Exercise 1.1: 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.FIELDS: definitions and examples.theorem.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

\[
\begin{align*}
\alpha^0 &= 1 & \alpha^1 &= 1 + i \\
\alpha^2 &= -i & \alpha^3 &= 1 - i \\
\alpha^4 &= -1 & \alpha^5 &= -1 - i \\
\alpha^6 &= i & \alpha^7 &= -1 + i \\
\alpha^8 &= 1.
\end{align*}
\]

From this we see that every nonzero element of $\mathbb{F}_3[i]$ is $\alpha^k$ for some $k \in \{0, \ldots, 7\}$, and that this has inverse $\alpha^{8-k}$. This shows that $\mathbb{F}_3[i]$ is a field.

Exercise 1.2: 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 1.3: Put $\alpha = a^{1/n}$, so the field in question is $K = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Let $\sigma: K \to K$ be an automorphism, and put $\zeta = \sigma(\alpha)/\alpha \in K \subseteq \mathbb{R}$. We can apply $\sigma$ 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 $\zeta$ is real and $n$ is odd, we see that $\zeta$ has the same sign as $\zeta^n$, but $\zeta^n = 1 > 0$, so $\zeta > 0$. We also have $(\zeta - 1)(1 + \zeta + \cdots + \zeta^{n-1}) = \zeta^n - 1 = 0$, but all terms in the sum $1 + \zeta + \cdots + \zeta^{n-1}$ are strictly positive, so $\zeta = 1$. This means that $\sigma(\alpha) = \alpha$, so $\sigma$ acts as the identity on $\mathbb{Q}(\alpha) = K$.

Exercise 1.4: We have $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ with $\alpha^2 = \alpha^{-1} = 1 + \alpha$. Any automorphism $\phi: \mathbb{F}_4 \to \mathbb{F}_4$ 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 (b) we see that $\phi$ 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 $(\alpha^2)^2 = \alpha^4 = \alpha^2 = \alpha = \phi(\alpha^2)$.) Given this, it is clear that $\phi(xy) = x^2y^2 = \phi(x)\phi(y)$ for all $x$ and $y$. 

\begin{flushright}
Date: June 9, 2010.
\end{flushright}
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 1.5:** This is very similar to Proposition 1.31Fields: definitions and examplestheorem.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

$$
\phi(a + b) = \phi(a) + \phi(b) = \psi(a) + \psi(b) = \psi(a + b)
$$

$$
\phi(a - b) = \phi(a) - \phi(b) = \psi(a) - \psi(b) = \psi(a - b)
$$

$$
\phi(ab) = \phi(a)\phi(b) = \psi(a)\psi(b) = \psi(ab),
$$

which shows that $a+b, a-b, ab \in K$. Finally, if $a \in K^*$ then we can apply Proposition 1.29Fields: definitions and examplestheorem.1.29(a) to both $\phi$ and $\psi$ 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 1.6:** 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 $R$:

$$(a_0, a_1) + (b_0, b_1) = (a_0 + b_0, a_1 + b_1)$$

$$(a_0, a_1)(b_0, b_1) = (a_0b_0, a_1b_1).$$

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

$$a + (b + c) = (a_0, a_1) + ((b_0, b_1) + (c_0, c_1))$$

$$= (a_0, a_1) + (b_0 + c_0, b_1 + c_1)$$

$$= (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1))$$

$$= ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1)$$

$$= (a_0 + b_0, a_1 + b_1) + (c_0, c_1)$$

$$= ((a_0, a_1) + (b_0, b_1)) + (c_0, c_1) = (a + b) + c.$$

(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

$$a(b + c) = (a_0, a_1)(b_0 + c_0, b_1 + c_1)$$

$$= (a_0(b_0 + c_0), a_1(b_1 + c_1))$$

$$= (a_0b_0 + a_0c_0, a_1b_1 + a_1c_1)$$

$$= (a_0b_0, a_1b_1) + (a_0c_0, a_1c_1) = ab + ac.$$

(The other commutative ring axioms can be checked in the same way.

As $1 \not\in K_0$, we see that the element $e = (1,0) \in R$ is nonzero. For any element $a = (a_0, a_1) \in R$ we have $ea = (a_0,0) \not= (1,1) = 1_R$, 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:**
\[ \phi_0 \text{ is not linear because } \phi_0(-I) = (-I)^2 = I \neq -\phi(I). \]
\[ \phi_1 \text{ is linear because } \phi_1(sA + tB) = sA + tB - (sA + tB)^T = sA + tB - sAT - tB^T = s(A - AT) + t(B - B^T) = s\phi_1(A) + t\phi_1(B). \]

(This is enough by Remark 2.10 Vector space theorem 2.10.)
\[ \phi_2 \text{ is also linear, because } \phi_2(s[t + a]) = \phi_2(s[t + a]) = (sa + tc)x + (sb + td)x^2 = s(ax + bx^2) + t(cx + dx^2) = s\phi_2[t] + t\phi_2[a]. \]
\[ \phi_3 \text{ is not linear, because } \phi_3(-[0]) = \phi_3([-1]) = (-x)^2 \neq -x^2 = -\phi_3([1]). \]
\[ \phi_4 \text{ is linear, because } h(x) = sf(x) + tg(x) \text{ then } h(2) = sf(2) + tg(2) \text{ and } h(-2) = sf(-2) + tg(-2) \]
\[ \phi_4(sf(x) + tg(x)) = [h(2)]h([-2]) = [f(2)] + t[g(2)] = s\phi_4(f(x)) + t\phi_4(g(x)). \]
\[ \phi_5 \text{ is not linear. Indeed, for constant polynomials we just have } \phi_5(c) = c^3, \text{ so } \phi_5(1 + 1) = 8 \neq 2 = \phi_5(1) + \phi_5(1). \]

**Exercise 2.2:** The general form for elements of \( V \) is
\[ M = \begin{bmatrix} a & b & c \\ b & d & e \\ c & e & d \end{bmatrix} = aA + dB + cC + dD + eE, \]
where
\[ A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} C = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} D = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} E = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \]

It follows easily from this that the list \( A, B, C, D, E \) is a basis for \( V \).

**Exercise 2.3:**
- Put \( A = iI = [i 0; 0 -i] \). As \( i = -i \) 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 \( C \) of \( M_2(C) \).
- If \( A = [a b; c d] \) then \( A + A^\dagger = [a + \bar{b} \ b + \bar{a} \ \bar{c} + \bar{d} \ d + \bar{c}] \). For this to be zero, we need \( a + \bar{a} = d + \bar{d} = 0 \) (so \( a \) and \( d \) are purely imaginary) and \( c = -\bar{b} \). Equivalently, \( A \) must have the form

\[ A = \begin{bmatrix} iw & x + iy \\ -ix + iy & iz \end{bmatrix} = w[0 \ 1] + x[0 \ -1] + y[1 \ 0] + z[0 \ -i] \]

for some \( w, x, y, z \in R \). It follows that \( V \) is a subspace over \( R \) of \( M_2(C) \), with basis given by the matrices

\[ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \]

In particular, this basis has size four, so \( \dim R(V) = 4 \) as required.

**Exercise 2.4:** As \( L \) is generated over \( C \) 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 \( L = K(x) \cong K[t]/g(t) \), 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 \( K = Q(x^n) \), 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 \( c_i(s), d(s) \in C[s] \). 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 \( x^{ni+i} \) (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 $\phi : \mathbb{Z}[x] \to \mathbb{F}_4$ by

$$
\phi(a_0 + a_1 x + \cdots + a_d x^d) = \alpha_0 + \alpha_1 \alpha + \cdots + \alpha_d \alpha^d.
$$

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 $\phi$, so $\phi$ is surjective. Let $I$ be the kernel of $\phi$. Proposition 3.10 Ideals and quotient ringstheorem 3.10 then gives us an induced isomorphism $\overline{\phi} : \mathbb{Z}[x]/I \to \mathbb{F}_4$. 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:

- $R.0 = \{0\}$
- $R.1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = R.5 = R.7 = R.11$
- $R.2 = \{0, 2, 4, 6, 8, 10\} = R.10$
- $R.3 = \{0, 3, 6, 9\} = R.9$
- $R.4 = \{0, 4, 8\} = R.8$
- $R.6 = \{0, 6\}$.

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 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

$$f_0(x) = (x + \frac{1}{2})f_1(x) + \left(\frac{3}{4}x^2 + \frac{3}{4}x + \frac{3}{4}\right),$$

so $f_2(x) = x^2 + x + 1$. We then divide $f_1(x)$ by $f_2(x)$ and obtain

$$f_1(x) = (x + \frac{1}{2})f_2(x)$$

(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 4.2:** 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 4.3:** 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

$$f(x) = (x^2 + x^2)(x^2 + x + 1) + 1,$$

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 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 $\alpha$, $\omega \alpha$ and $\omega^2 \alpha$, where $\alpha$ is the real cube root of 2, and $\omega = e^{2\pi i/3} = (\sqrt{-3} - 1)/2$. It follows that $K_3$ contains $\alpha$ 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 $\beta$ 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 $\alpha$ 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: First define $\chi_0: K[x] \to L$ by $\chi_0(p(x)) = p(\alpha)$, or more explicitly

$$
\chi_0(\sum_{i} a_i x^i) = \sum_{i} a_i \alpha^i.
$$


The kernel of this is $I(\alpha, K)$, which is zero because $\alpha$ 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 $\chi: K(x) \to L$ as described. We know from Proposition 1.29Fields: definitions and examples that $\chi(I(K(x)))$ is a subfield of $L$ and that $\chi$ 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 $\alpha = \chi(\alpha) \in \chi(K(x))$, and by definition $K(\alpha)$ is the smallest subfield of $L$ containing $K$ and $\alpha$, so $K(\alpha) \subseteq \chi(K(x))$. Conversely, as $K(\alpha)$ is a field containing $K$ and $\alpha$, we see that it must contain all powers of $\alpha$, 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 5.3: We can define a function $\mu: L \to L$ by $\mu(a) = aa$ 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 $\mu$. More explicitly, we can choose a basis $e_1, \ldots, e_d$ 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 $
abla_{i=0}^d c_i t^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 $\mu(a) = aa$ (and so $\mu^2(a) = \mu(\mu(a)) = \mu^2(a)$, 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 5.4:
(a) If \( \alpha \in \overline{Q} \) then Proposition 5.8 Adjoining rootstheorem 5.8 tells us that \( \left[ Q(\alpha) : Q \right] = \deg(\min(\alpha, Q)) < \infty \). If \( \left[ Q(\alpha) : Q \right] < \infty \) then evidently \( Q(\alpha) \) is an example of a subfield \( K \subseteq \mathbb{C} \) with \( \alpha \in K \) and \( \left[ K : Q \right] < \infty \). If we are given such a field \( K \), then Proposition 5.10 Adjoining rootstheorem 5.10 (applied to the extension \( Q \subseteq K \)) tells us that \( \alpha \in \overline{Q} \). Thus, the three conditions mentioned are all equivalent.

(b) First, it is clear that \( \overline{Q} \) contains \( Q \), so \( 0, 1 \in \overline{Q} \). Suppose that \( \alpha, \beta \in \overline{Q} \). This means that there are subfields \( L, M \subseteq C \) with \( \alpha \in L \) and \( \beta \in M \) and \( [L : Q], [M : Q] < \infty \). Now Proposition 5.12 Adjoining rootstheorem 5.12 tells us that \( LM \) is a subfield of \( C \) containing both \( \alpha \) and \( \beta \), such that \( [LM : Q] < \infty \). As (iii) implies (i) above, we see that \( LM \subseteq \overline{Q} \). Now \( \alpha + \beta, \alpha - \beta, \alpha\beta \) all lie in \( LM \), so they lie in \( \overline{Q} \). Similarly, if \( \alpha \neq 0 \) then \( \alpha^{-1} \in L \subseteq LM \subseteq \overline{Q} \). It follows that \( \overline{Q} \) is a subfield as claimed.

(c) Now suppose that \( \alpha \in C \) and \( \alpha \) is algebraic over \( \overline{Q} \). We thus have a minimal polynomial \( f(x) = \min(\alpha, \overline{Q})(x) = \sum_{i=0}^{d} a_i x^i \), with \( a_d = 1 \) and \( a_i \in \overline{Q} \) for all \( i \). Now part (a) tells us that there exists a field \( L_i \subseteq C \) with \( a_i \in L_i \subseteq C \) and \( [L_i : Q] \leq \infty \). Put \( L = L_0 L_1 \cdots L_d \), so Proposition 5.12 Adjoining rootstheorem 5.12 tells us that \( [L : Q] < \infty \). Moreover, as \( f(\alpha) = 0 \) we see that \( [L(\alpha) : L] \leq d \), so \( [L(\alpha) : Q] = [L(\alpha) : L][L : Q] < \infty \). This means that \( L(\alpha) \) is a finite degree extension of \( Q \) containing \( \alpha \), so \( \alpha \in \overline{Q} \) by criterion (iii) above.

(d) Suppose we have a nonconstant polynomial \( f(x) \in \overline{Q}[x] \). We can regard this as a nonconstant polynomial over \( C \), so the Fundamental Theorem of Algebra tells us that there is a root (say \( \alpha \)) in \( C \). Now the relation \( f(\alpha) = 0 \) tells us that \( \alpha \) is algebraic over \( \overline{Q} \), so part (c) tells us that \( \alpha \in \overline{Q} \). We therefore see that any nonconstant polynomial over \( \overline{Q} \) has a root in \( \overline{Q} \), which means that \( \overline{Q} \) is algebraically closed.

**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 \( \sigma \) is the identity. Thus the action is free, as claimed.

Next, as \( A \) is transitive we can choose \( \sigma_i \in A \) (for \( i = 1, \ldots, N \)) such that \( \sigma_i(1) = i \). Now let \( \tau \) 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 \( A = \{\sigma_1, \ldots, \sigma_n\} \), 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 \( \alpha_1, \ldots, \alpha_d \) be the roots of \( f(x) \) in \( C \). 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 \( \beta_i \) for \( \alpha_i \). 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 \( L = Q(\beta_1, \ldots, \beta_d) \) and

\[
K = Q(\alpha_1, \ldots, \alpha_d) = Q(\beta_1^2, \ldots, \beta_d^2) \subseteq L.
\]

As both \( K \) and \( L \) are normal over \( Q \), we know that \( G(L/K) \) is a normal subgroup of \( G(L/Q) \), and that \( G(L/Q)/G(L/K) \simeq G(K/Q) \). 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 \( \chi_i : G(L/K) \to \{1, -1\} \). We can put these together to define a map \( \chi : G(L/K) \to \{1, -1\}^d \) by \( \chi(\sigma) = (\chi_1(\sigma), \ldots, \chi_d(\sigma)) \). As the elements \( \beta_i \) generate \( L \) over \( K \), we see that \( \chi \) 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 7.1:** Put \( \alpha = \sqrt{p} + \sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{q}) \). Then
\[
\alpha^2 = p + q + 2\sqrt{pq} \quad \quad \quad \alpha^3 = (p + 3q)\sqrt{p} + (q + 3p)\sqrt{q},
\]
so
\[
\sqrt{p} = \frac{\alpha^3 - (q + 3p)\alpha}{2(q - p)} \quad \quad \quad \sqrt{q} = \frac{\alpha^3 - (p + 3q)\alpha}{2(p - q)}.
\]
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:
\[
(x - \sqrt{p} - \sqrt{q})(x - \sqrt{p} + \sqrt{q})(x + \sqrt{p} - \sqrt{q})(x + \sqrt{p} + \sqrt{q})
\]
\[
= ((x - \sqrt{p})^2 - q)((x + \sqrt{p})^2 - q) = (x^2 - 2\sqrt{px} + p - q)(x^2 + 2\sqrt{px} + p - q)
\]
\[
= (x^2 + p - q)^2 - (2\sqrt{px})^2 = x^4 - 2(p + q)x^2 + (p - q)^2 = f(x).
\]
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 7.2:** 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 \( f(t) = t^4 - 3 \in \mathbb{Q}[t] \). 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 \( \Sigma_3 \) of all permutations, or the subgroup \( A_R \) of even permutations. However, complex conjugation restricts to give an automorphism of \( L \) corresponding to the transposition that exchanges \( \omega\alpha \) and \( \omega^2\alpha \). This shows that \( G(L/K) \not\subseteq A_R \), so we must have \( G(L/K) \cong \Sigma_3 \).

**Exercise 7.3:** There is an automorphism \( \sigma \) of \( L \) given by \( z \mapsto \overline{z} \). We claim that this is the only nontrivial automorphism. To see this, write \( \alpha = \sqrt{3} \), 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
\[
a^2 + 6bc = 3 \quad \quad \quad 2ab + 3c^2 = 0 \quad \quad \quad 2ac + b^2 = 0.
\]
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 $\rho$ be any automorphism of $L$. Then $\rho(i)^2 + 1 = \rho(1) + 1 = \rho(0) = 0$, 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 $\rho$ is either the identity (if $\rho(i) = i$) or $\sigma$ (if $\rho(i) = -i$).

As 1 and $\sigma$ both act as the identity on $\alpha$, we see that $G(L/Q(\alpha)) = G(L/Q) = \{1, \sigma\}$. Now $[L : Q(\alpha)] = 2 = |G(L/Q(\alpha))|$, so $L$ is normal over $Q(\alpha)$. On the other hand, $[L : Q] = 4 > 2 = |G(L/Q)|$, so $L$ is not normal over $Q$. Explicitly, the polynomial $f(t) = t^4 - 3 \in Q[t]$ has a root in $L$ but does not split in $L$.

Exercise 7.4: Put $\alpha = \sqrt[3]{3}$ 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 $L = Q(\alpha, i)$ is a splitting field for $f(t)$ over $Q$, so $L$ is normal over $Q$. 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 $G(L/Q)$ is just the dihedral group of rotations and reflections of this square. Indeed, complex conjugation gives an automorphism $\sigma$ 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 $G(L/Q)$ acts transitively on $R$. It follows that there is an automorphism $\phi$ 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 $\rho(m\alpha) = i^{m+1}\alpha$ for all $m$, so $\rho$ is a quarter turn of the square. This means that $\rho$ and $\sigma$ generate $D_8$, so $|G(L/Q)| \geq |D_8| = 8$. 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 $Q$, so $[L : Q] \leq |B| = 8$, and for any extension we have $|G(L/Q)| \leq [L : Q]$. It follows that all these inequalities must be equalities, so $G(L/Q) = D_8$ and $B$ is a basis.

Exercise 7.5: 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 $\alpha \approx 0.87 + 0.12i$, and from that one can check that $\alpha, -\alpha, 2/\alpha$ and $-2/\alpha$ are all distinct. We must therefore have

$$f(x) = (x - \alpha)(x + \alpha)(x - 2/\alpha)(x + 2/\alpha).$$
Exercise 7.6:

(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 \( \alpha^2 + 3 = 3\sqrt{2} = \sqrt{18} \), and squaring again shows that \( \alpha^4 + 8\alpha^2 + 16 = 18 \), so \( \alpha = 0 \). We now prove that \( f(x) \) is irreducible. It is clear that \( f(x) = x^4 \) 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

\[
\begin{align*}
b + d - a^2 &= 1 \\
a(d - b) &= 0 \\
bd &= 4.
\end{align*}
\]

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 \( a \in \mathbb{Q} \).

(c) We have \( 3\sqrt{2} - 2 \approx 0.24 > 0 \) so \( \alpha \) is real, so \( \mathbb{Q}(\alpha) \subseteq \mathbb{M} \cap \mathbb{R} \). As \( f(x) \) is irreducible, it must be the minimal polynomial for \( \alpha \), and so \( [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x)) = 4 \). As \( \alpha \in \mathbb{R} \) and \( \sqrt{-2} \) is purely imaginary we see that \( 1, \sqrt{-2} \) is a basis for \( \mathbb{M} \) over \( \mathbb{Q}(\alpha) \), so \( \mathbb{M} \cap \mathbb{R} = \mathbb{Q}(\alpha) \) and \( [\mathbb{M} : \mathbb{Q}(\alpha)] = [\mathbb{M} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 4 = 8 \).

(d) First let \( \psi : \mathbb{M} \to \mathbb{M} \) 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 \( \sigma \in G(\mathbb{M}/\mathbb{Q}) \) with \( \sigma(\alpha) = \sqrt{-2}/\alpha \). Now \( \sigma \) 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

\[
\phi(\alpha) = \phi(\sqrt{-2}/\alpha) = \phi(\sqrt{-2}/\alpha) = -\sqrt{-2}/(\sqrt{-2}/\alpha) = -\alpha
\]

and \( \phi(\sqrt{-2}) = \sqrt{-2} \). It follows in turn that \( \phi^4 = 1 \). We now have various different automorphisms, whose effect we can tabulate as follows:

<table>
<thead>
<tr>
<th></th>
<th>( \alpha )</th>
<th>( \beta )</th>
<th>( -\alpha )</th>
<th>( -\beta )</th>
<th>( \alpha )</th>
<th>( \beta )</th>
<th>( -\alpha )</th>
<th>( -\beta )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha )</td>
<td>( \alpha )</td>
<td>( \beta )</td>
<td>( -\alpha )</td>
<td>( -\beta )</td>
<td>( \alpha )</td>
<td>( \beta )</td>
<td>( -\alpha )</td>
<td>( -\beta )</td>
</tr>
<tr>
<td>( \beta )</td>
<td>( \beta )</td>
<td>( -\alpha )</td>
<td>( -\beta )</td>
<td>( \alpha )</td>
<td>( -\alpha )</td>
<td>( \beta )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \sqrt{-2} )</td>
<td>( \sqrt{-2} )</td>
<td>( -\sqrt{-2} )</td>
<td>( -\sqrt{-2} )</td>
<td>( \sqrt{-2} )</td>
<td>( -\sqrt{-2} )</td>
<td>( \sqrt{-2} )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We see that the eight automorphisms listed are all different, but \( |G(\mathbb{M}/\mathbb{Q})| = [\mathbb{M} : \mathbb{Q}] = 8 \), 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 $\phi$ corresponding to a rotation through $\pi/2$, and $\psi$ to a reflection.

Exercise 8.1: We have

\[
x^{200} - 1 = \varphi_{200}(x)\varphi_{100}(x)\varphi_{50}(x)\varphi_{40}(x)\varphi_{25}(x)\varphi_{20}(x)\varphi_{10}(x)\varphi_8(x)\varphi_5(x)\varphi_4(x)\varphi_2(x)\varphi_1(x)
\]
\[
x^{100} - 1 = \varphi_{100}(x)\varphi_{50}(x)\varphi_{25}(x)\varphi_{20}(x)\varphi_{10}(x)\varphi_5(x)\varphi_4(x)\varphi_2(x)\varphi_1(x)
\]
\[
x^{40} - 1 = \varphi_{40}(x)\varphi_{20}(x)\varphi_{10}(x)\varphi_8(x)\varphi_5(x)\varphi_4(x)\varphi_2(x)\varphi_1(x)
\]
\[
x^{20} - 1 = \varphi_{20}(x)\varphi_{10}(x)\varphi_5(x)\varphi_4(x)\varphi_2(x)\varphi_1(x)
\]

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 8.2: 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 $\zeta$ is a primitive 14th root of unity, and so is a root of the cyclotomic polynomial $\varphi_{14}(t)$. We know that

\[
t^{14} - 1 = \varphi_{14}(t)\varphi_7(t)\varphi_2(t)\varphi_1(t)
\]
\[
t^7 - 1 = \varphi_7(t)\varphi_1(t)
\]
\[
t + 1 = \varphi_2(t).
\]

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

\[
f(t) = \frac{(t - 1)^7 + 1}{t - 1 + 1} = ((t - 1)^7 + 1)/t = \sum_{i=0}^{6} (-1)^i \binom{7}{i} t^6 - t^5 + 21t^4 - 35t^3 + 35t^2 - 21t + 7.
\]

This reduces to $t^6$ modulo 7, either by inspecting the coefficients directly, or by recalling that $(t - 1)^7 = t^7 - 1^7 (\bmod 7)$. 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 8.3: 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 $\sigma_k$ 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 $2^3 = 8 = -7 (\bmod 15)$ and $2^4 = 16 = 1 (\bmod 15)$. 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 8.4:

(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, $\zeta$ 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 $[\mathbb{Q}(\zeta) : \mathbb{Q}(\beta)] \leq 2$. 
We next observe that \( \zeta^n = 1 \) so \(|\zeta| > 0\) and \(|\zeta|^n = 1\), so \(|\zeta| = 1\). If \( \zeta \) is real this means that \( \zeta = \pm 1\), so \( \zeta^2 = 1\), but this contradicts the assumption that \( \zeta \) is a primitive \( n \)th root for some \( n \geq 3 \). Thus, we see that \( \zeta \not\in \mathbb{R} \). On the other hand, as \(|\zeta| = 1\) we see that \( \zeta^{-1} = \overline{\zeta} \), so \( \beta = \zeta + \overline{\zeta} = 2 \text{Re}(\zeta) \in \mathbb{R} \). It follows that \( \mathbb{Q}(\beta) \subseteq \mathbb{R} \) and so \( \zeta \not\in \mathbb{Q}(\beta) \). 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 \( p_{k+1}(x) = xp_k(x) - p_k(x) \). 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

\[
p_{m+1}(\beta) = \beta p_m(\beta) - p_{m-1}(\beta)
\]

\[
= (\zeta + \zeta^{-1})(\zeta^m + \zeta^{-m}) - (\zeta^{m-1} + \zeta^{1-m})
\]

\[
= (\zeta^{m+1} + \zeta^{1-m} + \zeta^{m-1} + \zeta^{-m-1}) - (\zeta^{m-1} + \zeta^{1-m})
\]

\[
= \zeta^{m+1} + \zeta^{-m-1}.
\]

The claim therefore holds for all \( m \), by induction.

(d) The first few steps of the recursive scheme are as follows:

\[
p_0(x) = 2
\]

\[
p_1(x) = x
\]

\[
p_2(x) = xp_1(x) - p_0(x) = x^2 - 2
\]

\[
p_3(x) = xp_2(x) - p_1(x) = x^3 - 3x
\]

\[
p_4(x) = xp_3(x) - p_2(x) = x^4 - 4x^2 + 2
\]

\[
p_5(x) = xp_4(x) - p_3(x) = x^5 - 5x^3 + 5x.
\]

Thus, we have \( \zeta^5 + \zeta^{-5} = \beta^5 - 5\beta^3 + 5\beta \).

**Exercise 8.5:** 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

\[
g(t) = \frac{(t + 1)^p - 1}{(t + 1) - 1} = t^{-1}((t + 1)^p - 1) = \sum_{i=0}^{p-1} \binom{p}{i+1} t^i.
\]

This is monic, and using Lemma 8.7Cyclotomic extension theorem 8.7 we see that \( g(t) = t^{p-1} \mod p \), 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 8.6:** 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 \( s^2 = t^{2^k} \cdot t^{2^k} = t^{2^{k+1}} \), 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 \( \zeta \) is a \( 2^{k+1} \)th root of unity, then \( \zeta^{2^k} \) 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 \( \zeta \) runs over the roots, which is \( \varphi_{2^{k+1}}(t) \).

**Exercise 8.7:** We will write \( \mu_k \) for the set of all \( k \)th roots of unity, and \( \mu_k^\times \) for the subset of primitive roots.
(a) Note that \( \zeta^k = 1 \) if and only if \( \zeta^k = 1 \), so \( \zeta \) and \( \zeta \) have the same order. In other words, \( \zeta \) is a primitive \( n \)th root of unity if and only if \( \zeta \) is a primitive \( n \)th 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 \( n \)th 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 \( n \mid k \). 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 \( \zeta^m = (-1)^m (-\zeta)^m = (-1)^{m+1} \), 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 \( \{-\zeta \mid \zeta \in \mu_m^\times \} = \mu_m^\times \), so we see that \( \varphi_m(-x) = \varphi_m(x) \).

(c) We can write \( n = p^2m \) for some \( m \), so \( n/p = mp \). Suppose that \( \zeta \in \mu_n^\times \). Then \( (\zeta^p)^m = \zeta^n = 1 \). 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 \( \zeta^n = (\zeta^p)^m = 1 \), 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 \( k = mjp \). 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 \( k = mjp = p.mj = mp^2i = ni \), 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 \( x^p - \zeta \) for \( \zeta \in \mu_{n/p}^\times \). Here \( x^p - \zeta \) can be rewritten as the product of the terms \( x - \zeta \), as \( \zeta \) runs over the \( p \)th roots of \( \xi \). Thus, \( \varphi_{n/p}(x^p) \) is the product of all terms \( x - \zeta \) for which \( \zeta \in \mu_{n/p}^\times \), 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 (d) 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


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 \(-2x^7\) and \(-2x^{41}\), 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:

```maple
def 
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 8.8:** We can reorganise the definition and use the geometric progression formula as follows:

\[
f(x) = (1 - x) \left( \sum_{i=0}^{q-1} x^{ip} \right) \left( \sum_{j=0}^{p-1} x^{jq} \right) \left( \sum_{k=0}^{\infty} x^{kpq} \right)
\]

\[
= (1 - x) \frac{x^{pq} - 1}{x^p - 1} \frac{x^{pq} - 1}{x^q - 1} \frac{1}{1 - x^{pq}}
\]

\[
= \frac{\varphi_1(x) \varphi_{pq}(x) \varphi_p(x) \varphi_q(x) \varphi_1(x)}{\varphi_p(x) \varphi_1(x) \varphi_{pq}(x) \varphi_1(x)} = \varphi_{pq}(x).
\]

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 8.9:**

- Any automorphism is uniquely determined by its effect on \( \alpha \) and on \( \zeta \). The image of \( \alpha \) must be a root of \( x^5 - 2 \), so must be one of \( \alpha, \zeta \alpha, \zeta^2 \alpha, \zeta^3 \alpha \) or \( \zeta^4 \alpha \). In the same way, the image of \( \zeta \) must be another primitive 5th root of unity, i.e., a root of \( \varphi_5 \), so is one of \( \zeta, \zeta^2, \zeta^3 \) or \( \zeta^4 \). This gives 20 possible automorphisms, \( \theta_{ij} \) say, defined by

\[
\theta_{ij}(\zeta) = \zeta^i \\
\theta_{ij}(\alpha) = \zeta^j \alpha
\]

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 \( \psi \) which fixes \( \zeta \) and maps \( \alpha \) to \( \zeta \alpha \) is clearly of order 5. The automorphism \( \phi \) which fixes \( \alpha \) and maps \( \zeta \) to \( \zeta^2 \) 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 \( \phi \) and \( \psi \) 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:

\[
\phi \psi \phi^{-1}(\alpha) = \phi \psi(\alpha) = \phi(\zeta \alpha) = \phi(\zeta) \phi(\alpha) = \zeta^2 \alpha \\
\phi \psi \phi^{-1}(\zeta) = \phi \psi(\zeta^i) = \phi(\zeta^i) = \zeta
\]

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 $\beta$ is a root of $X^2 + X - 1$, and so $\beta = \frac{-1 + \sqrt{5}}{2}$, 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 $\text{Gal}(M/\mathbb{Q})$ 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 $\phi$). Let $G$ be the subgroup associated to $\mathbb{Q}(\beta)$. If we can show that $\beta$ is fixed by both $\phi^2$ and by $\psi$, 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:

$$\phi^2(\beta) = \phi^2(\zeta) + \frac{1}{\phi^2(\zeta)} = \zeta^{-1} + \frac{1}{\zeta^{-1}} = \frac{1}{\zeta} + \zeta = \beta$$

$$\psi(\beta) = \psi(\zeta) + \frac{1}{\psi(\zeta)} = \zeta + \frac{1}{\zeta} = \beta.$$ 

**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 $\alpha$ say. It follows that the subgroup generated by $\alpha^2$ 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 $\varphi_3(0) = 1 \neq 0$ and $\varphi_3(\pm 1) = 2 = -1 \neq 0$, so $\varphi_3(t)$ 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

$$a + c = 0$$

$$b + d + ac = 0$$

$$ad + bc = 0$$

$$bd = 1.$$ 

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

$$\varphi_3(t) = t^4 + 1 = (t^2 + t - 1)(t^2 - t - 1) \in \mathbb{F}_3[t].$$ 

This gives two fields of order 9:

$$K = \mathbb{F}_3[\alpha]/(\alpha^2 + \alpha - 1)$$

$$L = \mathbb{F}_3[\beta]/(\beta^2 - \beta - 1).$$ 

Now consider the field $\mathbb{F}_3[i]$ and the group

$$\mathbb{F}_3[i]^\times = \{ 1, -1, i, -i, 1 + i, 1 - i, -1 + i, -1 - i \} \cong C_8.$$ 

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 $\phi: K \to \mathbb{F}_3[i]$ with $\phi(\alpha) = 1 + i$, and a unique isomorphism $\psi: L \to \mathbb{F}_3[i]$ with $\psi(\beta) = -1 - i = -\phi(\alpha)$. It follows that the composite isomorphism $\psi^{-1} \phi: K \to L$ sends $\alpha$ to $-\beta$.

**Exercise 9.3:** Put $\alpha = [\frac{1}{2} \ 1]$, and identify each element $a \in \mathbb{F}_5$ with the matrix $aI = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$. The set $K$ then consists of all matrices $a + ba$ 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

$$\alpha^2 = \begin{bmatrix} \frac{1}{2} \\ 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{3}{2} \\ 3 \end{bmatrix}$$

$$2\alpha + 1 = 2 \begin{bmatrix} \frac{1}{2} \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{5}{2} \\ 2 \end{bmatrix} = \alpha^2.$$

It follows that

$$(a + ba)(c + da) = ac + (ad + bc)\alpha + bda^2 = ac + (ad + bc)\alpha + bd(2\alpha + 1)$$

$$= (ac + bd) + (ad + bc + 2bd)\alpha \in K,$$

so $K$ is closed under multiplication. We also see from the above formulæ that $(a + ba)(c + da) = (c + da)(a + ba)$, so multiplication in $K$ is commutative. The remaining parts of Definition 1.1Fields: definitions and examplestheorem.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 $\phi$ from the ring $K' = K[x]/f(x)$ to $K$ with $\phi(x + K[x]f(x)) = \alpha$. We also have

$$f(0) = -1$$

$$f(1) = -2$$

$$f(2) = -1$$

$$f(3) = 2$$

$$f(4) = 2$$

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 $\phi$ is an isomorphism. This means that $K$ is also a field.

**Exercise 9.4:** Proposition 8.11Cyclotomic extensionstheorem.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 9.13Finite fieldstheorem.9.13.

**Exercise 9.5:** We have $\mathbb{F}_7^\times = \{-3, -2, -1, 1, 2, 3\}$, and we check that

$$3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 2 \quad 3^3 = -1 \quad 3^4 = -3 \quad 3^5 = -2.$$

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 no 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 $K = \mathbb{F}_7[a]/(a^3 - 3)$ of order $7^3 = 343$. Now $a^3 = 3$ and $3^6 = 1$, so $a^{18} = 1$, but the whole group $K^\times$ has order 342, so $\alpha$ 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

\[
x^4 - 2x^2 - 1 = g_2(x)g_3(x) = x^4 + (a + c)x^2 + (b + d + ac)x^2 + (ad + bc)x + bd.
\]

By comparing coefficients, we get

\[
\begin{align*}
a + c &= 0 \\
b + d + ac &= -2 \\
ad + bc &= 0 \\
bd &= -1.
\end{align*}
\]

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

\[
\begin{align*}
g_2(x) &= x^2 + x + 2 \\
g_3(x) &= x^2 - x + 2.
\end{align*}
\]

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 \( g_1(x) \) 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 \( \alpha \), 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 \( p \)th power (remembering that \( (x + y)^p = x^p + y^p \) (mod \( p \))) 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 \( \alpha \) over \( \mathbb{F}_p \), which is an irreducible factor of \( f(x) \). If \( g(x) \) has degree \( d \), we have \( |K| = p^d \). By the general theory of finite fields, we have \( \alpha^{p^d} = a \) 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 11.1:** Put \( A = G(L/(L^HL^K)) \leq G \). Every automorphism \( \sigma \in A \) acts as the identity on \( L^HL^K \), 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 \( A \leq G(L/L^K) = K \), so in fact \( A \leq H \cap K \). Conversely, suppose that \( \sigma \in H \cap K \). Any element \( a \in L^HL^K \) 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 \( a \in L^HL^K \), 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 \( M = L^HL^K \) we see that \( L^HL^K = L^A = L^{H\cap K} \) as claimed.
Exercise 11.2: Choose elements $\rho$ and $\sigma$ 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

$$
A = \{1, \rho\} \quad B = \{1, \sigma\} \quad C = \{1, \rho \sigma\}
$$

Then $A, B$ and $C$ are the only proper non-trivial 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 $\sigma$ 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 $\alpha$ 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 formulæ to understand $\sigma(a)$ and $\rho(a)$, and we find that

$$
\begin{align*}
    a + \rho(a) + \sigma(a) + \rho \sigma(a) &= 4w \\
    a + \rho(a) - \sigma(a) - \rho \sigma(a) &= 4x\alpha \\
    a - \rho(a) + \sigma(a) - \rho \sigma(a) &= 4y\beta \\
    a - \rho(a) - \sigma(a) + \rho \sigma(a) &= 4z\alpha \beta.
\end{align*}
$$

Thus, if $w + x\alpha + y\beta + z\alpha \beta = 0$ we see that $w = x = y = z = 0$. This shows that the list $B = 1, \alpha, \beta, \alpha \beta$ is linearly independent list, but $\dim_K(L) = |G| = 4$, so $B$ must actually be a basis.

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 $\alpha$ is one of the roots of $x^2 + x - 1 = 0$, namely, $\alpha = (-1 \pm \sqrt{5})/2$. However, $\zeta + \zeta^{-1} = \zeta + \bar{\zeta} = 2 \cos(2\pi/5) > 0$, 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 $\sigma_2$. It follows that the only subgroups are the trivial group, the whole group, and the subgroup $A = \{1, -1\}$. This means that the only subfields are $\mathbb{Q}(\mu_5)$, $\mathbb{Q}$ and the
intermediate field $M = \mathbb{Q}(\mu_5)^4$. Now $\sigma_1$ exchanges $\zeta$ and $\zeta^{-1}$ so it fixes $\alpha$ and sends $\beta$ 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:

$$
\begin{array}{ccc}
1 & \{1\} & \mathbb{Q}(\sqrt{-1+\sqrt{5}}/2) \\
2 & H & \mathbb{Q}(\sqrt{5}) \\
4 & G & \mathbb{Q} \\
\end{array}
$$

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
$$
\begin{align*}
\beta &= \zeta + \zeta^{-1} \\
\beta^2 &= \zeta^2 + 2 + \zeta^{-2} \\
\beta^3 &= \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} \\
\beta^4 &= \zeta^4 + 4\zeta^2 + 6\zeta + 4\zeta^{-2} + \zeta^{-4} \\
\beta^5 &= \zeta^5 + 5\zeta^3 + 10\zeta + 10\zeta^{-1} + 5\zeta^{-3} + \zeta^{-5}.
\end{align*}
$$

By combining these, we find that $\beta^5 + \beta^4 - 4\beta^3 - 3\beta^2 + 3\beta + 1 = 0$.

(b) We have
$$
\begin{align*}
\gamma^2 &= \zeta^2 + \zeta^8 + \zeta^7 + \zeta^{10} + \zeta^6 + 2(\zeta^5 + \zeta^3 + \zeta^4 + \zeta^2 + \zeta^9 + \zeta^3 + \zeta + \zeta^8) \\
&= (-1 - \zeta - \zeta^3 - \zeta^4 - \zeta^5 - \zeta^9) + 2(-1) \\
&= -3 - \gamma,
\end{align*}
$$
so $\gamma^2 + \gamma + 3 = 0$. Since $\gamma$ is a root of $x^2 + x + 3 = 0$, we see that $\gamma = (-1 \pm \sqrt{-11})/2$. The terms in $\gamma$ are distributed in the complex plane as follows:
Exercise 11.5: Put \( L = \{ k \in \mathbb{Z}/11^n \} \). We first claim that \( (\mathbb{Z}/11)^\times = \{-5, -4, -3, -2, -1, 1, 2, 3, 4, 5\} \).

The powers of 2 mod 11 are as follows:

\[
2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 5, \quad 2^5 = 10, \quad 2^6 = 4, \quad 2^7 = 8, \quad 2^8 = 5, \quad 2^9 = 10, \quad 2^{10} = 1.
\]

This shows that \( (\mathbb{Z}/11)^\times \) is cyclic of order 10, generated by 2, and thus \( G(K/Q) \) is cyclic of order 10, generated by \( \sigma_2 \). We write

\[
C_{10} = G(K/Q) = \langle \sigma_2 \rangle \\
C_5 = \langle \sigma_2^2 \rangle = \langle \sigma_4 \rangle = \{1, \sigma_4, \sigma_5, \sigma_{-2}, \sigma_3\} \\
C_2 = \langle \sigma_6 \rangle = \langle \sigma_{-1} \rangle = \{1, \sigma_{-1}\} \\
C_1 = \{1\}.
\]

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 \( K^{C_5} = K \). The terms in \( \gamma \) are precisely the orbit of \( \zeta \) 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:

\[
\begin{array}{ccc}
1 & & \{1\} \\
2 & & C_2 \\
5 & & C_5 \\
10 & & C_{10} \end{array}
\]

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 4.21Polynomials over fields theorem) 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 \(\Sigma_3\) (if the discriminant is not a square). Using the formula in Remark 12.3, the cubic theorem, 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 \(\Sigma_3\).

**Exercise 12.2:** The first claim can be checked using Maple as follows:

```maple
r := 1 + q + q^2;
f := (x) -> x^3 - (3*x - 2*q - 1)*r;
gr := 1 + q + q^2;
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 \(x = \alpha\) 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 \(\beta\) is another root of \(f(x)\). Next, as \(f(x)\) is assumed to be irreducible, it must have the form \(\alpha\) is the minimal polynomial of \(\alpha\), 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 \(\sigma: \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)\) with \(\sigma(\alpha) = \beta\).

We next claim that \(\beta \neq \alpha\), or equivalently that \(\alpha\) is not a root of the quadratic polynomial \(s(x) - x\). This is clear because the minimal polynomial of \(\alpha\) 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 \(\sigma\) is a nontrivial element, so we must have \(G(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma, \sigma^2\}\).

**Exercise 12.3:**

(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:

\[
\det \begin{bmatrix} 1 & \beta & \gamma \\ \alpha & \beta^2 & \gamma^2 \end{bmatrix} = \det \begin{bmatrix} 1 & 0 & 0 \\ \alpha^2 & \beta^2 - \alpha \beta & \gamma^2 - \alpha \gamma \end{bmatrix} = (\beta - \alpha)(\gamma - \alpha) \det \begin{bmatrix} 1 & 0 & 0 \\ \alpha^2 & \beta + \alpha \gamma + \alpha \end{bmatrix} = (\beta - \alpha)(\gamma - \alpha)(\gamma - \beta) = \delta(f).
\]

(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
\[
(\alpha^3 + \beta^3 + \gamma^3) + a(\alpha + \beta + \gamma) + b(1 + 1 + 1) = 0,
\]

20
or \( S_3 + aS_1 + bS_0 = 0 \). Thus \( S_3 = -aS_1 - bS_0 \). Also, add

\[
\begin{align*}
\alpha^4 + a\alpha^2 + b\alpha &= 0 \\
\beta^4 + a\beta^2 + b\beta &= 0 \\
\gamma^4 + a\gamma^2 + b\gamma &= 0
\end{align*}
\]

to get \( S_4 = -aS_2 - bS_1 \). Thus we conclude that

\[
S_3 = -3b \\
S_4 = 2a^2.
\]

(f) Substituting the values of \( S_0, \ldots, S_4 \) into the matrix in (c), we get:

\[
M M^T = \begin{pmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{pmatrix}.
\]

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 \( A_4 \). 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 \( \Sigma_3 \), so the Galois group for \( f_1(x) \) is \( \Sigma_4 \).

**Exercise 13.2:** The discriminant is

\[
\prod_{i<j}(\alpha_i - \alpha_j)^2 = (\alpha_0 - \alpha_1)^2(\alpha_0 - \alpha_2)^2(\alpha_0 - \alpha_3)^2(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2
\]

\[
= (2\sqrt{5})^2(2\sqrt{2})^2(2\sqrt{2} + 2\sqrt{5})^2(2\sqrt{2} - 2\sqrt{5})^2(2\sqrt{2})^2(2\sqrt{5})^2
\]

\[
= 2^{14}5^2(\sqrt{5} + \sqrt{2})^2(\sqrt{5} - \sqrt{2})^2
\]

\[
= 2^{14}5^2(5 - 2)^2 = 2^{14}3^25^2 = 3686400.
\]

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

\[
M M^T = \begin{pmatrix} S_0 & S_1 & S_2 & S_3 \\ S_1 & S_2 & S_3 & S_4 \\ S_2 & S_3 & S_4 & S_5 \\ S_3 & S_4 & S_5 & S_6 \end{pmatrix}.
\]
From the factorisation \( f(x) = (x - \alpha)(x - \beta)(x - \gamma)(x - \delta) \) we obtain
\[
\begin{align*}
\alpha + \beta + \gamma + \delta &= 0 \\
\alpha \beta + \alpha \gamma + \alpha \delta + \beta \gamma + \beta \delta + \gamma \delta &= 0 \\
\alpha \beta \gamma + \alpha \beta \delta + \alpha \gamma \delta + \beta \gamma \delta &= -p \\
\alpha \beta \gamma \delta &= q.
\end{align*}
\]
From this we deduce that \( S_0 = 4, S_1 = 0 \) and \( S_2 = 0 \). To compute \( S_3 \), use
\[
\begin{align*}
\alpha^3 + \beta^3 + \gamma^3 + \delta^3 &= S_1^3 - 3(\alpha^2 \beta + \text{similar terms}) - 6(\alpha \beta \gamma + \text{similar terms}) \\
\alpha^2 \beta + \text{similar terms} &= S_1(\alpha \beta + \text{similar terms}) - 3(\alpha \beta \gamma + \text{similar terms}) \\
\alpha \beta \gamma + \text{similar terms} &= -p.
\end{align*}
\]
Combining these, together with \( S_1 = 0 \), we see that \( S_3 = -3p \). Using the same trick as in Exercise 12.3Cubicsexercise.12.3, we get that
\[
\begin{align*}
S_4 &= -(pS_1 + qS_0) = -4q \\
S_5 &= -(pS_2 + qS_1) = 0 \\
S_6 &= -(pS_3 + qS_2) = -3p^2
\end{align*}
\]
and so
\[
\Delta(f) = \det \begin{pmatrix}
4 & 0 & 0 & -3p \\
0 & 0 & -3p & -4q \\
-3p & -4q & 0 & 0
\end{pmatrix} = 27p^4 + 256q^3.
\]

**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 \( \Sigma_4 \).)
- \( f_1(x) \) 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 \( \Sigma_5 \) by Corollary 7.8Some extensions of small degreethem.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 \( \alpha, \beta \) and \( \gamma \), then the roots of \( f_2(x) \) are \( \pm \sqrt[3]{{\alpha}}, \pm \sqrt[3]{{\beta}} \) and \( \pm \sqrt[3]{{\gamma}} \). 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 \( \Sigma_6 \) 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 \( \Sigma_5 \), 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 7.8Some extensions of small degreethem.7.8 to see that the Galois group is \( \Sigma_5 \) 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 \( \Sigma_7 \). Using Corollary 7.8Some extensions of small degreethem.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

\[ f(x) \rightarrow -\infty \text{ as } x \rightarrow -\infty \]
\[ f(-1) = 26 \]
\[ f(0) = -21 \]
\[ f(1) = 2 \]
\[ f(2) = -325 \]
\[ f(x) \rightarrow +\infty \text{ as } x \rightarrow +\infty \]

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 \(\rho_{10}\) is the identity, and that \(\rho_{1/a,-b/a}\) is an inverse for \(\rho_{ab}\). This means that \(U\) is a subgroup of \(\Sigma_5\). Now define \(\pi: U \rightarrow \mathbb{F}_5^\times\) by \(\pi(\rho_{ab}) = a\).

The above composition formula shows that \(\pi(\rho_{ab}\rho_{cd}) = ac = \pi(\rho_{ab})\pi(\rho_{cd})\), so \(\pi\) 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 \(\pi\) is surjective. The kernel is \(V = \{\rho_{ib} \mid b \in \mathbb{F}_5\}\), which is therefore a normal subgroup. The First Isomorphism Theorem tells us that \(U/V \cong \mathbb{F}_5^\times = \{-2, -1, 1, 2\}\), 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 \(\rho_{11}\).

(b) Let \(H\) be a subgroup of \(\Sigma_5\), and let \(C\) be a normal subgroup of \(H\) that is cyclic of order 5. Choose a generator \(\sigma\) for \(C\). This has order 5, and by considering the possible cycle types in \(\Sigma_5\) we see that it must be a 5-cycle, say \(\sigma = (p_0 \ p_1 \ p_2 \ p_3 \ p_4)\). Let \(\theta\) 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 \(\tau\rho_{11}^{-1}\tau^{-1}\) must be another generator for \(V\), so \(\tau\rho_{11}^{-1}\tau^{-1} = \rho_{1a}\) 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

\[ \rho_{ab}\rho_{11}\rho_{ab}^{-1} = \rho_{a,a+b}\rho_{1/a,-b/a} = \rho_{1a} = \tau\rho_{11}\tau^{-1}, \]

where \(\tau = \rho_{ab}\).
so \(\phi\rho_{11}\phi^{-1} = \rho_{11}\). This means that \(\phi\) commutes with \(\rho_{11}\), 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 \(\phi\) is the identity as claimed, so \(\tau = \rho_{ab}\). As \(\tau\) 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 \(\Sigma_5\). 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 \(|H| = |Hx| |\text{stab}_H(x)| = 5|\text{stab}_H(x)|\), 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 \(\Sigma_5\). 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 \(\Sigma_5\), 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 \(\Sigma_6\), 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).