p; and
(b) the constant term a_0 is not divisible by p^2,

then $g(x)$ is irreducible over $\mathbb{Q}$. We find the $f_0(x)$ is irreducible by Eisenstein's criterion with $p = 3$, and that $f_3(x)$ is irreducible by Eisenstein's criterion with $p = 5$. On the other hand, $f_1(x) = (x-2)(x^2+x+1)$ and $f_2(x) = (x-3)(x+6)$, so neither of these is irreducible over $\mathbb{Q}$.

Exercise 4.2: We start with $f_0(x) = f(x)$ and $f_1(x) = f'(x)/4 = x^3 + \frac{3}{2}x^2 + \frac{3}{2}x + \frac{1}{2}$. By long division we have

$$f_0(x) = (x + \tfrac{1}{2})f_1(x) + (\tfrac{3}{4}x^2 + \tfrac{3}{4}x + \tfrac{3}{4}),$$

so $f_2(x) = x^2 + x + 1$. We then divide $f_1(x)$ by $f_2(x)$ and obtain

$$f_1(x) = (x + \tfrac{1}{2})f_2(x)$$

(with no remainder). Thus the algorithm stops with $\gcd(f(x), f'(x)) = x^2 + x + 1$. This means that every root of x^2+x+1 is a double root of $f(x)$, so $f(x)$ is divisible by $(x^2+x+1)^2$, but these are monic polynomials of the same degree, so $f(x) = (x^2 + x + 1)^2$.

Exercise 4.3: The polynomial $f(x + 2) = x^4 + 3x^3 + 3x^2 + 3x + 3$ satisfies Eisenstein's criterion at $p = 3$, so $f(x + 2)$ is irreducible, so $f(x)$ is irreducible. We can also make the same argument using $f(x-1) = x^4 - 9x^3 + 30x^2 - 42x + 21$ (but $f(x + 1)$ does not work).

Exercise 4.4: First, in $\mathbb{F}_2$ we have $f(0) = 1$ and $f(1) = 1$, so $f(x)$ has no roots, so it has no factors of degree one. Thus, the only way it could factorise would be as an irreducible quadratic times an irreducible cubic. The only quadratics over $\mathbb{F}_2$ are x^2, $x^2 + 1 = (x + 1)^2$, $x^2 + x = x(x + 1)$ and $x^2 + x + 1$. Only the last of these is irreducible. We find by long division over $\mathbb{F}_2$ that

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

so $f(x)$ is not divisible by $x^2 + x + 1$. It is therefore irreducible as claimed.

Now suppose we have a factorisation $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$, where $g(x)$ and $h(x)$ are monic. We see from Gauss's Lemma that $g(x), h(x) \in \mathbb{Z}[x]$, so it makes sense to reduce everything modulo 2. We then have $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $\mathbb{F}_2[x]$, but $\overline{f}(x)$ is irreducible, so one of the factors must be equal to one, say $\overline{g}(x) = 1$. As $g(x)$ is monic, the only way we can have $\overline{g}(x) = 1$ is if $g(x) = 1$. We deduce that $f(x)$ is irreducible in $\mathbb{Q}[x]$, as claimed.

Exercise 4.5: I claim that R is just the ring $\mathbb{F}_p[x^p]$ of polynomials in x^p. To see this, consider an arbitrary element $f(x) \in \mathbb{F}_p[x]$, say $f(x) = \sum_{i=0}^N a_i x^i$ for some sequence of coefficients $a_i \in \mathbb{F}_p$. We then have $f'(x) = \sum_{i=0}^N i\, a_i\, x^{i-1}$, so $f'(x) = 0$ iff $i\, a_i = 0$ for all i. If i is divisible by p then it gives the zero element of $\mathbb{F}_p$ so the equation $i\, a_i = 0$ holds automatically. However, if i is not divisible by p then it gives a nonzero element of the field $\mathbb{F}_p$, so we can multiply by the inverse to get $a_i = 0$. It follows that $f'(x) = 0$ iff $f(x)$ has the form $\sum_{j=0}^M a_{jp} x^{jp}$ say, or equivalently $f(x)$ is a polynomial function of x^p.

Exercise 5.1: We will write K_i for the splitting field of $f_i(x)$.

- We can write $f_0(x)$ as $(x-1)^2$, so $K_0 = \mathbb{Q}$.
- We can factor $f_1(x)$ as $(x^2-2)(x^2-3)$, so the roots are $\pm\sqrt{2}$ and $\pm\sqrt{3}$, so the $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- The roots of $f_2(x)$ are $(1 \pm \sqrt{-3})/2$, so $K_2 = \mathbb{Q}(\sqrt{-3})$.
- The roots of $f_3(x)$ are α, $\omega\alpha$ and $\omega^2\alpha$, where α is the real cube root of 2, and $\omega = e^{2\pi i/3} = (\sqrt{-3} - 1)/2$. It follows that K_3 contains α and $\omega\alpha$, so it also contains $(\omega\alpha)/\alpha = \omega$, so it also contains $2\omega + 1 = \sqrt{-3}$. Form this it follows that $K_3 = \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \sqrt{-3})$.
- We can regard $f_4(x)$ as a quadratic function of x^2, and we find that it vanishes when $x^2 = (4 \pm \sqrt{12})/2 = 2 \pm \sqrt{3}$, so $x = \pm\sqrt{2 \pm \sqrt{3}}$. Thus, one root of $f(x)$ is $\alpha = \sqrt{2+\sqrt{3}}$, and another is $-\alpha$. The other two roots are β and $-\beta$, where $\beta = \sqrt{2-\sqrt{3}}$. However, we have $\alpha\beta = \sqrt{(2+\sqrt{3})(2-\sqrt{3})} = \sqrt{1} = 1$, so $\beta = \alpha^{-1}$. It follows that the full list of roots is $\alpha, -\alpha, 1/\alpha, -1/\alpha$, so $K_4 = \mathbb{Q}(\alpha)$.
- If we let α denote the positive real fourth root of 2, then the roots of $f_5(x)$ are $\alpha, i\alpha, -\alpha$ and $-i\alpha$. It follows that $K_5 = \mathbb{Q}(\alpha, i)$. It follows that $[K_5 : \mathbb{Q}] = 8$.
- The roots of $f_6(x)$ are the 6th roots of unity, which are the powers of $\alpha = e^{\pi i/3} = (1 + \sqrt{-3})/2$, so $K_6 = \mathbb{Q}(\sqrt{-3})$.
- The roots of $f_7(x)$ are the numbers $2\alpha^k$, where again $\alpha = e^{\pi i/3} = (1 + \sqrt{-3})/2$. It follows that $K_7 = K_6 = \mathbb{Q}(\sqrt{-3})$.

Exercise 5.2:

(a) The roots of $x^4 + 1$ are the primitive 8th roots of unity. One of these is $\alpha = e^{i\pi/4} = (1+i)/\sqrt{2}$, and the others are $\alpha^3 = i\alpha$, $\alpha^5 = -\alpha$ and $\alpha^7 = -i\alpha$. Note that $i = \alpha^2$ and $\sqrt{2} = (1+i)/\alpha = (1+\alpha^2)/\alpha$, so $i, \sqrt{2} \in \mathbb{Q}(\alpha)$. It is also clear that $\alpha \in \mathbb{Q}(i, \sqrt{2})$, so the relevant splitting field is $\mathbb{Q}(i, \sqrt{2})$.

(b) We may observe that $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$, and so its roots are just the roots of the two quadratic factors. These are

$$\frac{-1 \pm \sqrt{-3}}{2} \qquad \text{and} \qquad \frac{1 \pm \sqrt{-3}}{2}.$$

It follows that the splitting field is $\mathbb{Q}(\sqrt{-3})$, of degree 2 over $\mathbb{Q}$.

(c) The roots of $x^6 + 1$ are the 6th roots of -1. As $-1 = e^{i\pi}$, one of these roots is

$$\alpha = e^{i\pi/6} = (\sqrt{3} + i)/2.$$

The other roots are obtained by multiplying α by a 6th root of 1, but the 6th roots of 1 are just the powers of α^2, so the roots of $x^6 + 1$ are $\alpha, \alpha^3, \alpha^5, \alpha^7, \alpha^9$ and α^{11}. Thus, the splitting field is just $\mathbb{Q}(\alpha)$. Note that $\alpha \in \mathbb{Q}(i, \sqrt{3})$, but $i = e^{i\pi/2} = \alpha^3 \in \mathbb{Q}(\alpha)$, and so $\sqrt{3} = 2\alpha - i \in \mathbb{Q}(\alpha)$. It follows that the splitting field can also be described as $\mathbb{Q}(i, \sqrt{3})$. It therefore has degree 4 over $\mathbb{Q}$.

(d) Note that $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$, so the roots of $x^6 + x^3 + 1$ are the primitive 9th roots of unity. One may then observe that if ζ is a primitive 9th root of unity, all other primitive 9th roots of unity are powers of ζ, so that the splitting field is just $\mathbb{Q}(\zeta)$. Its degree over $\mathbb{Q}$ is just the degree of the minimal polynomial of ζ, but this is the given polynomial $x^6 + x^3 + 1$ as it is irreducible (substitute $x \mapsto x + 1$ and use Eisenstein with $p = 3$). So $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$.

Alternatively, the roots of y^2+y+1 are $\omega=\frac{-1+\sqrt{-3}}{2}\in\mathbb{Q}(\sqrt{-3})$ and $\omega^{-1}=\omega^2=\frac{-1-\sqrt{-3}}{2}\in\mathbb{Q}(\sqrt{-3})$. The roots of x^6+x^3+1 are the cube roots of these, so if $\alpha=\omega^{\frac{1}{3}}$, then the roots are $\alpha,\omega\alpha,\omega^2\alpha;\alpha^{-1},\omega\alpha^{-1},\omega^2\alpha^{-1}$. So the splitting field is $\mathbb{Q}(\alpha,\omega)$; but $\mathbb{Q}(\omega)=\mathbb{Q}(\sqrt{-3})$, so has degree 2 over $\mathbb{Q}$. Further, α satisfies the cubic equation $x^3-\omega$ with coefficients in $\mathbb{Q}(\omega)$, so $\mathbb{Q}(\omega,\alpha)$ has degree at most 3 over $\mathbb{Q}(\omega)$. Thus the degree of the splitting field is at most 6 over $\mathbb{Q}$ (using the Degrees Theorem). On the other hand, the polynomial is irreducible (as above), so adjoining any root of it gives a field extension of degree 6, and so adjoining all the roots gives a field extension of degree at least 6. Thus the degree equals 6.

Exercise 5.3: First define $\chi_0\colon K[x]\to L$ by $\chi_0(p(x))=p(\alpha)$, or more explicitly

$$\chi_0(\sum_i a_ix^i)=\sum_i a_i\alpha^i.$$

The kernel of this is $I(\alpha,K)$, which is zero because α is transcendental. Thus, if $q(x)\neq 0$ we see that $q(\alpha)$ is a nonzero element of L, so it has an inverse in L. Thus, given a rational function $f(x)=p(x)/q(x)$, we can try to define $\chi(f(x))=p(\alpha)/q(\alpha)\in L$. There is a potential ambiguity here: what if $f(x)$ can be represented in a different way, say as $f(x)=r(x)/s(x)$ for some $r(x),s(x)\in K[x]$ with $s(x)\neq 0$? By the construction of $K(x)$, this means that $p(x)s(x)=r(x)q(x)$ in $K[x]$, which implies that $p(\alpha)s(\alpha)=r(\alpha)q(\alpha)$ in L, which means that $p(\alpha)/q(\alpha)=r(\alpha)/s(\alpha)$ in L. We therefore have a well-defined function $\chi\colon K(x)\to L$ as described. We know from Proposition 1.29 that $\chi(K(x))$ is a subfield of L and that χ gives an isomorphism $K(x)\to\chi(K(x))$, so it will suffice to show that $\chi(K(x))=K(\alpha)$. It is clear that $K=\chi(K)\subseteq\chi(K(x))$ and $\alpha=\chi(x)\in\chi(K(x))$, and by definition $K(\alpha)$ is the smallest subfield of L containing K and α, so $K(\alpha)\subseteq\chi(K(x))$. Conversely, as $K(\alpha)$ is a field containing K and α, we see that it must contain all powers of α, and then all K-linear combinations of powers; equivalently, it must contain $q(\alpha)$ for all $q\in K[x]$. If $q(x)$ is nonzero then $q(\alpha)\in K(\alpha)\setminus\{0\}=K(\alpha)^\times$, so $1/q(\alpha)\in K(\alpha)$, so $p(\alpha)/q(\alpha)\in K(\alpha)$ for all $p(x)\in K[x]$. This shows that $K(\alpha)$ contains $\chi(K(x))$, so we must have $K(\alpha)=\chi(K(x))$, as required.

Exercise 5.4: We can define a function $\mu\colon L\to L$ by $\mu(a)=\alpha a$ for all $a\in L$. This is clearly K-linear (or even L-linear, but we will not use that). Let $f(t)\in K[t]$ be the characteristic polynomial of μ. More explicitly, we can choose a basis $e_1,\dots,e_d$ for L over K, and note that there must be elements $A_{ij}\in K$ with $\mu(e_i)=\alpha e_i=\sum_j A_{ij}e_j$ for all i. This gives a matrix $A\in M_d(K)$, and thus a matrix $tI-A\in M_d(K[t])$. We then have $f(t)=\det(tI-A)$, which is a monic polynomial of degree d over K, so it can be written as $\sum_{i=0}^d c_it^i$ for some coefficients $c_i\in K$. The Cayley-Hamilton theorem then tells us that $\sum_{i=0}^d c_i\mu^i=f(\mu)=0$ as a K-linear map from L to L. As $\mu(a)=\alpha a$ (and so $\mu^2(a)=\mu(\alpha a)=\alpha^2 a$, and so on) we deduce that $\sum_{i=0}^d c_i\alpha^i a=\sum_{i=0}^d c_i\mu^i(a)=0$. In particular, we can take $a=1$ and thus deduce that $f(\alpha)=0$, so $f(x)\in I(\alpha,K)$. As f is monic we also have $f(x)\neq 0$, so $I(\alpha,K)\neq 0$ as claimed.

Exercise 5.5:

(a) If $\alpha\in\overline{\mathbb{Q}}$ then Proposition 5.8 tells us that $[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg(\min(\alpha,\mathbb{Q}))<\infty$. If $[\mathbb{Q}(\alpha):\mathbb{Q}]<\infty$ then evidently $\mathbb{Q}(\alpha)$ is an example of a subfield $K\subseteq\mathbb{C}$ with $\alpha\in K$ and $[K:\mathbb{Q}]<\infty$. If we are given such a field K, then Proposition 5.10 (applied to the extension $\mathbb{Q}\subset K$) tells us that $\alpha\in\overline{\mathbb{Q}}$. Thus, the three conditions mentioned are all equivalent.

(b) First, it is clear that $\overline{\mathbb{Q}}$ contains $\mathbb{Q}$, so $0,1\in\overline{\mathbb{Q}}$. Suppose that $\alpha,\beta\in\overline{\mathbb{Q}}$. This means that there are subfields $L,M\subset\mathbb{C}$ with $\alpha\in L$ and $\beta\in M$ and $[L:\mathbb{Q}],[M:\mathbb{Q}]<\infty$. Now Proposition 5.12 tells us that LM is a subfield of $\mathbb{C}$ containing both α and β, such that $[LM:\mathbb{Q}]<\infty$. As (iii) implies (i) above, we see that $LM\subseteq\overline{\mathbb{Q}}$. Now $\alpha+\beta$, $\alpha-\beta$ and $\alpha\beta$ all lie in LM, so they lie in $\overline{\mathbb{Q}}$. Similarly, if $\alpha\neq 0$ then $\alpha^{-1}\in L\subseteq LM\subseteq\overline{\mathbb{Q}}$. It follows that $\overline{\mathbb{Q}}$ is a subfield as claimed.

(c) Now suppose that $\alpha\in\mathbb{C}$ and α is algebraic over $\overline{\mathbb{Q}}$. We thus have a minimal polynomial $f(x)=\min(\alpha,\overline{\mathbb{Q}})(x)=\sum_{i=0}^d a_ix^i$, with $a_d=1$ and $a_i\in\overline{\mathbb{Q}}$ for all i. Now part (a) tells us that there exists a field $L_i\subset\mathbb{C}$ with $a_i\in L_i\subset\mathbb{C}$ and $[L_i:\mathbb{Q}]<\infty$. Put $L=L_0L_1\cdots L_d$, so Proposition 5.12 tells us that $[L:\mathbb{Q}]<\infty$. Moreover, as $f(\alpha)=0$ we see that $[L(\alpha):L]\leq d$, so $[L(\alpha):\mathbb{Q}]=[L(\alpha):L][L:\mathbb{Q}]<\infty$. This means that $L(\alpha)$ is a finite degree extension of $\mathbb{Q}$ containing α, so $\alpha\in\overline{\mathbb{Q}}$ by criterion (iii) above.

(d) Suppose we have a nonconstant polynomial $f(x)\in\overline{\mathbb{Q}}[x]$. We can regard this as a nonconstant polynomial over $\mathbb{C}$, so the Fundamental Theorem of Algebra tells us that there is a root (say α) in $\mathbb{C}$. Now the relation $f(\alpha)=0$ tells us that α is algebraic over $\overline{\mathbb{Q}}$, so part (c) tells us that $\alpha\in\overline{\mathbb{Q}}$. We therefore see that any nonconstant polynomial over $\overline{\mathbb{Q}}$ has a root in $\overline{\mathbb{Q}}$, which means that $\overline{\mathbb{Q}}$ is algebraically closed.

Exercise 5.6:

(a) It is a general fact that if θ is algebraic over K and the minimal polynomial has degree d, then the set $\{1,\theta,\dots,\theta^{d-1}\}$ is a basis for $K(\theta)$ over K. From this it follows that $\{1,\alpha\}$ is a basis for $\mathbb{F}_4$ over $\mathbb{F}_2$. This means that every element of $\mathbb{F}_4$ can be written as $a_0+a_1\alpha$ for some $a_0,a_1\in\mathbb{F}_2=\{0,1\}$, so

$$\mathbb{F}_4=\{0,1,\alpha,1+\alpha\}.$$

(b) Similarly, as the minimal polynomial of β over $\mathbb{F}_2$ has degree 4 we see that the set $\{1,\beta,\beta^2,\beta^3\}$ is a basis for $\mathbb{F}_{16}$ over $\mathbb{F}_2$. This gives the following list of elements of $\mathbb{F}_{16}$:

$$0,1,\beta,1+\beta,\beta^2,1+\beta^2,\beta+\beta^2,1+\beta+\beta^2,$$
$$\beta^3,1+\beta^3,\beta+\beta^3,1+\beta+\beta^3,\beta^2+\beta^3,1+\beta^2+\beta^3,\beta+\beta^2+\beta^3,1+\beta+\beta^2+\beta^3.$$

(c) As the minimal polynomial of β is $t^4+t^3+t^2+t+1$, we have $\beta^4+\beta^3+\beta^2+\beta+1=0$. If we multiply by $\beta-1$ and cancel we get $\beta^5-1=0$, so $\beta^5=1$.

(d) The homomorphisms from $\mathbb{F}_4$ to $\mathbb{F}_{16}$ biject with the roots of the minimal polynomial $g(t)=t^2+t+1=0$ in $\mathbb{F}_{16}$. As this polynomial has degree two, it can have at most two roots in any field. Thus, if we can find two roots then we need not look for any more. By working through our list of elements of $\mathbb{F}_{16}$ we find that the required roots are as follows:

$$\gamma=\beta^2+\beta^3$$
$$\delta=1+\beta^2+\beta^3.$$

Indeed, we have

$$g(\gamma)=1+\gamma+\gamma^2=1+\beta^2+\beta^3+(\beta^4+2\beta^2\beta^3+\beta^6).$$

We can discard the term $2\beta^2\beta^3$ because $2=0$ in $\mathbb{F}_2$. We also know that $\beta^5=1$, so $\beta^6=\beta$. Using these the above equation simplifies to $g(\gamma)=1+\beta+\beta^2+\beta^3+\beta^4$, but this is just the minimal polynomial evaluated at β, so $g(\gamma)=0$. A similar argument shows that $g(\delta)=0$ as well. It follows that the two homomorphisms $\phi,\psi\colon\mathbb{F}_4\to\mathbb{F}_{16}$ are given by

$$\phi(a_0+a_1\alpha)=a_0+a_1\gamma=a_0+a_1\beta^2+a_1\beta^3$$
$$\psi(a_0+a_1\alpha)=a_0+a_1\delta=a_0+a_1+a_1\beta^2+a_1\beta^3.$$

Exercise 6.1: Suppose that $\sigma(i)=i$. Transitivity means that for any $j\in N$ we can choose $\tau\in A$ with $\tau(i)=j$. As A is commutative we then have

$$\sigma(j)=\sigma(\tau(i))=\tau(\sigma(i))=\tau(i)=j.$$

As j was arbitrary, this means that σ is the identity. Thus the action is free, as claimed.

Next, as A is transitive we can choose $\sigma_i\in A$ (for $i=1,\dots,N$) such that $\sigma_i(1)=i$. Now let τ be any element of A. Put $i=\tau(1)$, and note that $\tau^{-1}\sigma_i$ sends 1 to 1. As the action is free this means that $\tau^{-1}\sigma_i=1$, so $\tau=\sigma_i$. This means that $A=\{\sigma_1,\dots,\sigma_n\}$, and these elements are all different, so $|A|=n$.

Exercise 6.2:

(a) Suppose that $f(x^2)$ is irreducible. If $f(x) = u(x)v(x)$ then $f(x^2) = u(x^2)v(x^2)$, and as $f(x^2)$ is irreducible this means that either $u(x^2)$ or $v(x^2)$ is constant, so either $u(x)$ or $v(x)$ is constant. This proves that $f(x)$ is irreducible.

(b) The polynomial $f(x) = \varphi_3(x) = x^2 + x + 1$ is irreducible, but one can check directly that $f(x^2) = f(x)f(-x)$, which shows that $f(x^2)$ is reducible.

(c) Let $\alpha_1, \dots, \alpha_d$ be the roots of $f(x)$ in $\mathbb{C}$. As $f(x)$ has degree greater than one and is irreducible, it cannot be divisible by x, so we must have $\alpha_i \neq 0$ for all i. Choose a square root β_i for α_i. We then have $f(x) = \prod_i (x - \alpha_i) = \prod_i (x - \beta_i^2)$, so

$$f(x^2) = \prod_i (x^2 - \beta_i)^2 = \prod_i (x - \beta_i)(x - (-\beta_i)).$$

It follows that $L = \mathbb{Q}(\beta_1, \dots, \beta_d)$ and

$$K = \mathbb{Q}(\alpha_1, \dots, \alpha_d) = \mathbb{Q}(\beta_1^2, \dots, \beta_d^2) \subseteq L.$$

As both K and L are normal over $\mathbb{Q}$, we know that $G(L/K)$ is a normal subgroup of $G(L/\mathbb{Q})$, and that $G(L/\mathbb{Q})/G(L/K) \simeq G(K/\mathbb{Q})$. For $\sigma \in G(L/K)$ we know that $\sigma(\beta_i)^2 = \alpha_i = \beta_i^2$, so $\sigma(\beta_i)/\beta_i \in \{1, -1\}$. We define $\chi_i(\sigma) = \sigma(\beta_i)/\beta_i$; it is not hard to check that this gives a group homomorphism $\chi_i \colon G(L/K) \to \{1, -1\}$. We can put these together to define a map $\chi \colon G(L/K) \to \{1, -1\}^d$ by $\chi(\sigma) = (\chi_1(\sigma), \dots, \chi_d(\sigma))$. As the elements β_i generate L over K, we see that χ is injective, so $G(L/K)$ is an elementary abelian 2-group. We cannot say much more than this without more information about the polynomial $f(x)$.

Exercise 6.3: Put $\alpha_1 = \sqrt{1111}$ and $\alpha_2 = \sqrt{11 + \alpha_1}$ and $\alpha_3 = \sqrt{111 + \alpha_2}$, so $K_i = K_{i-1}(\alpha_i)$.

(a) Homomorphisms $\phi_1 \colon K_1 \to \mathbb{R}$ biject with roots in $\mathbb{R}$ of the polynomial $\min(\alpha_1, K_0)(t) = \min(\sqrt{1111}, \mathbb{Q})(t) = t^2 - 1111$. These roots are $\alpha_1 \simeq 33.332$ and $-\alpha_1 \simeq -33.332$. More explicitly, there are two possible homomorphisms, namely

$$\phi_{11}(u + v\alpha_1) = u + v\alpha_1$$
$$\phi_{12}(u + v\alpha_1) = u - v\alpha_1.$$

(b) The minimal polynomial of α_2 over K_1 is $t^2 - 11 - \alpha_1$. If we apply ϕ_{11} to the coefficients of this, we just get the polynomial $t^2 - 11 - \alpha_1$ again. The extensions of ϕ_{11} biject with the roots in $\mathbb{R}$ of this polynomial, which are $\alpha_2 \simeq 6.658$ and $-\alpha_2 \simeq -6.658$. More explicitly, there are two possible extensions of ϕ_{11}, given by

$$\phi_{21}(u + v\alpha_2) = u + v\alpha_2$$
$$\phi_{22}(u + v\alpha_2) = u - v\alpha_2$$

for all $u, v \in K_1$. Alternatively, we can look back at the proof of the degree formula $[K_2 : K_0] = [K_2 : K_1][K_1 : K_0] = 2 \times 2 = 4$ and see that the list $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ is a basis for K_2 over $\mathbb{Q}$. In terms of this basis, we have

$$\phi_{21}(u + v\alpha_1 + w\alpha_2 + x\alpha_1\alpha_2) = u + v\alpha_1 + w\alpha_2 + x\alpha_1\alpha_2$$
$$\phi_{22}(u + v\alpha_1 + w\alpha_2 + x\alpha_1\alpha_2) = u + v\alpha_1 - w\alpha_2 - x\alpha_1\alpha_2$$

for all $u, v, w, x \in \mathbb{Q}$. Now consider instead extensions of the homomorphism ϕ_{12}. These again biject with the roots in $\mathbb{R}$ of a certain polynomial. To find the required polynomial, we take $\min(\alpha_2, K_1)(t) = t^2 - 11 - \alpha_1$ and apply ϕ_{12} to the coefficients, giving $t^2 - 11 + \alpha_1$. Here $11 - \alpha_1 \simeq -22.332 < 0$, so there are no such roots. This means that the homomorphism $\phi_{12} \colon K_1 \to \mathbb{R}$ cannot be extended over K_2.

(c) The minimal polynomial of α_3 over K_2 is $t^2 - 111 - \alpha_2$. If we apply ϕ_{21} to the coefficients of this, we just get the polynomial $t^2 - 111 - \alpha_2$ again. The extensions of ϕ_{21} over K_3 biject with the roots in $\mathbb{R}$ of this polynomial, which are $\alpha_3 \simeq 10.847$ and $-\alpha_3 \simeq -10.847$. More explicitly, any element $a \in K_3$ can be written as

$$a = a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_1\alpha_2 + a_4\alpha_3 + a_5\alpha_1\alpha_3 + a_6\alpha_2\alpha_3 + a_7\alpha_1\alpha_2\alpha_3,$$

and we then have

$$\begin{aligned}
\phi_{31}(a) &= a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_1\alpha_2 + a_4\alpha_3 + a_5\alpha_1\alpha_3 + a_6\alpha_2\alpha_3 + a_7\alpha_1\alpha_2\alpha_3 \\
\phi_{32}(a) &= a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_1\alpha_2 - a_4\alpha_3 - a_5\alpha_1\alpha_3 - a_6\alpha_2\alpha_3 - a_7\alpha_1\alpha_2\alpha_3.
\end{aligned}$$

Now consider instead extensions of the homomorphism ϕ_{22}. These biject with the roots in $\mathbb{R}$ of the polynomial $t^2 - 111 + \alpha_2$ (obtained by applying ϕ_{22} to the coefficients of $\min(\alpha_3, K_2)(t) = t^2 - 111 - \alpha_2$). Here $111 - \alpha_2 \simeq 104.342 > 0$ so there are two roots, say $\alpha_3' \simeq 10.214$ and $-\alpha_3' \simeq -10.214$. This gives two extensions of ϕ_{22}:

$$\begin{aligned}
\phi_{33}(a) &= a_0 + a_1\alpha_1 - a_2\alpha_2 - a_3\alpha_1\alpha_2 + a_4\alpha_3' + a_5\alpha_1\alpha_3' - a_6\alpha_2\alpha_3' - a_7\alpha_1\alpha_2\alpha_3' \\
\phi_{34}(a) &= a_0 + a_1\alpha_1 - a_2\alpha_2 - a_3\alpha_1\alpha_2 - a_4\alpha_3' - a_5\alpha_1\alpha_3' + a_6\alpha_2\alpha_3 + a_7\alpha_1\alpha_2\alpha_3.
\end{aligned}$$

(d) We now have $E_{\mathbb{Q}}(K, \mathbb{R}) = \{\phi_{31}, \phi_{32}, \phi_{33}, \phi_{34}\}$ and so $|E_{\mathbb{Q}}(K, \mathbb{R})| = 4$. On the other hand, we have $[K : \mathbb{Q}] = [K_3 : K_2][K_2 : K_1][K_1 : K_0] = 2 \times 2 \times 2 = 8$, so $|E_{\mathbb{Q}}(K, \mathbb{R})| < [K : \mathbb{Q}]$ as claimed.

(e) The same methods show that there are eight different homomorphisms from K to $\mathbb{C}$, which can be characterised as follows:

$$\begin{aligned}
\phi_{31}(\alpha_3) &= \sqrt{111 + \sqrt{11 + \sqrt{1111}}} \simeq 10.847 \\
\phi_{32}(\alpha_3) &= -\sqrt{111 + \sqrt{11 + \sqrt{1111}}} \simeq -10.847 \\
\phi_{33}(\alpha_3) &= \sqrt{111 - \sqrt{11 + \sqrt{1111}}} \simeq 10.214 \\
\phi_{34}(\alpha_3) &= -\sqrt{111 - \sqrt{11 + \sqrt{1111}}} \simeq -10.214 \\
\phi_{35}(\alpha_3) &= \sqrt{111 + \sqrt{11 - \sqrt{1111}}} \simeq 10.538 + 0.224i \\
\phi_{36}(\alpha_3) &= -\sqrt{111 + \sqrt{11 - \sqrt{1111}}} \simeq -10.538 - 0.224i \\
\phi_{37}(\alpha_3) &= \sqrt{111 - \sqrt{11 - \sqrt{1111}}} \simeq 10.214 - 0.224i \\
\phi_{38}(\alpha_3) &= -\sqrt{111 - \sqrt{11 - \sqrt{1111}}} \simeq -10.214 + 0.224i.
\end{aligned}$$

Exercise 6.4: Suppose we have $\sum_i b_i\theta_i$, or in other words $\sum_i b_i\theta_i(a) = 0$ for all $a \in L$. Taking $a = 1$ we get

(A) $$b_0 + b_1 + b_2 + b_3 = 0$$

Similarly, we can take a to be $\sqrt{p}$, $\sqrt{q}$ or $\sqrt{pq}$ to get three more equations:

$$\begin{aligned}
b_0\sqrt{p} + b_1\sqrt{p} - b_2\sqrt{p} - b_3\sqrt{p} &= 0 \\
b_0\sqrt{q} - b_1\sqrt{q} + b_2\sqrt{q} - b_3\sqrt{q} &= 0 \\
b_0\sqrt{pq} - b_1\sqrt{pq} - b_2\sqrt{pq} + b_3\sqrt{pq} &= 0.
\end{aligned}$$

After dividing by $\sqrt{p}$, $\sqrt{q}$ and $\sqrt{pq}$ respectively we get

(B) $$b_0 + b_1 - b_2 - b_3 = 0$$

(C) $$b_0 - b_1 + b_2 - b_3 = 0$$

(D) $$b_0 - b_1 - b_2 + b_3 = 0.$$

Adding (A), (B), (C) and (D) gives $b_0 = 0$. We can then add (A) and (B) to get $b_1 = 0$. Similar manipulations then give $b_2 = b_3 = 0$, as required.

Exercise 6.5:

(a) Note that α is a root of the polynomial $f(x) = x^4 - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion at the prime 2. It follows that $f(x)$ is the minimal polynomial of α over $\mathbb{Q}$, and so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x)) = 4$.

(b) Any element of $a \in K$ can be written as $a = x + iy$ with $x, y \in \mathbb{Q}(\alpha)$, and x and y are the real and imaginary part of a, so they are uniquely determined. It follows that $1, i$ is a basis for K over $\mathbb{Q}(\alpha)$, so $[K : \mathbb{Q}(\alpha)] = 2$. We see in the same way that $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

(c) We now have

$$[K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

After inserting the values obtained in (a) and (b) we see that $[K : \mathbb{Q}] = 8$ and $[K : \mathbb{Q}(i)] = 4$.

(d) We have $f(x) = (x - \alpha)(x - i\alpha)(x - i^2\alpha)(x - i^3\alpha)$ in $K[x]$, so K is a splitting field for $f(x)$ over $\mathbb{Q}(i)$, so it is normal over $\mathbb{Q}(i)$. Note also that $[K : \mathbb{Q}(i)] = [\mathbb{Q}(i, \alpha) : \mathbb{Q}(i)] = 4$, so $\min(\alpha, \mathbb{Q}(i))$ must have degree 4, so it must be the same as $f(x)$. This means that $f(x)$ is still irreducible over $\mathbb{Q}(i)$, so the Galois group acts transitively on the roots. Thus, there is an automorphism $\sigma \in G(K/\mathbb{Q}(i))$ with $\sigma(\alpha) = i\alpha$. Alternatively, we can be more concrete as follows. Every element $a \in K$ can be written in a unique way as $a = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ with $a_0, \dots, a_3 \in \mathbb{Q}(i)$. We can thus define a $\mathbb{Q}(i)$-linear map $\sigma \colon K \to K$ by

$$\sigma(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3) = a_0 + ia_1\alpha + i^2a_2\alpha^2 + i^3a_3\alpha^3.$$

It is clear that σ respects addition and sends 0 to 0 and 1 to 1. Just by expanding everything out, one can also check that $\sigma(ab) = \sigma(a)\sigma(b)$, so σ is a homomorphism. We now find that $1, \sigma, \sigma^2$ and σ^3 are all different, but that $\sigma^4 = 1$. Thus σ generates a subgroup of $G(K/\mathbb{Q}(i))$ isomorphic to C_4. As $|G(K/\mathbb{Q}(i))| = [K : \mathbb{Q}(i)] = 4$, this must be the whole group.

Exercise 6.6:

(a) Here $L = \mathbb{Q}(\mu_5)$, so we know from the general cyclotomic theory that L is Galois over $\mathbb{Q}$, and the Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{-2}, \overline{-1}, \overline{1}, \overline{2}\}$. As $\mathbb{Z}/5\mathbb{Z}$ is a field we know that $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclic. Explicitly, we have $\overline{2}^2 = \overline{4} = \overline{-1}$, and it follows easily from this that the group is generated by $\overline{2}$.

(b) Here K and L are both normal over $\mathbb{Q}$, and $G(L/\mathbb{Q}) = (\mathbb{Z}/25\mathbb{Z})^\times$ whereas $G(K/\mathbb{Q}) = (\mathbb{Z}/5\mathbb{Z})^\times$. More explicitly, we can put $\zeta = e^{2\pi i/25}$, and for each $k \in (\mathbb{Z}/25\mathbb{Z})^\times$ there is a unique automorphism σ_k of L with $\sigma_k(\zeta) = \zeta^k$. Note that $K = \mathbb{Q}(\zeta^5)$, so σ_k acts as the identity on K if and only if $\zeta^{5k} = \zeta^5$, or equivalently $5k = 5 \pmod{25}$, or equivalently $k = 1 \pmod{5}$. This means that

$$G(L/K) = \{\sigma_1, \sigma_6, \sigma_{11}, \sigma_{16}, \sigma_{21}\} = \{\sigma_{1+5i} \mid 0 \leq i < 5\}.$$

Note that σ_i only depends on i modulo 25, so

$$\sigma_{1+5i}\sigma_{1+5j} = \sigma_{1+5i+5j+25ij} = \sigma_{1+5(i+j)}.$$

It follows from this that $G(L/K)$ is cyclic of order 5, generated by σ_6.

(c) Here the polynomial $f(x) = x^5 - 12$ is irreducible over $\mathbb{Q}$ (by Eisenstein's criterion at the prime 3) and has a root in L. However, we have $L \subseteq \mathbb{R}$ and $f(x)$ has only one real root so $f(x)$ does not split in $L[x]$. It follows that L is not normal over K.

(c) This is normal, with Galois group C_5. Here is a rigorous argument (in practice, you wouldn't necessarily write down all these steps):

Firstly, observe that $[L : \mathbb{Q}] = 20$. For we have

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}]$$

and

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[5]{3})][\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}].$$

As $[K : \mathbb{Q}] = 4$ (by (a)) and $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$ (the minimal polynomial is $x^5 - 3$, irreducible by Eisenstein with $p = 3$), we see that $[L : \mathbb{Q}]$ is a multiple of 4 and of 5, so is divisible by 20. Conversely, $[L : K] = [K(\sqrt[5]{3}) : K] \leq 5$, as it is the degree of the minimal polynomial of $\sqrt[5]{3}$ over K, and this must divide $x^5 - 3$, so be of degree at most 5. As $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}]$, we see $[L : \mathbb{Q}] \leq 20$. Combining these, we get that $[L : \mathbb{Q}] = 20$ and thus that $[L : K] = 5$.

So $x^5 - 3$ is the minimal polynomial of $\sqrt[5]{3}$ over K. Write $\alpha = \sqrt[5]{3}$ and $\zeta = e^{2\pi i/5}$. The roots of the minimal polynomial are α, $\alpha\zeta$, $\alpha\zeta^2$, $\alpha\zeta^3$ and $\alpha\zeta^4$. All these roots lie in $K(\alpha)$, so it follows that $|G(K(\alpha)/K)| = 5$, and the extension is Galois.

As every group with 5 elements is cyclic, this implies that the Galois group is C_5. Explicitly, however, the 5 automorphisms are determined by the their effects on α; α must be sent to one of α, $\alpha\zeta$, $\alpha\zeta^2$, $\alpha\zeta^3$ or $\alpha\zeta^4$. It is easy to see that the automorphism sending α to $\alpha\zeta$ generates all of the automorphisms (as do any of the non-trivial automorphisms).

Exercise 7.1: The obvious basis is the set $B = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Note that

$$\frac{1}{2+\sqrt{2}+\sqrt{3}} = \frac{2+\sqrt{2}-\sqrt{3}}{(2+\sqrt{2}-\sqrt{3})(2+\sqrt{2}+\sqrt{3})} = \frac{2+\sqrt{2}-\sqrt{3}}{(2+\sqrt{2})^2-(\sqrt{3})^2} = \frac{2+\sqrt{2}-\sqrt{3}}{3+4\sqrt{2}}.$$

Here

$$\frac{1}{3+4\sqrt{2}} = \frac{3-4\sqrt{2}}{(3+4\sqrt{2})(3-4\sqrt{2})} = \frac{3-4\sqrt{2}}{3^2-(4\sqrt{2})^2} = \frac{4\sqrt{2}-3}{23}.$$

Putting this together, we get

$$\frac{1}{2+\sqrt{2}+\sqrt{3}} = (2+\sqrt{2}-\sqrt{3})(4\sqrt{2}-3)/23 = \tfrac{2}{23} + \tfrac{5}{23}\sqrt{2} + \tfrac{3}{23}\sqrt{3} - \tfrac{4}{23}\sqrt{6}.$$

Exercise 7.2: Clearly $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$. But if $\alpha = \sqrt{3}+\sqrt{5}$, then $\alpha^3 = 18\sqrt{3} + 14\sqrt{5}$, so

$$\sqrt{3} = \frac{\alpha^3 - 14\alpha}{4}$$
$$\sqrt{5} = \frac{18\alpha - \alpha^3}{4}.$$

This gives the other inclusion.

Exercise 7.3: Put $\alpha = \sqrt{p} + \sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Then

$$\alpha^2 = p + q + 2\sqrt{pq} \qquad\qquad \alpha^3 = (p+3q)\sqrt{p} + (q+3p)\sqrt{q},$$

so

$$\sqrt{p} = \frac{\alpha^3 - (q+3p)\alpha}{2(q-p)} \qquad\qquad \sqrt{q} = \frac{\alpha^3 - (p+3q)\alpha}{2(p-q)}.$$

This shows that $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. The assumed linear independence statement shows that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, so the minimal polynomial $\min(\alpha, \mathbb{Q})$ must have degree 4. We saw above that $\alpha^2 = p + q + 2\sqrt{pq}$, so $(\alpha^2 - (p+q))^2 = 4pq$, so $\alpha^4 - 2(p+q)\alpha + (p+q)^2 - 4pq = 0$. As $(p+q)^2 - 4pq = (p-q)^2$, this can be rewritten as $f(\alpha) = 0$. This means that $f(x)$ is divisible by $\min(\alpha, \mathbb{Q})$, but both these polynomials are monic of degree 4, so they must be the same. One can show in the same way that $f(\pm\sqrt{p} \pm \sqrt{q}) = 0$, for any of the four possible choices of signs. Alternatively, we can perform the following expansion:

$$\begin{aligned}
&(x-\sqrt{p}-\sqrt{q})(x-\sqrt{p}+\sqrt{q})(x+\sqrt{p}-\sqrt{q})(x+\sqrt{p}+\sqrt{q}) \\
=&((x-\sqrt{p})^2-q)((x+\sqrt{p})^2-q) = (x^2-2\sqrt{p}x+p-q)(x^2+2\sqrt{p}x+p-q) \\
=&(x^2+p-q)^2-(2\sqrt{p}x)^2 = x^4-2(p+q)x^2+(p-q)^2 = f(x).
\end{aligned}$$

Either way, we see that the roots of $f(x)$ are $\sqrt{p}+\sqrt{q}$, $\sqrt{p}-\sqrt{q}$, $-\sqrt{p}+\sqrt{q}$ and $-\sqrt{p}-\sqrt{q}$, so the splitting field of $f(x)$ is $\mathbb{Q}(\sqrt{p},\sqrt{q})$.

On the other hand, we see by inspection that

$$g(x)=(x^2-p)(x^2-q)=(x-\sqrt{p})(x+\sqrt{p})(x-\sqrt{q})(x+\sqrt{q}).$$

It is clear from this that the splitting field of $g(x)$ is also $\mathbb{Q}(\sqrt{p},\sqrt{q})$.

Exercise 7.4: Put $\alpha=\sqrt[3]{3}\in\mathbb{R}$ and $\omega=e^{2\pi i/3}=(\sqrt{-3}-1)/2$, so L can also be described as $\mathbb{Q}(\alpha,\omega)$. Put $f(t)=t^3-3\in\mathbb{Q}[t]$. This is irreducible over $\mathbb{Q}$ by Eisenstein's criterion at the prime 3, but it splits over L as $(t-\alpha)(t-\omega\alpha)(t-\omega^2\alpha)$. It follows that L is the splitting field of $f(t)$, so that the Galois group $G=G(L/\mathbb{Q})$ can be regarded as a group of permutations of the set $R=\{\alpha,\omega\alpha,\omega^2\alpha\}$. This group acts transitively on R (because $f(t)$ is irreducible), so it must be either the full group Σ_R of all permutations, or the subgroup A_R of even permutations. However, complex conjugation restricts to give an automorphism of L corresponding to the transpositon that exchanges $\omega\alpha$ and $\omega^2\alpha$. This shows that $G(L/K)\not\subseteq A_R$, so we must have $G(L/K)=\Sigma_R\simeq\Sigma_3$.

Exercise 7.5: There is an automorphism σ of L given by $z\mapsto\overline{z}$. We claim that this is the only nontrivial automorphism. To see this, write $\alpha=\sqrt[3]{3}$, so $L=\mathbb{Q}(\alpha,i)$ and

$$L\cap\mathbb{R}=\mathbb{Q}(\alpha)=\{a+b\alpha+c\alpha^2\mid a,b,c\in\mathbb{Q}\}.$$

We will need to know that $\sqrt{3}$ does not lie in L. It certainly does not appear to lie in L, but there could in principle be a strange coincidence, so we should check rigorously. As $\sqrt{3}$ is real, if it lay in L we would have $\sqrt{3}=a+b\alpha+c\alpha^2$ for some $a,b,c\in\mathbb{Q}$. Squaring this gives

$$(a^2+6bc)+(2ab+3c^2)\alpha+(2ac+b^2)\alpha^2=3,$$

so

$$\begin{aligned}a^2+6bc&=3\\2ab+3c^2&=0\\2ac+b^2&=0.\end{aligned}$$

If either of b or c is zero then the first equation gives $a^2=3$, which is impossible as a is rational. We may thus assume that b and c are nonzero, and rearrange the second and third equations as $3c^2/b=-2a=b^2/c$, and thus $3=(b/c)^3$. This is again impossible, as b/c is rational. Thus, we have $\sqrt{3}\notin L$, as expected. Now consider $\omega=e^{2\pi i/3}=(\sqrt{3}i-1)/2$. If this were in L, then $(2\omega+1)/i=\sqrt{3}$ would also be in L, which is false. So $\omega\notin L$, and similarly $\omega^{-1}\notin L$, so the only cube root of unity in L is 1.

Now let ρ be any automorphism of L. Then $\rho(i)^2+1=\rho(i^2+1)=\rho(0)=0$, so $\rho(i)=\pm i$. Similarly $(\rho(\alpha)/\alpha)^3=\rho(\alpha^3)/\alpha^3=\rho(3)/3=1$, so $\rho(\alpha)/\alpha$ is a cube root of unity in L. By the previous paragraph we therefore have $\rho(\alpha)=\alpha$. It follows that ρ is either the identity (if $\rho(i)=i$) or σ (if $\rho(i)=-i$).

As 1 and σ both act as the identity on α, we see that $G(L/\mathbb{Q}(\alpha))=G(L/\mathbb{Q})=\{1,\sigma\}$. Now $[L:\mathbb{Q}(\alpha)]=2=|G(L/\mathbb{Q}(\alpha))|$, so L is normal over $\mathbb{Q}(\alpha)$. On the other hand, $[L:\mathbb{Q}]=4>2=|G(L/\mathbb{Q})|$, so L is not normal over $\mathbb{Q}$. Explicitly, the polynomial $f(t)=t^3-3\in\mathbb{Q}[t]$ has a root in L but does not split in L.

Exercise 7.6: Put $\alpha=\sqrt[4]{3}$ and

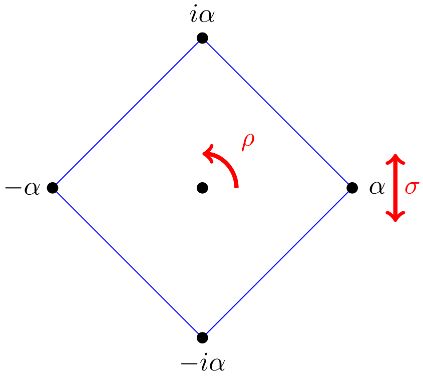
$$f(t)=(t-\alpha)(t+\alpha)(t-i\alpha)(t+i\alpha).$$

We find that $(t-\alpha)(t+\alpha)=t^2-\sqrt{3}$, but $(t-i\alpha)(t+i\alpha)=t^2+\sqrt{3}$, so $f(t)=t^4-3$. It follows easily that $L=\mathbb{Q}(\alpha,i)$ is a splitting field for $f(t)$ over $\mathbb{Q}$, so L is normal over $\mathbb{Q}$. The set $R=\{\alpha,i\alpha,-\alpha,-i\alpha\}$ of roots is the set of vertices of a square in the complex plane. We claim that the group $G(L/\mathbb{Q})$ is just the dihedral group of rotations and reflections of this square. Indeed, complex conjugation gives an automorphism σ which reflects the square across the real axis. Next, we can use Eisenstein's criterion at the prime 3 to see that $f(t)$ is irreducible, so $G(L/\mathbb{Q})$ acts transitively on R. It follows that there is an automorphism ϕ with

$\phi(\alpha) = i\alpha$. Now $\phi(i)$ must be a square root of -1, so $\phi(i) = \pm i$. If $\phi(i) = i$ then we put $\rho = \phi$, otherwise we put $\rho = \phi\sigma$. Either way we find that $\rho(i) = i$ and $\rho(\alpha) = i\alpha$. This implies that $\rho(i^m\alpha) = i^{m+1}\alpha$ for all m, so ρ is a quarter turn of the square. This means that ρ and σ generate D_8, so $|G(L/\mathbb{Q})| \geq |D_8| = 8$. On the other hand, the set

$$B = \{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$$

clearly spans L over $\mathbb{Q}$, so $[L : \mathbb{Q}] \leq |B| = 8$, and for any extension we have $|G(L/\mathbb{Q})| \leq [L : \mathbb{Q}]$. It follows that all these inequalities must be equalities, so $G(L/\mathbb{Q}) = D_8$ and B is a basis.



Exercise 7.7: We will do (a) and (b) first, and then check that $f(x)$ is irreducible.

(a) From the definition we have $2\alpha^2 + 1 = \sqrt{-15}$, and squaring again gives $4\alpha^4 + 4\alpha^2 + 16 = 0$, so $f(\alpha) = 0$. As $f(x)$ only involves even powers of x we have $f(-x) = f(x)$ and so $f(-\alpha) = 0$. Now

$$f(2/\alpha) = \frac{16}{\alpha^4} + \frac{4}{\alpha^2} + 4 = \frac{4}{\alpha^4}(4 + \alpha^2 + \alpha^4) = \frac{4}{\alpha^4} f(\alpha) = 0,$$

and similarly $f(-2/\alpha) = 0$. Numerically we have $\alpha \simeq 0.87 + 0.12i$, and from that one can check that $\alpha, -\alpha, 2/\alpha$ and $-2/al$ are all distinct. We must therefore have

$$f(x) = (x - \alpha)(x + \alpha)(x - 2/\alpha)(x + 2/\alpha).$$

(b) We have a normal extension of degree 4, so the Galois group G must have order 4. We know that G acts transitively on the roots, so there are automorphisms σ and ρ with $\sigma(\alpha) = -\alpha$ and $\rho(\alpha) = 2/\alpha$. These satisfy $\sigma^2(\alpha) = \sigma(-\alpha) = -\sigma(\alpha) = \alpha$ and $rho^2(\alpha) = \rho(2/\alpha) = 2/\rho(\alpha) = \alpha$, so $\sigma^2 = \rho^2 = 1$. We also have $\sigma(\rho(\alpha)) = \rho(\sigma(\alpha)) = -2/\alpha$. It follows that

$$G = \{1, \sigma, \rho, \sigma\rho\},$$

and this is isomorphic to $C_2 \times C_2$.

We now prove that $f(x)$ is irreducible. It is clear that $f(x) > 0$ for all $x \in \mathbb{R}$, so there are no roots in $\mathbb{Q}$. This means that the only way $f(x)$ could factor would be as the product of two quadratics, say $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ for some $a, b, c, d \in \mathbb{Q}$. By looking at the term in x^3, we see that $c = -a$. After substituting this, expanding and comparing the remaining coefficients we obtain

$$\begin{aligned} b + d - a^2 &= 1 \\ a(d - b) &= 0 \\ bd &= 4. \end{aligned}$$

If $a = 0$ we quickly obtain $b = (1 \pm \sqrt{-3})/2$, which is impossible as $b \in \mathbb{Q}$. Thus $a \neq 0$, so the second equation above gives $d = b$, so the last equation gives $b = \pm 2$. The first equation then becomes $a^2 = \pm 4 - 1$, which is impossible for $a \in \mathbb{Q}$.

Exercise 7.8:

(a) As $f(x) = x^4 \pmod{2}$ and $f(0) \neq 0 \pmod{4}$ we can use Eisenstein's criterion to see that $f(x)$ is irreducible.

(b) Note that $\alpha^2 + 4 = 3\sqrt{2} = \sqrt{18}$, and squaring again shows that $\alpha^4 + 8\alpha^2 + 16 = 18$, so $f(\alpha) = 0$. As $f(x)$ only involves even powers of x we have $f(-x) = f(x)$ and so $f(-\alpha) = 0$. Now put $\beta = \sqrt{-3\sqrt{2} - 4}$; the same argument shows that $f(\pm\beta) = 0$. We also have $(\alpha\beta)^2 = (3\sqrt{2} - 4)(-3\sqrt{2} - 4) = -2$, so $\beta = \pm\sqrt{-2}/\alpha$. (With the standard conventions for square roots we have $\alpha > 0$, and β and $\sqrt{-2}$ are positive multiples of i, and it follows that $\beta = \sqrt{-2}/\alpha$.) It follows that the roots of $f(x)$ are as described, so the splitting field is $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \alpha\beta) = \mathbb{Q}(\alpha, \sqrt{-2}) = M$ as claimed.

(c) We have $3\sqrt{2} - 4 \simeq 0.24 > 0$ so α is real, so $\mathbb{Q}(\alpha) \subseteq M \cap \mathbb{R}$. As $f(x)$ is irreducible, it must be the minimal polynomial for α, and so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x)) = 4$. As $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ and $\sqrt{-2}$ is purely imaginary we see that $1, \sqrt{-2}$ is a basis for M over $\mathbb{Q}(\alpha)$, so $M \cap \mathbb{R} = \mathbb{Q}(\alpha)$ and $[M : \mathbb{Q}] = [M : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 4 = 8$.

(d) First let $\psi \colon M \to M$ be given by complex conjugation, so $\psi(\sqrt{-2}) = -\sqrt{-2}$ and $\psi(\alpha) = \alpha$. It is clear that $\psi^2 = 1$. Next, the Galois group of the splitting field of an irreducible polynomial always acts transitively on the roots, so we can find $\sigma \in G(M/\mathbb{Q})$ with $\sigma(\alpha) = \sqrt{-2}/\alpha$. Now σ must permute the roots of $x^2 + 2$, so $\sigma(\sqrt{-2}) = \pm\sqrt{-2}$. If the sign is positive we put $\phi = \sigma\psi$, otherwise we put $\phi = \sigma$. In either case we then have $\phi(\alpha) = \sqrt{-2}/\alpha = \beta$ and $\phi(\sqrt{-2}) = -\sqrt{-2}$. This means that

$$\phi^2(\alpha) = \phi(\sqrt{-2}/\alpha) = \phi(\sqrt{-2})/\phi(\alpha) = -\sqrt{-2}/(\sqrt{-2}/\alpha) = -\alpha$$

and $\phi^2(\sqrt{-2}) = \sqrt{-2}$. It follows in turn that $\phi^4 = 1$. We now have various different automorphisms, whose effect we can tabulate as follows:

	1	ϕ	ϕ^2	ϕ^3	ψ	$\phi\psi$	$\phi^2\psi$	$\phi^3\psi$
α	α	β	$-\alpha$	$-\beta$	α	β	$-\alpha$	$-\beta$
β	β	$-\alpha$	$-\beta$	α	$-\beta$	α	β	$-\alpha$
$\sqrt{-2}$	$\sqrt{-2}$	$-\sqrt{-2}$	$\sqrt{-2}$	$-\sqrt{-2}$	$-\sqrt{-2}$	$\sqrt{-2}$	$-\sqrt{-2}$	$\sqrt{-2}.$

We see that the eight automorphisms listed are all different, but $|G(M/\mathbb{Q})| = [M : \mathbb{Q}] = 8$, so we have found all the automorphisms.

(e) We can read off from the above table that $\psi\phi\psi^{-1} = \phi^3 = \phi^{-1}$. This means that $G(M/\mathbb{Q})$ is the dihedral group D_8, with ϕ corresponding to a rotation through $\pi/2$, and ψ to a reflection.

Exercise 8.1: Recall the key fact that

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

In particular, we have

$$\begin{aligned}
x - 1 &= \varphi_1(x) \\
x^2 - 1 &= \varphi_1(x)\varphi_2(x) \\
x^4 - 1 &= \varphi_1(x)\varphi_2(x)\varphi_4(x) \\
x^5 - 1 &= \varphi_1(x)\varphi_5(x) \\
x^{10} - 1 &= \varphi_1(x)\varphi_2(x)\varphi_5(x)\varphi_{10}(x) \\
x^{20} - 1 &= \varphi_1(x)\varphi_2(x)\varphi_4(x)\varphi_5(x)\varphi_{10}(x)\varphi_{20}(x).
\end{aligned}$$

Dividing the second and third of these gives

$$\varphi_4(x) = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1.$$

On the other hand, we can divide the last two equations to give

$$\varphi_{20}(x)\varphi_4(x) = \frac{x^{20}-1}{x^{10}-1} = x^{10}+1.$$

Putting these together, we get

$$\varphi_{20}(x) = \frac{x^{10}+1}{x^2+1} = x^8 - x^6 + x^4 - x^2 + 1.$$

(The calculation can also be arranged in various other ways, but this is probably the most efficient.)

Exercise 8.2: We have

$$\begin{aligned} x^{200}-1 &= \varphi_{200}(x)\varphi_{100}(x)\varphi_{50}(x)\varphi_{40}(x)\varphi_{25}(x)\varphi_{20}(x)\varphi_{10}(x)\varphi_8(x)\varphi_5(x)\varphi_4(x)\varphi_2(x)\varphi_1(x) \\ x^{100}-1 &= \varphi_{100}(x)\varphi_{50}(x)\varphi_{25}(x)\varphi_{20}(x)\varphi_{10}(x)\varphi_5(x)\varphi_4(x)\varphi_2(x)\varphi_1(x) \\ x^{40}-1 &= \varphi_{40}(x)\varphi_{20}(x)\varphi_{10}(x)\varphi_8(x)\varphi_5(x)\varphi_4(x)\varphi_2(x)\varphi_1(x) \\ x^{20}-1 &= \varphi_{20}(x)\varphi_{10}(x)\varphi_5(x)\varphi_4(x)\varphi_2(x)\varphi_1(x) \end{aligned}$$

and it follows that

$$\varphi_{200}(x) = \frac{(x^{200}-1)(x^{20}-1)}{(x^{100}-1)(x^{40}-1)} = \frac{x^{100}+1}{x^{20}+1} = x^{80} - x^{60} + x^{40} - x^{20} + 1.$$

Exercise 8.3: Put $\zeta = e^{3\pi i/7} = (e^{2\pi i/14})^3$ and $\alpha = \zeta + 1$. As 3 and 14 are coprime, we see that ζ is a primitive 14th root of unity, and so is a root of the cyclotomic polynomial $\varphi_{14}(t)$. We know that

$$\begin{aligned} t^{14}-1 &= \varphi_{14}(t)\varphi_7(t)\varphi_2(t)\varphi_1(t) \\ t^7-1 &= \varphi_7(t)\varphi_1(t) \\ t+1 &= \varphi_2(t). \end{aligned}$$

We can divide the first of these by the second and the third to give

$$\varphi_{14}(t) = \frac{t^7+1}{t+1} = t^6 - t^5 + t^4 - t^3 + t^2 - t + 1.$$

Now put $f(t) = \varphi_{14}(t-1)$. This is again a polynomial of degree 6 over $\mathbb{Q}$, and we have $f(\alpha) = \varphi_{14}(\alpha-1) = \varphi_{14}(\zeta) = 0$. More explicitly, we can use the expression $\varphi_{14}(t) = (t^7+1)/(t+1)$ to get

$$f(t) = \frac{(t-1)^7+1}{t-1+1} = ((t-1)^7+1)/t = \sum_{i=0}^{6}(-1)^i \begin{pmatrix} 7 \\ i \end{pmatrix} t^{6-i} = t^6 - 7t^5 + 21t^4 - 35t^3 + 35t^2 - 21t + 7.$$

This reduces to t^6 modulo 7, either by inspecting the coefficients directly, or by recalling that $(t-1)^7 = t^7 - 1^7 \pmod{7}$. Moreover, the constant term is 7, which is not divisible by 7^2. Thus Eisenstein's criterion is applicable, and we see that $f(t)$ is irreducible.

Exercise 8.4: Put $\zeta = e^{2\pi i/15}$ and $K = \mathbb{Q}(\zeta) = \mathbb{Q}(\mu_{15})$. The general theory tells us that for each integer k that is coprime to 15, there is a unique automorphism σ_k of K with $\sigma_k(\zeta) = \zeta^k$, and that the rule $k + 15\mathbb{Z} \mapsto \sigma_k$ gives a well-defined isomorphism $(\mathbb{Z}/15\mathbb{Z})^\times \to G(K/\mathbb{Q})$. Every element of $\mathbb{Z}/15\mathbb{Z}$ has a unique representative lying between -7 and 7, and the integers in that range that are coprime to 15 form the set

$$U = \{-7, -4, -2, -1, 1, 2, 4, 7\},$$

so we can identify this set with $(\mathbb{Z}/15\mathbb{Z})^\times$. Put $A = \{1, -1\}$, which is a cyclic subgroup of U of order 2. Note that $2^3 = 8 = -7 \pmod{15}$ and $2^4 = 16 = 1 \pmod{15}$. It follows that the set $B = \{1, 2, 4, -7\}$ is a cyclic subgroup of U of order 4, and we see directly that $U = A \times B$.

Exercise 8.5:

(a) Put $f(x) = x^2 - \beta x + 1 \in \mathbb{Q}(\beta)[x]$. As $\beta = \zeta + \zeta^{-1}$, we see that $\beta\zeta = \zeta^2 + 1$, so $f(\zeta) = 0$. Thus, ζ satisfies a quadratic equation over $\mathbb{Q}(\beta)$, as claimed. The minimal polynomial $\min(\zeta, \mathbb{Q}(\beta))$ must divide $f(x)$, so it has degree one (if $\zeta \in \mathbb{Q}(\beta)$) or two (if $\zeta \notin \mathbb{Q}(\beta)$). Thus, we have $[\mathbb{Q}(\zeta) : \mathbb{Q}(\beta)] \leq 2$.

(b) We next observe that $\zeta^n = 1$ so $|\zeta| > 0$ and $|\zeta|^n = 1$, so $|\zeta| = 1$. If ζ is real this means that $\zeta = \pm 1$, so $\zeta^2 = 1$, but this contradicts the assumption that ζ is a primitive nth root for some $n \geq 3$. Thus, we see that $\zeta \notin \mathbb{R}$. On the other hand, as $|\zeta| = 1$ we see that $\zeta^{-1} = \overline{\zeta}$, so $\beta = \zeta + \overline{\zeta} = 2\mathrm{Re}(\zeta) \in \mathbb{R}$. It follows that $\mathbb{Q}(\beta) \subseteq \mathbb{R}$ and so $\zeta \notin \mathbb{Q}(\beta)$. In conjunction with (a) this means that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\beta)] = 2$.

(c) We claim that $\zeta^m + \zeta^{-m} = p_m(\beta)$ for some polynomial $p_m(x)$. Indeed, we can put $p_0(x) = 2$ and $p_1(x) = x$, and then define $p_m(x)$ recursively for $m > 1$ by $p_{k+1}(x) = x\, p_k(x) - p_{k-1}(x)$. We claim that $p_k(\beta) = \zeta^k + \zeta^{-k}$. This is clear for $k \in \{0, 1\}$. If the claim holds for all $k \leq m$, we have

$$\begin{aligned}
p_{m+1}(\beta) &= \beta p_m(\beta) - p_{m-1}(\beta) \\
&= (\zeta + \zeta^{-1})(\zeta^m + \zeta^{-m}) - (\zeta^{m-1} + \zeta^{1-m}) \\
&= (\zeta^{m+1} + \zeta^{1-m} + \zeta^{m-1} + \zeta^{-m-1}) - (\zeta^{m-1} + \zeta^{1-m}) \\
&= \zeta^{m+1} + \zeta^{-m-1}.
\end{aligned}$$

The claim therefore holds for all m, by induction.

(d) The first few steps of the recursive scheme are as follows:

$$\begin{aligned}
p_0(x) &= 2 \\
p_1(x) &= x \\
p_2(x) &= x\, p_1(x) - p_0(x) = x^2 - 2 \\
p_3(x) &= x\, p_2(x) - p_1(x) = x^3 - 3x \\
p_4(x) &= x\, p_3(x) - p_2(x) = x^4 - 4x^2 + 2 \\
p_5(x) &= x\, p_4(x) - p_3(x) = x^5 - 5x^3 + 5x.
\end{aligned}$$

Thus, we have $\zeta^5 + \zeta^{-5} = \beta^5 - 5\beta^3 + 5\beta$.

Exercise 8.6: Suppose that $g(t) = f(t + a)$ is irreducible as above. Suppose we have a factorisation $f(t) = p(t)q(t)$, where $p(t)$ and $q(t)$ are nonconstant polynomials in $K[t]$. We then have nonconstant polynomials $r(t) = p(t + a)$ and $s(t) = q(t + a)$ with $g(t) = r(t)s(t)$. This is impossible, because $g(t)$ is assumed to be irreducible. This means that no such factorisation $f(t) = p(t)q(t)$ can exist, so $f(t)$ must be irreducible.

Now take $f(t) = \varphi_p(t) = (t^p - 1)/(t - 1)$ and $a = 1$. We then have

$$g(t) = \frac{(t+1)^p - 1}{(t+1) - 1} = t^{-1}((t+1)^p - 1) = \sum_{i=0}^{p-1} \left(\begin{array}{c} p \\ i+1 \end{array} \right) t^i.$$

This is monic, and using Lemma 8.7 we see that $g(t) = t^{p-1} \pmod{p}$, so the coefficients of $t^0, \ldots, t^{p-2}$ are all divisible by p. Moreover, the constant term is $g(0) = p$, which is not divisible by p^2. Eisenstein's criterion therefore tells us that $g(t) = f(t + 1)$ is irreducible, so we can use the first paragraph above to see that $f(t)$ is also irreducible.

Exercise 8.7: Put $s = t^{2^k}$. As the divisors of 2^k are just the powers 2^j for $j \leq k$, we have $s - 1 = \prod_{j=0}^{k} \varphi_{2^j}(t)$. We also have $s^2 = t^{2 \times 2^k} = t^{2^{k+1}}$, so $s^2 - 1 = \prod_{j=0}^{k+1} \varphi_{2^j}(t)$. By dividing these two equations we get $\varphi_{2^{k+1}}(t) = (s^2 - 1)/(s - 1) = s + 1 = t^{2^k} + 1$ as claimed.

Alternatively, if ζ is a 2^{k+1}th root of unity, then ζ^{2^k} cannot be equal to 1 (by primitivity) but $(\zeta^{2^k})^2 = \zeta^{2^{k+1}} = 1$. We must therefore have $\zeta^{2^k} = -1$. It follows that the primitive 2^{k+1}th roots of unity are precisely the same as the roots of $t^{2^k}+1$. This polynomial is monic and coprime with its derivative, so there are no repeated roots. It follows that $t^{2^k}+1$ is the product of $t-\zeta$ as ζ runs over the roots, which is $\varphi_{2^{n+1}}(t)$.

Exercise 8.8: We will write μ_k for the set of all kth roots of unity, and $\mu_k^\times$ for the subset of primitive roots.

(a) Note that $\zeta^k=1$ if and only if $\overline{\zeta}^k=1$, so ζ and $\overline{\zeta}$ have the same order. In other words, ζ is a primitive mth root of unity if and only if $\overline{\zeta}$ is a primitive mth root of unity. Now suppose that $m>2$. The only roots of unity on the real axis are $+1$ (of order 1) and -1 (of order 2), so all primitive mth roots of unity have nonzero imaginary part. Our first observation shows that the roots with positive imaginary part biject with those of negative imaginary part, so the total number of roots is even. This number is the same as the degree of $\varphi_m(x)$.

(b) We can write $n=2m$, where m is odd. Suppose that $\zeta\in\mu_n^\times$, so $\zeta^k=1$ if and only if $n|k$. This means that $\zeta^m\neq 1$, but $(\zeta^m)^2=\zeta^n=1$, so we must have $\zeta^m=-1$. This means that $(-\zeta)^m=(-1)^m\zeta^m=(-1)^{m+1}$, which is 1 because m is odd. On the other hand, if $(-\zeta)^k=1$ then $\zeta^{2k}=(-\zeta)^{2k}=1^2=1$, so $2k$ must be divisible by $n=2m$, so k must be divisible by m. This proves that $-\zeta\in\mu_m^\times$.

Conversely, suppose that $-\zeta\in\mu_m^\times$. As m is odd we then have $\zeta^m=(-1)^m(-\zeta)^m=-1$, and thus $\zeta^n=(\zeta^m)^2=1$, so $\zeta\in\mu_n$. On the other hand, if $\zeta^k=1$ then $(-\zeta)^{2k}=(\zeta^k)^2=1$, so $2k$ is divisible by m. As m is odd this can only happen if k is divisible by m, say $k=mj$. This means that $\zeta^k=(\zeta^m)^j=(-1)^j$, but we also assumed that $\zeta^k=1$, so j must be even. As $k=mj$ this means that k is divisible by $2m=n$. This shows that $\zeta\in\mu_n^\times$.

Next, $\varphi_m(x)$ is the product of the terms $x-\zeta$ for $\zeta\in\mu_m^\times$, so $\varphi_m(-x)$ is the product of the corresponding terms $-x-\zeta$. The number of terms here is $|\mu_m^\times|$, which is even, by part (a). It therefore does not matter if we change all the signs, so $\varphi_m(x)$ is the product of the terms $x+\zeta$. Now $x+\zeta=x-(-\zeta)$, and $\{-\zeta\mid\zeta\in\mu_m^\times\}=\mu_n^\times$, so we see that $\varphi_m(-x)=\varphi_n(x)$.

(c) We can write $n=p^2m$ for some m, so $n/p=mp$. Suppose that $\zeta\in\mu_n^\times$. Then $(\zeta^p)^{mp}=\zeta^n=1$. On the other hand, if $(\zeta^p)^k=\zeta^{pk}=1$, then pk must be divisible by p^2m, so k must be divisible by pm. It follows that $\zeta^p\in\mu_{pm}^\times$.

Conversely, suppose that $\zeta^p\in\mu_{mp}^\times$. It is then clear that $\zeta^n=(\zeta^p)^{mp}=1$, so $\zeta\in\mu_n$. On the other hand, suppose that $\zeta^k=1$. Then $(\zeta^p)^k=1$, so k is divisible by mp, say $k=mpj$. Now the original relation $\zeta^k=1$ can be written as $(\zeta^p)^{mj}=1$, so mj must be divisible by mp, say $mj=mpi$. It follows that $k=mpj=p.mj=mp^2i=ni$, so k is divisible by n. This shows that $\zeta\in\mu_n^\times$ as claimed.

Now note that $\varphi_{n/p}(x^p)$ is the product of the terms $x^p-\xi$ for $\xi\in\mu_{n/p}^\times$. Here $x^p-\xi$ can be rewritten as the product of the terms $x-\zeta$, as ζ runs over the pth roots of ξ. Thus, $\varphi_{n/p}(x^p)$ is the product of all terms $x-\zeta$ for which $\zeta^p\in\mu_{n/p}^\times$, or equivalently (by what we just proved) $\zeta\in\mu_n^\times$. This means that $\varphi_{n/p}(x^p)=\varphi_n(x)$.

(d) If we start with $\varphi_p(x)$ and apply (c) repeatedly we can find $\varphi_{p^k}(x)$ for all k (and any prime p). If p is odd we can then use (b) to find $\varphi_{2p^k}(x)$, and then we can use method (c) at the prime 2 to find $\varphi_{4p^k}(x)$, $\varphi_{8p^k}(x)$ and so on. Eventually this gives $\varphi_{2^ip^j}(x)$ for all i and j. If p and q are distinct odd primes, then we cannot find $\varphi_{pq}(x)$ by this method. In particular, the first case that we do not cover is $\varphi_{15}(x)$. However, if we compute $\varphi_{pq}(x)$ by some other method then using (b) and (c) we can find $\varphi_{2^ip^jq^k}(x)$.

(e) Let N be the smallest number such that $\varphi_N(x)$ has a coefficient not in $\{0,1,-1\}$. If N is divisible by p^2 for some prime p, then $\varphi_N(x)=\varphi_{N/p}(x^p)$ by (c). Here $N/p<N$ so (by the definition of N) the coefficients of $\varphi_{N/p}(x)$ are all in $\{0,1,-1\}$. It follows that the same is true of $\varphi_{N/p}(x^p)$, which gives a contradiction. Thus, N cannot be divisible by p^2 for any p, so N is a product of distinct primes. If one of these primes is 2 then the remaining primes are odd, so (b) is applicable and $\varphi_N(x)=\varphi_{N/2}(-x)$, which again gives a contradiction. Thus, N must be a product of distinct odd primes. There must be more than one prime factor, because of the rule $\varphi_p(x)=\sum_{i=0}^{p-1}x^i$.

(f) The first few numbers that are products of at least two odd primes are

$$15, 21, 33, 35, 39, 51, 65, 69, 77, 85, 87, 91, 93, 95, 105.$$

We can ask Maple to calculate the corresponding cyclotomic polynomials, and we find that they all have coefficients in $\{0, 1, -1\}$ until we get to $\varphi_{105}(x)$. This has degree 48 and involves $-2t^7$ and $-2t^{41}$, so $N = 105$. In fact $105 = 3 \times 5 \times 7$, which is the smallest number that is a product of three distinct odd primes.

Alternatively, we can make Maple do all the work automatically, as follows:

```
for n from 1 to 1000 do
 f := numtheory[cyclotomic](n,x);
 A := {coeffs(f,x)} minus {0,1,-1};
 if nops(A) > 0 then
  print([n,sort(f)]);
  break;
 fi:
od:
```

Exercise 8.9: We can reorganise the definition and use the geometric progression formula as follows:

$$\begin{aligned}
f(x) &= (1-x)\left(\sum_{i=0}^{q-1} x^{ip}\right)\left(\sum_{j=0}^{p-1} x^{jq}\right)\left(\sum_{k=0}^{\infty} x^{kpq}\right) \\
&= (1-x)\frac{x^{pq}-1}{x^p-1}\frac{x^{pq}-1}{x^q-1}\frac{1}{1-x^{pq}} = \frac{(x-1)(x^{pq}-1)}{(x^p-1)(x^q-1)} \\
&= \frac{\varphi_1(x)\varphi_{pq}(x)\varphi_p(x)\varphi_q(x)\varphi_1(x)}{\varphi_p(x)\varphi_1(x)\varphi_q(x)\varphi_1(x)} = \varphi_{pq}(x).
\end{aligned}$$

Now consider an arbitrary natural number m. The element $m/p \in \mathbb{F}_q$ is represented by some $i \in \{0, \ldots, q-1\}$, and the element $m/q \in \mathbb{F}_p$ is represented by some $j \in \{0, \ldots, p-1\}$. We find that $m-(ip+jq)$ is divisible by both p and q, so $m = ip + jq + kpq$ for some $k \in \mathbb{Z}$. We define $\lambda(m)$ to be 1 if $k \geq 0$, and 0 if $k < 0$. Note that $ip + jq \leq (q-1)p + (p-1)q < 2pq$, so $\lambda(m) = 1$ for $m \geq 2pq$. The definition of $f(x)$ can now be rewritten as

$$f(x) = \sum_{m=0}^{\infty} \lambda(m)(x^m - x^{m+1}) = \sum_{m=0}^{\infty} (\lambda(m) - \lambda(m-1))x^m.$$

It follows that all the coefficients of $f(x)$ are in $\{0, 1, -1\}$. We also see that for $m > 2pq$ we have $\lambda(m) - \lambda(m-1) = 1 - 1 = 0$, so $f(x)$ is a polynomial as expected.

Exercise 8.10:

- Any automorphism is uniquely determined by its effect on α and on ζ. The image of α must be a root of $x^5 - 2$, so must be one of α, $\zeta\alpha$, $\zeta^2\alpha$, $\zeta^3\alpha$ or $\zeta^4\alpha$. In the same way, the image of ζ must be another primitive 5th root of unity, i.e., a root of φ_5, so is one of ζ, ζ^2, ζ^3 or ζ^4. This gives 20 possible automorphisms, θ_{ij} say, defined by

$$\begin{aligned}
\theta_{ij}(\zeta) &= \zeta^i \\
\theta_{ij}(\alpha) &= \zeta^j\alpha
\end{aligned}$$

for $i = 1$, 2, 3 or 4 and $j = 0$, 1, 2, 3 or 4. As the extension $\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}$ is Galois and has degree 20, these are all of the automorphisms.
- The automorphism ψ which fixes ζ and maps α to $\zeta\alpha$ is clearly of order 5. The automorphism ϕ which fixes α and maps ζ to ζ^2 is of order 4 because $\phi^2(\zeta) = \phi(\zeta^2) = \zeta^4$, and so $\phi^4(\zeta) = \phi^2(\zeta^4) = (\zeta^4)^4 = \zeta$.

The group generated by ϕ and ψ has as subgroups $\langle\phi\rangle$ and $\langle\psi\rangle$ so its order must be a multiple of 4 and of 5 by Lagrange's Theorem. It follows that this group must have order 20, so is the whole Galois group.

- We have:
  $$\phi\psi\phi^{-1}(\alpha) = \phi\psi(\alpha) = \phi(\zeta\alpha) = \phi(\zeta)\phi(\alpha) = \zeta^2.\alpha$$
  $$\phi\psi\phi^{-1}(\zeta) = \phi\psi(\zeta^3) = \phi(\zeta^3) = \zeta$$
  It follows that $\phi\psi\phi^{-1} = \psi^2$.
- We see that
  $$\zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = 0.$$
  Rearranging, we get
  $$(\zeta + \frac{1}{\zeta})^2 + (\zeta + \frac{1}{\zeta}) - 1 = 0.$$
  It follows that β is a root of $X^2 + X - 1$, and so $\beta = \frac{-1\pm\sqrt{5}}{2}$, from the quadratic formula. It is then easy to see that $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{5})$.

  $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$, so the index of the corresponding subgroup of $\mathrm{Gal}(M/\mathbb{Q})$ must be 2, so its order must be 10.
- The group $\langle\phi^2, \psi\rangle$ is of order 10 (it contains an element of order 2, and an element of order 5, so its order must be a multiple of 10 – but it isn't the whole group, as it doesn't contain ϕ). Let G be the subgroup associated to $\mathbb{Q}(\beta)$. If we can show that β is fixed by both ϕ^2 and by ψ, we will know that $\langle\phi^2, \psi\rangle \subseteq G$. But by the previous part of the question, $|G| = 10$, and so we have to have $G = \langle\phi^2, \psi\rangle$, as required.

  But this is easy to check:
  $$\phi^2(\beta) = \phi^2(\zeta) + \tfrac{1}{\phi^2(\zeta)} = \zeta^{-1} + \tfrac{1}{\zeta^{-1}} = \tfrac{1}{\zeta} + \zeta = \beta$$
  $$\psi(\beta) = \psi(\zeta) + \tfrac{1}{\psi(\zeta)} = \zeta + \tfrac{1}{\zeta} = \beta.$$

Exercise 8.11:

- $L = \mathbb{Q}(\alpha, \zeta)$, where $\zeta = e^{2\pi i/7}$ and α is the real 7th root of 3. Any automorphism must send ζ to another primitive 7th root of unity, and send α to a 7th root of 3.

  There is an automorphism ψ which fixes ζ but maps α to $\zeta\alpha$. Clearly ψ is of order 7, as doing ψ seven times fixes α.

  Further, there is an automorphism ϕ which fixes α but sends ζ to ζ^3. Applying ϕ successively to ζ we see that ζ is sent successively to
  $$\zeta \mapsto \zeta^3 \mapsto \zeta^2 \mapsto \zeta^6 \mapsto \zeta^4 \mapsto \zeta^5 \mapsto \zeta \mapsto \cdots$$
  so ϕ has order 6.
- Further,
  $$\phi\psi\phi^{-1}(\alpha) = \phi\psi(\alpha) = \phi(\zeta\alpha) = \phi(\zeta)\phi(\alpha) = \zeta^3\alpha = \psi^3(\alpha)$$
  and
  $$\phi\psi\phi^{-1}(\zeta) = \phi\psi(\zeta^5) = \phi(\zeta^5) = \zeta = \psi^3(\zeta)$$
  Thus $\phi\psi\phi^{-1} = \psi^3$.
- Finally, it remains to see that ϕ and ψ generate the whole Galois group. But the Galois group has order 42, and the subgroup generated by ϕ and ψ has order which is a multiple of both 6 and 7, so it must be the whole group.

Exercise 9.1: By the general theory of finite fields, we see that $\mathbb{F}_{11}^\times$ is cyclic of order 10, generated by some element α say. It follows that the subgroup generated by α^2 is cyclic of order 5.

In general, if K is a finite field then $|K^\times| + 1 = |K|$, which is a power of a prime. As $5 + 1$ is not a power of a prime, we see that $|K^\times|$ cannot be 5, so $K^\times$ cannot be isomorphic to C_5.

Exercise 9.2: In $\mathbb{F}_3$ we have $\varphi_8(0) = 1 \neq 0$ and $\varphi_8(\pm 1) = 2 = -1 \neq 0$, so $\varphi_8(t)$ has no roots in $\mathbb{F}_3$, and thus has no factors of degree one in $\mathbb{F}_3[t]$. Thus, the only way it can factor is as the product of two quadratic polynomials, say

$$t^4 + 1 = (t^2 + at + b)(t^2 + ct + d) = t^4 + (a + c)t^3 + (b + d + ac)t^2 + (ad + bc)t + bd.$$

By comparing coefficients we get

$$\begin{aligned} a + c &= 0 \\ b + d + ac &= 0 \\ ad + bc &= 0 \\ bd &= 1. \end{aligned}$$

The last equation shows that $b \neq 0$, so $b = \pm 1$, so $b^2 = 1$. We can thus multiply the last equation by b to see that $d = b$. On the other hand, the first equation gives $c = -a$. Substituting these into the second equation and rearranging gives $b = -a^2$. Here $a \in \{0, 1, -1\}$ so $-a^2 \in \{0, -1\}$ but we already know that $d = b \neq 0$ so $d = b = -1$. As $b = -a^2$ we have $a \in \{1, -1\}$, and we have seen that $c = -a$. We can arbitrarily choose to take $a = 1$ and then $c = -1$, so we have the factorisation

$$\varphi_8(t) = t^4 + 1 = (t^2 + t - 1)(t^2 - t - 1) \in F_3[t].$$

This gives two fields of order 9:

$$\begin{aligned} K &= \mathbb{F}_3[\alpha]/(\alpha^2 + \alpha - 1) \\ L &= \mathbb{F}_3[\beta]/(\beta^2 - \beta - 1). \end{aligned}$$

Now consider the field $\mathbb{F}_3[i]$ and the group

$$\mathbb{F}_3[i]^\times = \{1, -1, i, -i, 1 + i, 1 - i, -1 + i, -1 - i\} \simeq C_8.$$

The elements $1, -1, i$ and $-i$ are the roots of $t^4 - 1$, so the remaining elements are roots of $(t^8 - 1)/(t^4 - 1) = t^4 + 1 = \varphi_4(t)$. One checks that the elements $1 \pm i$ are roots of $t^2 + t - 1$, and the elements $-1 \pm i$ are roots of $t^2 - t - 1$. There is thus a unique isomorphism $\phi\colon K \to \mathbb{F}_3[i]$ with $\phi(\alpha) = 1 + i$, and a unique isomorphism $\psi\colon L \to \mathbb{F}_3[i]$ with $\psi(\beta) = -1 - i = -\phi(\alpha)$. It follows that the composite isomorphism $\psi^{-1}\phi\colon K \to L$ sends α to $-\beta$.

Exercise 9.3: Put $\alpha = \left[\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right]$, and identify each element $a \in \mathbb{F}_5$ with the matrix $aI = \left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right]$. The set K then consists of all matrices $a + b\alpha$ with $a, b \in \mathbb{F}_5$. It is clear that this is a vector space of dimension two over $\mathbb{F}_5$, and so has order $5^2 = 25$. Next, observe that

$$\begin{aligned} \alpha^2 &= \left[\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 3 & 2 \\ 4 & 3 \end{smallmatrix}\right] \\ 2\alpha + 1 &= 2\left[\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right] + \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 3 & 2 \\ 4 & 3 \end{smallmatrix}\right] = \alpha^2. \end{aligned}$$

It follows that

$$\begin{aligned} (a + b\alpha)(c + d\alpha) &= ac + (ad + bc)\alpha + bd\alpha^2 = ac + (ad + bc)\alpha + bd(2\alpha + 1) \\ &= (ac + bd) + (ad + bc + 2bd)\alpha \in K, \end{aligned}$$

so K is closed under multiplication. We also see from the above formulae that $(a + b\alpha)(c + d\alpha) = (c + d\alpha)(a + b\alpha)$, so multiplication in K is commutative. The remaining parts of Definition 1.1(b) are standard properties of matrix addition and multiplication. We therefore see that K is a commutative ring. All that is left is to check that it is a field. To see this, put $f(x) = x^2 - 2x - 1 \in \mathbb{F}_5[x]$, so $f(\alpha) = 0$, so there is a unique homomorphism ϕ from the ring $K' = K[x]/f(x)$ to K with $\phi(x + K[x]f(x)) = \alpha$. We also have

$$\begin{aligned} f(0) &= -1 \\ f(1) &= -2 \\ f(2) &= -1 \\ f(3) &= 2 \\ f(4) &= 2 \end{aligned}$$

so $f(x)$ has no roots in $\mathbb{F}_5$. As it is quadratic and has no roots, it must be irreducible, so K' is a field. As $1, x$ gives a basis for K' over $\mathbb{F}_5$, and $1, \alpha$ gives a basis for K over $\mathbb{F}_5$, we see that ϕ is an isomorphism. This means that K is also a field.

Exercise 9.4: Proposition 8.11 tells us that $G(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$, which is cyclic of order $p-1$ by Corollary 9.13.

Exercise 9.5: We have $\mathbb{F}_7^\times = \{-3, -2, -1, 1, 2, 3\}$, and we check that

$$3^0 = 1 \qquad 3^1 = 3 \qquad 3^2 = 2 \qquad 3^3 = -1 \qquad 3^4 = -3 \qquad 3^5 = -2.$$

It follows that $\mathbb{F}_7^\times$ is a cyclic group of order 6, generated by 3. It follows that for every $a \in \mathbb{F}_7^\times$ we have $a^6 = 1$, so $(a^3)^2 = 1$. Thus, if $b^2 \neq 1$ then b is not the cube of any element in $\mathbb{F}_7^\times$. In particular, 3 is not a cube. (We could also have checked this by just writing out the cubes of all elements.) Thus, the polynomial $f(t) = t^3 - 3$ has not roots in $\mathbb{F}_7$. Any nontrivial factorisation would have to involve a quadratic term and a linear term, which would thus give a root; so $f(t)$ must be irreducible. We therefore have a field $K = \mathbb{F}_7[\alpha]/(\alpha^3 - 3)$ of order $7^3 = 343$. Now $\alpha^3 = 3$ and $3^6 = 1$, so $\alpha^{18} = 1$, but the whole group $K^\times$ has order 342, so α does not generate $K^\times$.

Exercise 9.6: We first remark that $\mathbb{F}_5 = \{-2, -1, 0, 1, 2\}$, with $(\pm 1)^2 = 1$ and $(\pm 2)^2 = 4 = -1$. It follows that 2 is a generator of $\mathbb{F}_5^\times$. We also see that $2^3 = 8 = -2$, so we can write

$$f(x) = (x^2)^3 + 2^3 = (x^2 + 2)(x^4 - 2x^2 + 4) = (x^2 + 2)(x^4 - 2x^2 - 1).$$

We can thus take $g_1(x) = x^2 + 2$. For the other two factors, suppose that $g_2(x) = x^2 + ax + b$ and $g_3(x) = x^2 + cx + d$. We should then have

$$x^4 - 2x^2 - 1 = g_2(x)g_3(x) = x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd.$$

By comparing coefficients, we get

$$\begin{aligned} a + c &= 0 \\ b + d + ac &= -2 \\ ad + bc &= 0 \\ bd &= -1. \end{aligned}$$

If $a = 0$ then these equations reduce to $c = 0$ and $d = -2 - b$ and $bd = -1$. By checking through the five possible values of b, we see that these equations are inconsistent. Thus, we must have $a \neq 0$. The first equation gives $c = -a$, and we can feed this into the third equation to get $a(d - b) = 0$, but $a \neq 0$ so $d = b$. The last equation now says that $b^2 = -1$, and it follows that $b = \pm 2$. The second equation can now be rearranged as $a^2 = 2b + 2$. If $b = -2$ this gives $a^2 = -2$, but -2 is not a square in $\mathbb{F}_5$, so this is impossible. If $b = 2$ then we get $a^2 = 6 = 1$, so $a = \pm 1$. We should therefore take

$$\begin{aligned} g_2(x) &= x^2 + x + 2 \\ g_3(x) &= x^2 - x + 2. \end{aligned}$$

One can then check directly that $f(x) = g_1(x)g_2(x)g_3(x)$ as expected.

Note that 2 is not a square in $\mathbb{F}_5$, so it is certainly not a sixth power, so $f(x)$ has no roots in $\mathbb{F}_5$. It follows that $g_i(x)$ has no roots, and a quadratic with no roots is irreducible, so the three factors $g_i(x)$ are irreducible as claimed.

Now suppose we have an extension field K and an element $\alpha \in K$ with $g_i(\alpha) = 0$. Let d be the multiplicative order of α, so we have $\alpha^m = 1$ if and only if m is divisible by d. As $g_i(x)$ is a factor of $f(x)$ we see that $f(\alpha) = 0$, so $\alpha^6 = 2$, so $\alpha^{12} = 4 = -1$ and $\alpha^{24} = 1$. It follows that d divides 24 but d does not divide 12; the only possibilities are $d = 8$ or $d = 24$. In fact, if $g_1(\alpha) = 0$ then $\alpha^2 = -2$ and it follows easily that $\alpha^8 = 1$, so $d = 8$. On the other hand, if $g_2(\alpha) = 0$ or $g_3(\alpha) = 0$ then $\alpha^8 = \alpha^6\alpha^2 = 2\alpha^2 = 2(\pm\alpha - 2) \neq 1$, so d must be 24.

Exercise 9.7: As $f(\alpha) = 0$ we have $\alpha^p = \alpha + 1$. We can raise this to the pth power (remembering that $(x + y)^p = x^p + y^p \pmod{p}$) to get $\alpha^{p^2} = \alpha^p + 1$, and then use $\alpha^p = \alpha + 1$ again to get $\alpha^{p^2} = \alpha + 2$. By continuing in the same way, we find that $\alpha^{p^k} = \alpha + k$ for all k. In particular, for $0 < k < p$ this gives $\alpha^{p^k} \neq \alpha$.

Now let $g(x)$ be the minimal polynomial of α over $\mathbb{F}_p$, which is an irreducible factor or $f(x)$. If $g(x)$ has degree d, we have $|K| = p^d$. By the general theory of finite fields, we have $a^{p^d} = a$ for all $a \in K$. In particular $\alpha^{p^d} = \alpha$, so by our first paragraph we must have $d \geq p$. On the other hand, $g(x)$ divides $f(x)$ and $f(x)$ has degree p, so we must have $d \leq p$. We deduce that $d = p$ and $f(x) = g(x)$, so $f(x)$ is irreducible.

Exercise 9.8: Let K be a finite field. We then have $|K| = p^d$, for some prime p and $d > 0$. We have seen that $a^{p^d} = a$ for all $a \in K$. Put $f(x) = x^{p^d} - x + 1 \in K[x]$, so $f(a) = 1$ for all $a \in K$. It follows that $f(x)$ has no roots in K, so K is not algebraically closed.

Exercise 11.1: Put $A = G(L/(L^H L^K)) \leq G$. Every automorphism $\sigma \in A$ acts as the identity on $L^H L^K$, so in particular it acts as the identity on $L^H \subseteq L$, which means that $A \leq G(L/L^H) = H$. By the same argument we have $A \subseteq G(L/L^K) = K$, so in fact $A \subseteq H \cap K$. Conversely, suppose that $\sigma \in H \cap K$. Any element $a \in L^H L^K$ can be written as $a = b_1c_1 + \cdots + b_rc_r$ with $b_i \in L^H$ and $c_i \in L^K$. We have $\sigma(b_i) = b_i$ (because $\sigma \in H$) and $\sigma(c_i) = c_i$ (because $\sigma \in K$). It follows that $\sigma(a) = a$ for all $a \in L^H L^K$, so $\sigma \in A$. This means that $A = H \cap K$. The Galois Correspondence tells us that for all M with $K \leq M \leq L$ we have $M = L^{G(L/M)}$. By taking $M = L^H L^K$ we see that $L^H L^K = L^A = L^{H\cap K}$ as claimed.

Exercise 11.2: Choose elements ρ and σ that generate $G(L/K)$, so $G(L/K) = \{1, \rho, \sigma, \rho\sigma\}$ with $\rho^2 = \sigma^2 = 1$ and $\rho\sigma = \sigma\rho$. Put $G = G(L/K)$ and

$$\begin{array}{ccc} A = \{1, \rho\} & B = \{1, \sigma\} & C = \{1, \rho\sigma\} \\ M = L^A & N = L^B & P = L^C. \end{array}$$

Then A, B and C are the only proper nontrivial subgroups of G, so M, N and P are the only fields strictly between K and L. As G is abelian, we see that all subroups are normal, so M, N and P are normal over $\mathbb{Q}$, with Galois groups G/A, G/B and G/C respectively. All of these are of order 2. As $\sigma \notin A$, we see that σ acts nontrivially on M, so we can choose $\mu \in M$ with $\sigma(\mu) \neq \mu$. It follows that the element $\alpha = \mu - \sigma(\mu)$ is nonzero, and it satisfies $\sigma(\alpha) = -\alpha$. It follows that $\alpha \notin K$, and $[M : K] = |G/A| = 2$, so 1 and α must give a basis for M over K, so $M = K(\alpha)$. We also have $\sigma(\alpha^2) = \alpha^2$, and so $\alpha^2 \in M^{G/A} = K$. Similarly, there is an element $\beta \in N$ such that $1, \beta$ is a basis for N over K, and $\rho(\beta) = -\beta$, and $\beta^2 \in K$. Note that $\rho(\alpha) = \alpha$ (as $\alpha \in M$) and $\sigma(\beta) = \beta$ (as $\beta \in N$). It follows that $\rho(\sigma(\alpha\beta)) = (-\alpha)(-\beta) = \alpha\beta$, so $\alpha\beta \in P$.

We next claim that the list $1, \alpha, \beta, \alpha\beta$ is linearly independent over K. To see this, suppose that $a = w + x\alpha + y\beta + z\alpha\beta$ for some $w, x, y, z \in K$. We can use the above formulae to understand $\sigma(a)$ and $\rho(a)$, and we find that

$$\begin{aligned} a+\rho(a)+\sigma(a)+\rho\sigma(a) &= 4w \\ a+\rho(a)-\sigma(a)-\rho\sigma(a) &= 4x\alpha \\ a-\rho(a)+\sigma(a)-\rho\sigma(a) &= 4y\beta \\ a-\rho(a)-\sigma(a)+\rho\sigma(a) &= 4z\alpha\beta. \end{aligned}$$

Thus, if $w+x\alpha+y\beta+z\alpha\beta=0$ we see that $w=x=y=z=0$. This shows that the list $\mathcal{B}=1,\alpha,\beta,\alpha\beta$ is linearly independent list, but $\dim_K(L)=|G|=4$, so $\mathcal{B}$ must actually be a basis.

$$\begin{tikzcd}
1 & & \{1\} \arrow[dl] \arrow[d] \arrow[dr] & & & L & \\
2 & A \arrow[dr] & B \arrow[d] & C \arrow[dl] & K(\alpha) \arrow[ur] & K(\beta) \arrow[u] & K(\alpha\beta) \arrow[ul] \\
4 & & G & & & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Exercise 11.3: Since $\zeta^4+\zeta^3+\zeta^2+\zeta+1=0$, we have $\zeta^2+\zeta+1+\zeta^{-1}+\zeta^{-2}=0$. Since $\alpha^2=\zeta^2+2+\zeta^{-2}$, we see that $\alpha^2+\alpha-1=0$. Thus α is one of the roots of $x^2+x-1=0$, namely, $\alpha=(-1\pm\sqrt{5})/2$. However, $\zeta+\zeta^{-1}=\zeta+\overline{\zeta}=2\cos(2\pi/5)>0$, so we must have $\alpha=(-1+\sqrt{5})/2$. It follows that $\sqrt{5}=2\alpha+1=2\zeta+2\zeta^{-1}+1$, so $\sqrt{5}=2\alpha+1\in\mathbb{Q}(\zeta)$.

Next, we have

$$\beta^2=\zeta^2-2+\zeta^{-2}=\alpha^2-4=\left(\frac{-1+\sqrt{5}}{2}\right)^2-4=\frac{6-2\sqrt{5}}{4}-4=-\frac{1+\sqrt{5}}{2}.$$

We also observe that $\sin(2\pi/5)>0$, and recall that when $t<0$ the symbol $\sqrt{t}$ refers to the square root in the upper half plane; we thus have $\beta=\sqrt{-(1+\sqrt{5})/2}$.

We now put $G=G(\mathbb{Q}(\mu_5)/\mathbb{Q})$ and look at the subgroup lattice. We know that

$$G=G(\mathbb{Q}(\mu_5)/\mathbb{Q})=\{\sigma_k\mid k\in(\mathbb{Z}/5\mathbb{Z})^\times\}==\{\sigma_{-2},\sigma_{-1},\sigma_1,\sigma_2\},$$

and this is cyclic of order 4, generated by σ_2. It follows that the only subgroups are the trivial group, the whole group, and the subgroup $A=\{\overline{1},\overline{-1}\}$. This means that the only subfields are $\mathbb{Q}(\mu_5)$, $\mathbb{Q}$ and the intermediate field $M=\mathbb{Q}(\mu_5)^A$. Now σ_{-1} exchanges ζ and ζ^{-1} so it fixes α and sends β to $-\beta$. We therefore see that $M=\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{5})$, and that $\mathbb{Q}(\beta)$ cannot be M so it must be all of $\mathbb{Q}(\zeta)$. (In fact, one can check that $\zeta=(\beta-\beta^2-3)/2$, which shows more explicitly that $\mathbb{Q}(\beta)=\mathbb{Q}(\zeta)$.)

The lattices can now be displayed as follows:

$$\begin{tikzcd}
1 & \{1\} \arrow[d] & \mathbb{Q}(\sqrt{-(1+\sqrt{5})/2}) \\
2 & H \arrow[d] & \mathbb{Q}(\sqrt{5}) \arrow[u] \\
4 & G & \mathbb{Q} \arrow[u]
\end{tikzcd}$$

Exercise 11.4:

(a) Since $\zeta^{10} = \zeta^{-1}$ etc., we can rewrite the given equation as

$$\zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} + \zeta^{-3} + \zeta^{-4} + \zeta^{-5} = 0.$$

Now

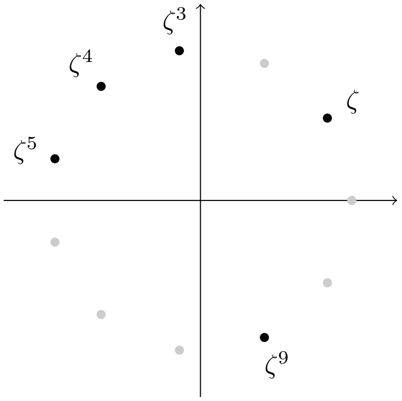
$$\begin{array}{lclllllllllll}
\beta & = & & & & & \zeta & & +\zeta^{-1} & & & & \\
\beta^2 & = & & & & \zeta^2 & & +2 & & +\zeta^{-2} & & & \\
\beta^3 & = & & & \zeta^3 & & +3\zeta & & +3\zeta^{-1} & & +\zeta^{-3} & & \\
\beta^4 & = & & \zeta^4 & & +4\zeta^2 & & +6 & & +4\zeta^{-2} & & +\zeta^{-4} & \\
\beta^5 & = & \zeta^5 & & +5\zeta^3 & & +10\zeta & & +10\zeta^{-1} & & +5\zeta^{-3} & & +\zeta^{-5}.
\end{array}$$

By combining these, we find that $\beta^5 + \beta^4 - 4\beta^3 - 3\beta^2 + 3\beta + 1 = 0$.

(b) We have

$$\begin{aligned}
\gamma^2 &= \zeta^2 + \zeta^8 + \zeta^7 + \zeta^{10} + \zeta^6 + \\
&\qquad 2(\zeta^5 + \zeta^{10} + \zeta^6 + \zeta^4 + \zeta^2 + \zeta^9 + \zeta^7 + \zeta^3 + \zeta + \zeta^8) \\
&= (-1 - \zeta - \zeta^3 - \zeta^4 - \zeta^5 - \zeta^9) + 2(-1) \\
&= -3 - \gamma,
\end{aligned}$$

so $\gamma^2 + \gamma + 3 = 0$. Since γ is a root of $x^2 + x + 3 = 0$, we see that $\gamma = (-1 \pm \sqrt{-11})/2$. The terms in γ are distributed in the complex plane as follows:



It is clear from this that the imaginary part of γ is positive, so $\gamma = (-1+\sqrt{-11})/2$, so $\sqrt{-11} = 2\gamma+1$. It is also clear from the definition that $\gamma \in \mathbb{Q}(\zeta)$, so $\sqrt{-11} \in \mathbb{Q}(\zeta)$.

(c),(d) The general cyclotomic theory says that $G(K/\mathbb{Q}) = \{\sigma_k \mid k \in (\mathbb{Z}/11)^\times\}$. We have

$$(\mathbb{Z}/11)^\times = \{-5, -4, -3, -2, -1, 1, 2, 3, 4, 5\}.$$

The powers of 2 mod 11 are as follows:

$$2^0 = 1,\ \ 2^1 = 2,\ \ 2^2 = 4,\ \ 2^3 = -3,\ \ 2^4 = 5,\ \ 2^5 = -1,\ \ 2^6 = -2,\ \ 2^7 = -4,\ \ 2^8 = 3,\ \ 2^9 = -5,\ \ 2^{10} = 1.$$

This shows that $(\mathbb{Z}/11)^\times$ is cyclic of order 10, generated by 2, and thus $G(K/\mathbb{Q})$ is cyclic of order 10, generated by σ_2. We write

$$\begin{aligned}
C_{10} &= G(K/\mathbb{Q}) = \langle \sigma_2 \rangle \\
C_5 &= \langle \sigma_2^2 \rangle = \langle \sigma_4 \rangle = \{1, \sigma_4, \sigma_5, \sigma_{-2}, \sigma_3\} \\
C_2 &= \langle \sigma_2^5 \rangle = \langle \sigma_{-1} \rangle = \{1, \sigma_{-1}\} \\
C_1 &= \{1\}.
\end{aligned}$$

These are all the subgroups of the Galois group. It follows that the only subfields of K are $K^{C_{10}} = \mathbb{Q}$, K^{C_5}, K^{C_2} and $K^{C_1} = K$. The terms in γ are precisely the orbit of ζ under C_5, so $\gamma \in K^{C_5}$, so $\sqrt{-11} \in K^{C_5}$. We also know that $[K^{C_5} : \mathbb{Q}] = |C_{10}|/|C_5| = 2$, which is the same as the degree of $\mathbb{Q}(\sqrt{-11})$, so we must have $K^{C_5} = \mathbb{Q}(\sqrt{-11})$. Similarly, we have

$$\sigma_{-1}(\beta) = \sigma_{-1}(\zeta) + \sigma_{-1}(\zeta)^{-1} = \zeta^{-1} + \zeta = \beta,$$

so $\beta \in K^{C_2}$, and it follows that $K^{C_2} = \mathbb{Q}(\beta)$. The subgroup and subfield lattices can thus be displayed as follows:

$$\begin{tikzcd}
1 & & & \{1\} \arrow[dr] \arrow[ddll] & & & & \mathbb{Q}(\mu_{11}) & \\
2 & & & & C_2 \arrow[ddll] & & & & \mathbb{Q}(\beta) \arrow[ul] \\
5 & C_5 \arrow[dr] & & & & \mathbb{Q}(\sqrt{-11}) \arrow[uurr] & & & \\
10 & & C_{10} & & & & \mathbb{Q} \arrow[ul] \arrow[uurr] & &
\end{tikzcd}$$

Exercise 11.5: Put $M_i = L^{H_i}$, so $L = M_0 \supset M_1 \supset \cdots \supset M_r = K$. The Galois Correspondence tells us that L is normal over M_i, with Galois group H_i (so $[L : M_i] = 2^i$) and M_i is normal over K (with Galois group G/H_i). It follows that $[M_i : M_{i+1}] = 2$, so the standard analysis of degree two extensions says that $M_i = M_{i+1}(\alpha_i)$ for some α_i with $\alpha_i^2 \in M_{i+1}$. This means that $L = K(\alpha_0, \ldots, \alpha_{r-1})$. More precisely, for any subset $I \subseteq \{0, 1, \ldots, r-1\}$ we can let α_I denote the product of the elements α_i for $i \in I$. We then find that these elements α_I give a basis for L over K.

This does not yet capture all the information that one might want, as revealed by the following question. Suppose we have fields $K \subset K(\alpha_1) \subset K(\alpha_0, \alpha_1)$, with $\alpha_1^2 \in K$ and $\alpha_0^2 \in K(\alpha_1)$. When is it true that $K(\alpha_0, \alpha_1)$ is normal over K? This is usually false but sometimes true. We do not know a good general criterion even in this case where $r = 2$, let alone the case of general r.

Exercise 12.1: We first claim that $g_0(x)$ is irreducible over $\mathbb{Q}$. If not, it would have to have a monic linear factor, say $x - a$ with $a \in \mathbb{Q}$. Then Gauss's Lemma (Proposition 4.21) would tell us that $a \in \mathbb{Z}$. We would also have $g_0(a) = 0$, which rearranges to give $a(3 - a^2) = 1$, so a divides 1, so $a = \pm 1$. However $g_0(1)$ and $g_0(-1)$ are nonzero, so this is impossible. By essentially the same argument, $g_1(x)$ is irreducible over $\mathbb{Q}$. This can also be proved by applying Eisenstein's criterion (with $p = 3$) to $g_0(x-1)$ and $g_1(x-1)$.

We now see from the general theory that the Galois groups are either $A_3 = C_3$ (if the discriminant is a square) or Σ_3 (if the discriminant is not a square). Using the formula in Remark 12.3 we see that the discriminant of $g_0(x)$ is $-4 \times (-27) - 27 = 81 = 9^2$, whereas the discriminant of $g_1(x)$ is $-4 \times 27 - 27 = -135$. Thus, the Galois group for $g_0(x)$ is A_3, and the Galois group for $g_1(x)$ is Σ_3.

Exercise 12.2: The first claim can be checked using Maple as follows:

```
r := 1 + q + q^2;
f := (x) -> x^3 - (3*x - 2*q - 1)*r;
g := (x) -> (x^3+3*q*x^2-3*(q+1)*x-(4*q^3+6*q^2+6*q+1));
s := (x) -> x^2+q*x-2*r;
expand(f(s(x)) - f(x)*g(x));
```

It is possible but painful to do this by hand; $f(s(x))$ has 25 terms when fully expanded.

Now suppose we have $\alpha \in L$ with $f(\alpha) = 0$, and we put $\beta = s(\alpha) \in \mathbb{Q}(\alpha)$. We can substitute $x = \alpha$ in the relation $f(s(x)) = f(x)g(x)$ to see that $f(\beta) = f(\alpha)g(\alpha) = 0$, so β is another root of $f(x)$. Next, as $f(x)$ is assumed to be irreducible, it must be the minimal polynomial of α, so $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/f(x)$. This means that homomorphisms from $\mathbb{Q}(\alpha)$ to any field M biject with roots of $f(x)$ in M. In particular, we can take $M = \mathbb{Q}(\alpha)$ and we find that there is a homomorphism $\sigma \colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ with $\sigma(\alpha) = \beta$.

We next claim that $\beta \neq \alpha$, or equivalently that α is not a root of the quadratic polynomial $s(x) - x$. This is clear because the minimal polynomial of α is $f(x)$, which is cubic, so it cannot divide $s(x) - x$. It follows that $f(x)$ is divisible in $\mathbb{Q}(\alpha)[x]$ by $(x-\alpha)(x-\beta)$. The remaining factor is a monic polynomial of degree 1, so it must have the form $x-\gamma$ for some $\gamma \in \mathbb{Q}(\alpha)$. We now have a splitting $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$, so $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$. This means that it is normal, and the order of the Galois group is $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. All groups of order 3 are cyclic, and σ is a nontrivial element, so we must have $G(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma, \sigma^2\}$.

Exercise 12.3: First, we have

$$x^3 + ux^2 + vx + w = f(x) = (x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta + \beta\gamma + \gamma\alpha)x - \alpha\beta\gamma,$$

so

$$\begin{aligned} u &= -\alpha - \beta - \gamma \\ v &= \alpha\beta + \beta\gamma + \gamma\alpha \\ w &= -\alpha\beta\gamma. \end{aligned}$$

It follows that

$$w^2 p = \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2.$$

This is similar to v^2, but not equal to it. More precisely, we have

$$v^2 = \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 + 2(\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2) = w^2 p + 2uw.$$

Rearranging this gives $p = v^2/w^2 - 2u/w$.

Exercise 12.4:

(a) One approach is to simply expand everything out. Alternatively, we can recall the behaviour of determinants under row and column operations, and argue as follows:

$$\det \begin{bmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{bmatrix} = \det \begin{bmatrix} 1 & 0 & 0 \\ \alpha & \beta-\alpha & \gamma-\alpha \\ \alpha^2 & \beta^2-\alpha^2 & \gamma^2-\alpha^2 \end{bmatrix} = (\beta-\alpha)(\gamma-\alpha)\det \begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 1 \\ \alpha^2 & \beta+\alpha & \gamma+\alpha \end{bmatrix} = (\beta-\alpha)(\gamma-\alpha)(\gamma-\beta) = \delta(f).$$

(At the first stage we subtracted the first column from each of the other two columns, then we extracted factors of $\beta - \alpha$ and $\gamma - \alpha$ from the second and third columns, then we calculated the final determinant directly.)

(b) We have

$$\det(MM^T) = \det(M)\det(M^T) = \det(M)^2 = \delta(f)^2 = \Delta(f).$$

(c) This is just a direct calculation:

$$\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix} \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} = \begin{pmatrix} 1+1+1 & \alpha+\beta+\gamma & \alpha^2+\beta^2+\gamma^2 \\ \alpha+\beta+\gamma & \alpha^2+\beta^2+\gamma^2 & \alpha^3+\beta^3+\gamma^3 \\ \alpha^2+\beta^2+\gamma^2 & \alpha^3+\beta^3+\gamma^3 & \alpha^4+\beta^4+\gamma^4. \end{pmatrix}$$

(d) We have

$$S_2 = \alpha^2 + \beta^2 + \gamma^2 = (\alpha+\beta+\gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = -2a,$$

as $\alpha + \beta + \gamma = S_1 = 0$ and $\alpha\beta + \beta\gamma + \gamma\alpha = a$.

(e) Add the three equations to get

$$(\alpha^3 + \beta^3 + \gamma^3) + a(\alpha + \beta + \gamma) + b(1+1+1) = 0,$$

or $S_3 + aS_1 + bS_0 = 0$. Thus $S_3 = -aS_1 - bS_0$. Also, add

$$\begin{aligned}\alpha^4 + a\alpha^2 + b\alpha &= 0\\ \beta^4 + a\beta^2 + b\beta &= 0\\ \gamma^4 + a\gamma^2 + b\gamma &= 0\end{aligned}$$

to get $S_4 = -aS_2 - bS_1$. Thus we conclude that

$$\begin{aligned}S_3 &= -3b\\ S_4 &= 2a^2.\end{aligned}$$

(f) Substituting the values of $S_0, \ldots, S_4$ into the matrix in (c), we get:

$$MM^T = \begin{pmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{pmatrix}.$$

By part (b), $\Delta(f)$ is the determinant of this matrix, which can be evaluated directly to give $\Delta(f) = -(4a^3 + 27b^2)$.

Exercise 13.1: Using the formula in Proposition 13.3, we see that the resolvent cubic for $f_0(x)$ is $x^3 - 32x - 64 = 64((x/4)^3 - 2(x/4) - 1)$. In the notation of Exercise 12.1, this is $64g_0(x/4)$, so the Galois group is the same as for $g_0(x)$, namely A_3. Using Remark 13.13 we deduce that the Galois group for $f_0(x)$ is A_4.

Similarly, the resolvent cubic for $f_1(x)$ is $64g_1(x/4)$, and the Galois group for $g_1(x)$ is Σ_3, so the Galois group for $f_1(x)$ is Σ_4.

Exercise 13.2: The discriminant is

$$\begin{aligned}\prod_{i<j}(\alpha_i - \alpha_j)^2 &= (\alpha_0 - \alpha_1)^2(\alpha_0 - \alpha_2)^2(\alpha_0 - \alpha_3)^2(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2\\ &= (2\sqrt{5})^2(2\sqrt{2})^2(2\sqrt{2} + 2\sqrt{5})^2(2\sqrt{2} - 2\sqrt{5})^2(2\sqrt{2})^2(2\sqrt{5})^2\\ &= 2^{14}5^2(\sqrt{5} + \sqrt{2})^2(\sqrt{5} - \sqrt{2})^2\\ &= 2^{14}5^2(5-2)^2 = 2^{14}3^25^2 = 3686400.\end{aligned}$$

The splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, so the Galois group is $C_2 \times C_2$ by Proposition 7.2.

Exercise 13.3: We merely sketch this. The matrix M is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha & \beta & \gamma & \delta \\ \alpha^2 & \beta^2 & \gamma^2 & \delta^2 \\ \alpha^3 & \beta^3 & \gamma^3 & \delta^3 \end{pmatrix}.$$

If we put $S_i = \alpha^i + \beta^i + \gamma^i + \delta^i$, then

$$MM^T = \begin{pmatrix} S_0 & S_1 & S_2 & S_3 \\ S_1 & S_2 & S_3 & S_4 \\ S_2 & S_3 & S_4 & S_5 \\ S_3 & S_4 & S_5 & S_6 \end{pmatrix}.$$

From the factorisation $f(x) = (x - \alpha)(x - \beta)(x - \gamma)(x - \delta)$ we obtain

$$\begin{aligned}
\alpha + \beta + \gamma + \delta &= 0 \\
\alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta &= 0 \\
\alpha\beta\gamma + \alpha\beta\delta + \alpha\gamma\delta + \beta\gamma\delta &= -p \\
\alpha\beta\gamma\delta &= q.
\end{aligned}$$

From this we deduce that $S_0 = 4$, $S_1 = 0$ and $S_2 = 0$. To compute S_3, use

$$\begin{aligned}
\alpha^3 + \beta^3 + \gamma^3 + \delta^3 &= S_1^3 - 3(\alpha^2\beta + \text{similar terms}) - 6(\alpha\beta\gamma + \text{similar terms}) \\
\alpha^2\beta + \text{similar terms} &= S_1(\alpha\beta + \text{similar terms}) - 3(\alpha\beta\gamma + \text{similar terms}) \\
\alpha\beta\gamma + \text{similar terms} &= -p.
\end{aligned}$$

Combining these, together with $S_1 = 0$, we see that $S_3 = -3p$. Using the same trick as in Exercise 12.4, we get that

$$\begin{aligned}
S_4 &= -(pS_1 + qS_0) = -4q \\
S_5 &= -(pS_2 + qS_1) = 0 \\
S_6 &= -(pS_3 + qS_2) = -3p^2
\end{aligned}$$

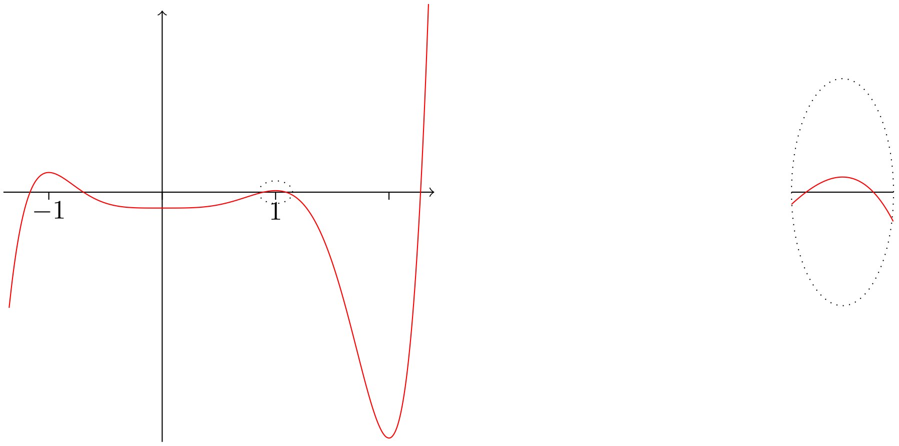
and so

$$\Delta(f) = \det \begin{pmatrix} 4 & 0 & 0 & -3p \\ 0 & 0 & -3p & -4q \\ 0 & -3p & -4q & 0 \\ -3p & -4q & 0 & -3p^2 \end{pmatrix} = 27p^4 + 256q^3.$$

Exercise 15.1: The polynomials $f_0(x)$ and $f_2(x)$ are solvable by radicals, but $f_1(x)$, $f_3(x)$, $f_4(x)$ and $f_5(x)$ are not. This can be proved as follows.

- $f_0(x)$ is x times a quartic, and quartics are solvable by radicals. (Maple says that the relevant Galois group is Σ_4.)
- $f_1(x)$ is irreducible by Eisenstein's criterion at $p = 5$. It also has precisely three real roots (approximately $-1.33, -0.51, 1.60$), as one can see by plotting or an argument with Rolle's Theorem and the Intermediate Value Theorem. The Galois group is thus Σ_5 by Corollary 7.8, which means that $f_1(x)$ is not solvable by radicals.
- Put $g_2(x) = 2x^3 - 10x + 5$, so $f_2(x) = g_2(x^2)$. As $g_2(x)$ is cubic, it is solvable by radicals. If the roots of $g_2(x)$ are α, β and γ, then the roots of $f_2(x)$ are $\pm\sqrt{\alpha}$, $\pm\sqrt{\beta}$ and $\pm\sqrt{\gamma}$. It follows that the splitting field for $f_2(x)$ is obtained from that for $g_2(x)$ by adjoining some square roots, which is a further radical extension; so $f_2(x)$ is solvable by radicals. Maple says that the relevant Galois group is of order 48, isomorphic to the subgroup of Σ_6 generated by $(1\ 2\ 3\ 4)$ and $(1\ 5)(3\ 6)$.
- We observe that $f_3(x) = x^5 f_1(1/x)$, so the roots of $f_3(x)$ are the inverses of the roots of $f_1(x)$. This means that $f_3(x)$ has the same splitting field as $f_1(x)$, so the Galois group is again Σ_5, so $f_3(x)$ is not solvable by radicals.
- $f_4(x)$ is irreducible by Eisenstein's criterion at $p = 3$, and has precisely three real roots (close to $x = 0$ and $x = \pm 4.5$). We can again use Corollary 7.8 to see that the Galois group is Σ_5 and the polynomial is not solvable by radicals.
- One can check that $f_5(x) = f_1(x)^2$, so $f_5(x)$ has the same roots and the same splitting field as $f_1(x)$, so it is not solvable by radicals.

Exercise 15.2: It will be enough to show that the Galois group of the splitting field is Σ_7. Using Corollary 7.8, it will thus be enough to show that $f(x)$ is irreducible and has precisely five real roots. Irreducibility follows from Eisenstein's criterion at $p = 7$. We can plot the graph using Maple, and we see that the roots are as required:



More rigorously, we can check that

$$f'(x) = 210(x^6 - 2x^5 - x^4 + 2x^3) = 210x^3(x-1)(x+1)(x-2),$$

which has four real roots, at $-1, 0, 1, 2$. Rolle's Theorem says that between any two real roots of $f(x)$ there is a real root of $f'(x)$, so there are at most five real roots. We also have

$$\begin{aligned} f(x) &\to -\infty \qquad \text{as } x \to -\infty \\ f(-1) &= 26 \\ f(0) &= -21 \\ f(1) &= 2 \\ f(2) &= -325 \\ f(x) &\to +\infty \qquad \text{as } x \to +\infty \end{aligned}$$

so (by the Intermediate Value Theorem) $f(x)$ has exactly five real roots.

Exercise 15.3:

(a) First note that

$$\rho_{ab}(\rho_{cd}(u)) = a(cu+d)+b = (ac)u + (ad+b) = \rho_{ac,ad+b}(u).$$

It follows that U is closed under composition. We also see that ρ_{10} is the identity, and that $\rho_{1/a,-b/a}$ is an inverse for ρ_{ab}. This means that U is a subgroup of Σ_5. Now define $\pi\colon U \to \mathbb{F}_5^\times$ by $\pi(\rho_{ab}) = a$. The above composition formula shows that $\pi(\rho_{ab}\rho_{cd}) = ac = \pi(\rho_{ab})\pi(\rho_{cd})$, so π is a homomorphism. For each $a \in \mathbb{F}_5^\times$ we have an element $\rho_{a0} \in U$ with $\pi(\rho_{a0}) = a$, so π is surjective. The kernel is $V = \{\rho_{1b} \mid b \in \mathbb{F}_5\}$, which is therefore a normal subgroup. The First Isomorphism Theorem tells us that $U/V \simeq \mathbb{F}_5^\times = \{-2,-1,1,2\}$, which is cyclic of order 4, generated by 2. We also see from the composition formula that $\rho_{1b}\rho_{1d} = \rho_{1,b+d}$, so $\rho_{1b} = \rho_{11}^b$. It follows that V is cyclic of order 5, generated by ρ_{11}.

(b) Let H be a subgroup of Σ_5, and let C be a normal subgroup of H that is cyclic of order 5. Choose a generator σ for C. This has order 5, and by considering the possible cycle types in Σ_5 we see that it must be a 5-cycle, say $\sigma = (p_0\ p_1\ p_2\ p_3\ p_4)$. Let θ be the permutation that sends i to p_i, and note that $\theta^{-1}\sigma\theta = \rho_{11}$. Put $H' = \theta^{-1}H\theta$ and $C' = \theta^{-1}C\theta$, so C' is normal in H'. As $\theta^{-1}\sigma\theta = \rho_{11}$ we see that $C' = V$. Now consider an arbitrary element $\tau \in H'$. Put $b = \tau(0) \in \mathbb{F}_5$. As V is normal in H' we see that $\tau\rho_{11}\tau^{-1}$ must be another generator for V, so $\tau\rho_{11}\tau^{-1} = \rho_{1a}$ for some $a \in \mathbb{F}_5^\times$. We now claim that $\tau = \rho_{ab}$, or equivalently that the permutation $\phi = \rho_{ab}^{-1}\tau$ is the identity. Indeed, we have $\rho_{ab}(0) = b = \tau(0)$, so $\phi(0) = 0$. We also have

$$\rho_{ab}\rho_{11}\rho_{ab}^{-1} = \rho_{a,a+b}\rho_{1/a,-b/a} = \rho_{1a} = \tau\rho_{11}\tau^{-1},$$

so $\phi\rho_{11}\phi^{-1} = \rho_{11}$. This means that ϕ commutes with ρ_{11}, and thus also with $\rho_{1m} = \rho_{11}^m$. It follows that

$$\phi(m) = \phi(\rho_{1m}(0)) = \rho_{1m}(\phi(0)) = \rho_{1m}(0) = m,$$

so ϕ is the identity as claimed, so $\tau = \rho_{ab}$. As τ was an arbitrary element of H', we conclude that $H' \subseteq U$, and so $H = \theta H'\theta^{-1} \subseteq \theta U\theta^{-1}$.

(c) Now instead let H be an arbitrary transitive subgroup of Σ_5. For any $x \in \mathbb{F}_5$, the orbit Hx is then the whole set $\mathbb{F}_5$. We have the standard orbit-stabiliser identity $|H| = |Hx|.|\operatorname{stab}_H(x)| = 5|\operatorname{stab}_H(x)|$, so $|H|$ must be divisible by 5. Moreover, $|H|$ must divide $|\Sigma_5| = 120$, so it cannot be divisible by 5^2. Let C be any Sylow 5-subgroup of H; then $|C| = 5$ is prime, so C must be cyclic. If C is normal in H then H is conjugate to a subgroup of U by part (b). From now on we suppose that C is not normal in H. Sylow theory tells us that the Sylow subgroups of H are precisely the conjugates of C, and that the number n of such conjugates divides $|H|/|C|$ and is congruent to 1 modulo 5. Moreover, as C is not normal we have $n > 1$, and $|H|/|C|$ must divide $|\Sigma_5|/|C| = 24$. It follows that $n = 6$, and this must divide $|H|/|C|$, so $|H| \in \{30, 60, 120\}$. If $|H| = 120$ then H is all of Σ_5. If $|H| = 60$ then H has index two, so it is normal by a standard lemma. It is not hard to deduce that $H = A_5$.

This just leaves the case where $|H| = 30$. I think that there are no subgroups of order 30 in Σ_5, but this needs a proof.

Exercise 15.4: These are not too difficult to construct. Here is one way to do it:

1: Choose a cubic with two positive real roots and one negative real root. For example, $x^3 - 7x + 6 = (x+3)(x-1)(x-2)$.

2: Move this polynomial up or down the y-axis slightly to make it irreducible, but still ensuring that there are two positive and one negative real root. (If you do this cleverly, you will be able to use Eisenstein's criterion to check irreducibility!) For example, $x^3 - 7x + 6 - \frac{1}{6} = \frac{1}{6}(6x^3 - 42x + 35)$ is irreducible by Eisenstein's criterion with $p = 7$.

3: Now replace x by x^2 to get a polynomial of degree 6. In our example, we can consider the polynomial $6x^6 - 42x^2 + 35$. Now this polynomial is still irreducible by Eisenstein with $p = 7$, and its roots are the square roots of the roots of the cubic in step 2, two of which were positive, giving 4 real roots, and one negative, giving 2 imaginary roots. Finally, the Galois group cannot be Σ_6, since the polynomial is solvable by radicals (the roots are just the square roots of the roots of the cubic, so are certainly expressible as radicals).

Department of Pure Mathematics, University of Sheffield, Sheffield S3 7RH, UK
Email address: N.P.Strickland@sheffield.ac.uk