Module MA3411: Galois Theory
Worked Solutions to Problems
Michaelmas Term 2013

1. *Use Eisenstein's criterion to verify that the following polynomials are irreducible over* $\mathbb{Q}$*:—*

   (i) $x^2 - 2$*;*

   (ii) $x^3 + 9x + 3$*;*

   (iii) $x^5 + 26x + 52$*.*

   The requirements of Eisenstein' Criterion are satisfied with the prime number employed in that criterion equal to 2, 3 and 13 in cases (i), (ii) and (iii) respectively.

2. *The Fundamental Theorem of Algebra ensures that every non-constant polynomial with complex coefficients factors as a product of polynomials of degree one. Use this result to show that a non-constant polynomial with real coefficients is irreducible over the field* $\mathbb{R}$ *of real numbers if and only if it is either a polynomial of the form* $ax + b$ *with* $a \neq 0$ *or a quadratic polynomial of the form* $ax^2 + bx + c$ *with* $a \neq 0$ *and* $b^2 < 4ac$*.*

   Polynomials over the form $ax + b$ can only have factors of degrees zero and one and are thus irreducible. A quadratic polynomial of the form $ax^2 + bx + c$ with $a \neq 0$ and $b^2 < 4ac$ has non-real roots and therefore cannot be factored as a product of two polynomials of degree one. Such quadratic polynomials are thus irreducible over the field of real numbers.

   Let $f(x)$ be an polynomial with real coefficients that is irreducible over the field $\mathbb{R}$ of real numbers. It follows from the Fundamental Theorem of Algebra that the polynomial f has at least one root in the field of complex numbers. Let α be a root of f. If α is a real number then $x - \alpha$ is a factor of f in the polynomial ring $\mathbb{R}[x]$, and therefore $f(x) = a(x - \alpha)$, where a is the leading coefficient of f. If α is not a real number then its complex conjugate $\overline{\alpha}$ is also a root of f. But then $(x - \alpha)(x - \overline{\alpha})$ is a polynomial with real coefficients that divides the irreducible polynomial f in the polynomial ring $\mathbb{R}$. Indeed

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + |\alpha|^2 = x^2 + 2px + p^2 + q^2,$$

where the real numbers p and q are the real and imaginary parts respectively of the complex number α. It follows from the irreducibility of f that

$$f(x) = a(x-\alpha)(x-\overline{\alpha}) = ax^2 + bx + c,$$

where $b = 2pa$ and $c = (p^2+q^2)a$. Moreover

$$b^2 = 4p^2a^2 < 4(p^2+q^2)a^2 = 4ac.$$

It follows that a polynomial with real coefficients that is irreducible over the field of real numbers must either be of the form $ax+b$, where $a, b \in \mathbb{R}$ and $a \neq 0$, or else must be of the form ax^2+bx+c, where $a, b, c \in \mathbb{R}$, $a \neq 0$ and $b^2 < 4ac$.

3. *Let d be a rational number that is not the square of any rational number, let $\sqrt{d}$ be a complex number satisfying $(\sqrt{d})^2 = d$, and let L denote the set of all complex numbers that are of the form $a + b\sqrt{d}$ for some rational numbers a and b. Prove that L is a subfield of the field of complex numbers, and that $L:\mathbb{Q}$ is a finite field extension of degree 2.*

If $z_1, z_2 \in L$ then $z_1 + z_2 \in L$, $z_1 - z_2 \in L$ and $z_1 z_2 \in L$. Indeed if $z_1 = a_1 + b_1\sqrt{d}$ and $z_2 = a_2 + b_2\sqrt{d}$ then

$$\begin{aligned} z_1 + z_2 &= (a_1+a_2) + (b_1+b_2)\sqrt{d}, \\ z_1 - z_2 &= (a_1-a_2) + (b_1-b_2)\sqrt{d}, \\ z_1 z_2 &= (a_1a_2 + b_1b_2d) + (a_1b_2 + b_1a_2)\sqrt{d}. \end{aligned}$$

The set L is therefore a unital commutative ring. In order to show that L is a field, it remains to show that all non-zero elements of L are invertible. Let a and b be rational numbers that are not both zero. Then

$$(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - b^2d,$$

Moreover $b^2d \neq a^2$, because d is not the square of any rational number. It follows that the reciprocal of $a + b\sqrt{d}$ is in L for all $a + b\sqrt{d} \in L$, and

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

The elements 1 and $\sqrt{d}$ are linearly independent over the field of rational numbers, because $\sqrt{d}$ is not itself a rational number, and therefore the field L is a two-dimensional vector space over the field $\mathbb{Q}$ of rational numbers with basis $1, \sqrt{d}$.

4. *A complex number is said to be* algebraic *if it is a root of some non-zero polynomial f with rational coefficients. A complex number is thus algebraic if and only if it is algebraic over the field $\mathbb{Q}$ of rational numbers. Moreover a simple field extension $K(\alpha)\colon K$ is finite if and only if the adjoined element α is algebraic over the ground field K. Thus a complex number z is algebraic if and only if $\mathbb{Q}(z)\colon\mathbb{Q}$ is a finite field extension. Use the Tower Law to prove that the set of all algebraic numbers is a subfield of $\mathbb{C}$.*

   Let z and w be algebraic numbers. The algebraic number w is algebraic over the field $\mathbb{Q}$ and is therefore algebraic over the field $\mathbb{Q}(z)$. It follows that $\mathbb{Q}(z)(w)\colon\mathbb{Q}(z)$ is a finite field extension. Now $\mathbb{Q}(z)(w) = \mathbb{Q}(z, w)$, because both fields are the smallest subfields of the complex numbers that contain the rational numbers together with the complex numbers z and w. It follows from the Tower Law that $\mathbb{Q}(z, w)\colon\mathbb{Q}$ is a finite field extension. Now the elements $z + w$, $z - w$ and zw all belong to $\mathbb{Q}(z, w)$. It follows that the field extensions $\mathbb{Q}(z + w)\colon\mathbb{Q}$, $\mathbb{Q}(z - w)\colon\mathbb{Q}$ and $\mathbb{Q}(zw)\colon\mathbb{Q}$, are finite, and therefore the complex numbers $z+w$, $z-w$ and zw are algebraic numbers. Moreover if $w \neq 0$ then $zw^{-1} \in \mathbb{Q}(z, w)$ and therefore zw^{-1} is an algebraic number. Thus the set of all algebraic numbers is a subfield of the field $\mathbb{C}$ of complex numbers.

5. *Let L be a splitting field for a polynomial of degree n with coefficients in K. Prove that $[L\colon K] \leq n!$.*

   We prove the result by induction on n. If L is a splitting field for a polynomial $ax + b$ of degree 1 with coefficients a and b in K then the unique root of that polynomial is $-b/a$, which is in K, and therefore $L = K$ and $[L\colon K] = 1$. Thus the result holds for $n = 1$.

   Suppose that $[M\colon K] \leq m!$ whenever M is a splitting field for a polynomial g of degree m with coefficients in K. Let L be a splitting field over K for some polynomial f of degree $m + 1$ with coefficients in K. Then all roots of f are in L. Let α be one of the roots of f. Then $f(x) = (x - \alpha)g(x)$ for some polynomial g satisfying $\deg g = m$. The polynomial g splits over L, and therefore there is a unique subfield M of L that is a splitting field for M over K. The induction hypothesis ensures that $[M\colon K] \leq m!$. Now $L = M(\alpha)$. It follows from a standard result concerning simple algebraic extensions that $[L\colon M]$ is equal to the degree of the minimum polynomial of α over M. This minimum polynomial divides the polynomial f and therefore is at most $m+1$. It

follows from the Tower Law that

$$[L\colon K] = [L\colon M][M\colon K] \leq (m+1)[M\colon K] \leq (m+1)m! = (m+1)!,$$

as required.

6. (a) *Using Eisenstein's criterion, or otherwise, prove that* $\sqrt{3}$ *is not a rational number, and is not of the form* $b\sqrt{2}$ *for any rational number* b*. Hence or otherwise, show that there cannot exist rational numbers* a *and* b *such that* $\sqrt{3} = a + b\sqrt{2}$*, and thus prove that* $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$*.*

An immediate application of Eisenstein's criterion shows that the polynomial polynomial $x^2 - 3$ is irreducible over the field of rational numbers. This polynomial is thus the minimum polynomial of $\sqrt{3}$ over the field $\mathbb{Q}$ of rational numbers. An application of Eisenstein's criterion with prime number 3 shows that the polynomial $2x^2 - 3$ is also irreducible. It follows that $\sqrt{3}/\sqrt{2}$ is not a rational number.
If it were the case that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ then there would exist rational numbers a and b such that $\sqrt{3} = a + b\sqrt{2}$. But then

$$3 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{3}.$$

But $\sqrt{3} \notin \mathbb{Q}$. Therefore it would follow that $ab = 0$, and thus either $a = 0$ or $b = 0$. But $b = 0$ would imply that $\sqrt{3} \in \mathbb{Q}$, which is not the case, and $a = 0$ would imply that $\sqrt{3} = b\sqrt{2}$, which is not the case. Therefore there cannot exist rational numbers a and b such that $\sqrt{3} = a + b\sqrt{2}$. It follows that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

(b) *Explain why* $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$*, and, using the result of (a) and the Tower Law, or otherwise, prove that* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = 4$*.*

Now $\mathbb{Q}(\sqrt{2}) \cup \{\sqrt{3}\} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and therefore

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Also $\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\} \subset \mathbb{Q}(\sqrt{2})(\sqrt{3})$, and therefore

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3}).$$

Therefore

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

It was shown in (a) that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. It follows that the polynomial $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, and is therefore the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. It follows that $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, and thus $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. It then follows from the Tower Law that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4,$$

as required.

(c) *Show that* $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ *and* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = 4$. *What is the degree of the minimum polynomial of* $\sqrt{2} + \sqrt{3}$ *over* $\mathbb{Q}$*?*

Clearly $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and therefore $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. To prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$, it suffices to show that $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Now $(\sqrt{2} + \sqrt{3})^n \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ for all positive integers n. Moreover

$$\begin{aligned}
(\sqrt{2} + \sqrt{3})^2 &= 2 + 3 + 2\sqrt{2}\,\sqrt{3} \\
&= 5 + 2\sqrt{6} \\
(\sqrt{2} + \sqrt{3})^3 &= (\sqrt{2} + \sqrt{3})(5 + 2\sqrt{6}) = 5\sqrt{2} + 5\sqrt{3} + 2\sqrt{12} + 2\sqrt{18} \\
&= 11\sqrt{2} + 9\sqrt{3}.
\end{aligned}$$

It follows that

$$\sqrt{2} = \frac{1}{2}(\sqrt{2} + \sqrt{3})^3 - \frac{9}{2}(\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

But then

$$\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

It follows that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$, and therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(d) *Show that* $\sqrt{2} + \sqrt{3}$ *is a root of the polynomial* $x^4 - 10x^2 + 1$*, and thus show that this polynomial is an irreducible polynomial whose splitting field over* $\mathbb{Q}$ *is* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Now

$$\begin{aligned}
(\sqrt{2} + \sqrt{3})^4 &= (\sqrt{2} + \sqrt{3})(11\sqrt{2} + 9\sqrt{3}) \\
&= 49 + 20\sqrt{6}
\end{aligned}$$

and therefore

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 0.$$

Thus $(\sqrt{2}+\sqrt{3})^4$ is a root of the polynomial $x^4 - 10x^2 + 1$. But

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4,$$

and therefore the minimum polynomial of $\sqrt{2}+\sqrt{3}$ must be a monic polynomial of degree 4. This monic polynomial must also divide the polynomial $x^4 - 10x^2 + 1$. Therefore $x^4 - 10x^2 + 1$ is the minimum polynomial of $\sqrt{2}+\sqrt{3}$. Thus x^4-10x^2+1 is an irreducible polynomial whose splitting field over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

(e) *Let φ_1 and φ_2 be $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Suppose that $\varphi_1(\sqrt{2}) = \varphi_2(\sqrt{2}) = \sqrt{2}$ and $\varphi_1(\sqrt{3}) = \varphi_2(\sqrt{3}) = \sqrt{3}$. Explain why $\varphi_1 = \varphi_2$.*

The set $\mathbb{Q} \cup \{\sqrt{2},\sqrt{3}\}$ is contained in the fixed field of $\varphi_2^{-1}\varphi_1$, and therefore the fixed field of $\varphi_2^{-1}\varphi_1$ must be the whole of $\mathbb{Q}(\sqrt{2},\sqrt{3})$, and thus $\varphi_1 = \varphi_2$.

(f) *Prove that there exist $\mathbb{Q}$-automorphisms σ and τ of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ satisfying*

$$\begin{array}{ll} \sigma(\sqrt{2}) = \sqrt{2}, & \sigma(\sqrt{3}) = -\sqrt{3}; \\ \tau(\sqrt{2}) = -\sqrt{2}, & \tau(\sqrt{3}) = \sqrt{3}; \end{array}.$$

The field $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field for the polynomial $x^2 - 3$ over the field $\mathbb{Q}(\sqrt{2})$ Moreover the polynomial $x^3 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$ and has roots $\sqrt{3}$ and $-\sqrt{3}$. It follows from the theory of isomorphisms of splitting fields that there exists an automorphism σ of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ that fixes the subfield $\mathbb{Q}(\sqrt{2})$ and satisfies $\sigma(\sqrt{3}) = -\sqrt{3}$. Similarly there exists an automorphism τ of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ that fixes the subfield $\mathbb{Q}(\sqrt{3})$ and satisfies $\tau(\sqrt{2}) = -\sqrt{2}$.

(g) *Prove that the $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$, constitute a group of order 4 isomorphic to a direct product of two cyclic groups of order 2.*

Let ι denote the identity automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and let $G = \{\iota, \sigma, \tau, \sigma\tau\}$. Now

$$\begin{array}{ll} \iota(\sqrt{2}) = \sqrt{2}, & \iota(\sqrt{3}) = \sqrt{3}; \\ \sigma(\sqrt{2}) = \sqrt{2}, & \sigma(\sqrt{3}) = -\sqrt{3}; \\ \tau(\sqrt{2}) = -\sqrt{2}, & \tau(\sqrt{3}) = \sqrt{3}; \\ \sigma\tau(\sqrt{2}) = -\sqrt{2}, & \sigma\tau(\sqrt{3}) = -\sqrt{3}. \end{array}$$

Moreover it follows from (e) that any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is determined by its action on $\sqrt{2}$ and $\sqrt{3}$. The possible images of $\sqrt{2}$ and $\pm\sqrt{2}$, and the possible images of $\sqrt{3}$ are $\pm\sqrt{3}$. It follows that the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$ can have at most four $\mathbb{Q}$-automorhisms. Thus the group G is the group of $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Moreover $\sigma\tau = \tau\sigma$, since the composition of σ with τ in either order sends $\sqrt{2}$ to $-\sqrt{2}$ And sends $\sqrt{3}$ to $-\sqrt{3}$. It follows that the group G is isomorphic to the direct product of the two subgroups $\{\iota,\sigma\}$ and $\{\iota\tau\}$. These subgroups are of order 2.

7. *Let K be a field of characteristic p, where p is prime.*

   (a) *Show that $f \in K[x]$ satisfies $Df = 0$ if and only if $f(x) = g(x^p)$ for some $g \in K[x]$.*

   Let
   $$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n = \sum_{j=0}^{n} c_j x^k.$$
   Then
   $$(Df)(x) = \sum_{j=1}^{n} j.c_j x^{j-1}.$$
   Now $j.c_j = (j.1_K)c_j$ for $j = 0, 1, \ldots, n$, where 1_K denotes the identity element of the field K. Also $j.1_K = 0_K$ if and only if j is divisible by the prime number p, because K is a field of characteristic p. Thus if $(Df) = 0$ then $(j.1_K)c_j = 0_K$ for all positive integers j satisfying $0 < j \leq n$, and therefore $c_j = 0_K$ for all positive integers j satisfying $0 < j \leq n$ that are not divisible by the prime number p. It follows that if $f \neq 0$ and $Df = 0$ then f is of degree mp for some non-negative integer p, and
   $$f(x) = x_0 + c_p x^p + c_{2p} x^{2p} + \cdots + c_{mp} x^{mp} = g(x^p),$$
   where
   $$g(x) = x_0 + c_p x + c_{2p} x^2 + \cdots + c_{mp} x^m.$$

   (b) *Let $h(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, where $a_0, a_1, \ldots, a_n \in K$. Show that $(h(x))^p = g(x^p)$, where $g(x) = a_0^p + a_1^p x + a_2^p x^2 + \cdots + a_n^p x^n$.*

Let $h_0(x)$ and $h_1(x)$ be polynomials with coefficients in the field K. Then

$$\Big(h_0(x) + h_1(x)\Big)^p = \sum_{j=0}^{p} \left(\begin{array}{c} p \\ j \end{array} \right) \cdot h_0(x)^{p-j} h_1(x)^j = h_0(x)^p + h_1(x)^p.$$

Indeed the Commutative, Associative and Distributive Laws are satisfied in the polynomial ring $K[x]$, and therefore the appropriate form of the Binomial Theorem is applicable in this ring. But the binomial coefficient $\left(\begin{array}{c} p \\ j \end{array} \right)$ is an integer divisible by p when $0 < j < p$, and therefore $\left(\begin{array}{c} p \\ j \end{array} \right) \cdot f(x) = 0$ for all polynomials $f(x)$ with coefficients in the field K when $0 < j < p$.
It follows by induction on n that

$$\left(\sum_{k=0}^{n} h_k(x) \right)^p = \sum_{k=0}^{n} h_k(x)^p$$

for all $h_0, h_1, \ldots, h_n \in K[x]$. In particular, if $h(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, then

$$h(x)^p = \left(\sum_{k=0}^{n} a_k x^k \right)^p = \sum_{k=0}^{n} a_k^p x^{kp} = g(x^p),$$

where $g(x) = a_0^p + a_1^p x + a_2^p x^2 + \cdots + a_n^p x^n$.

(c) *Now suppose that Frobenius monomorphism of K is an automorphism of K. Show that $f \in K[x]$ satisfies $Df = 0$ if and only if $f(x) = (h(x))^p$ for some $h \in K[x]$. Hence show that $Df \neq 0$ for any irreducible polynomial f in $K[x]$.*

Suppose that $f \in K[x]$ satisfies $Df = 0$. Then $f(x) = g(x_p)$ for some $g \in K[x]$. Let $g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$. Now, for each integer j between 0 and n there is some element a_j of K such that $a_j^p = c_j$, because the Frobenius monomorphism of K is an automorphism and is thus surjective. But then

$$g(x) = a_0^p + a_1^p x + a_2^p x^2 + \cdots + a_n^p x^n.$$

It follows from (b) that $f(x) = g(x^p) = h(x)^p$, where

$$h(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

We conclude that if $f \in K[x]$ satisfies $Df = 0$ then $f(x) = h(x)^p$ for seom $h \in K[x]$.

We now verify the converse. A straightforward proof by induction on k shows that $D(h(x))^k = k.h(x)^{k-1}Dh(x)$ for all positive integers k. In particular $D(h(x))^p = p.h(x)^{p-1}Dh(x) = 0$. We conclude that if the Frobenius monomorphism of the field K is an automorphism, and if $f \in K[x]$ satisfies $Df = 0$ then $f(x) = h(x)^p$ for some $h \in K[x]$.

(d) *Use these results to show that every algebraic extension $L\colon K$ of a finite field K is separable.*

An irreducible polynomial $f \in K[x]$ is inseparable if and only if $Df = 0$. (see Corollary 6.8). But if K is a finite field, then every injective function from K to itself is surjective, and therefore every monomorphism from K to itself is an automorphism. In particular the Frobenius monomorphism of a finite field is an automorphism. It follows from (c) that a polynomial $f \in K[x]$ satisfies $Df = 0$ if and only if $f(x) = h(x)^p$ for some $h \in K[x]$. We conclude from this that no irreducible polynomial f with coefficients in K can satisfy $Df = 0$. Thus there are no inseparable polynomials with coefficients in a finite field K, and therefore every algebraic extension $L\colon K$ of a finite field K is separable.

8. *For each positive integer n, let ω_n be the primitive nth root of unity in $\mathbb{C}$ given by $\omega_n = \exp(2\pi i/n)$, where $i = \sqrt{-1}$. Explain why the field extensions $\mathbb{Q}(\omega_n)\colon\mathbb{Q}$ and $\mathbb{Q}(\omega_n, i)\colon\mathbb{Q}$ are normal field extensions for all positive integers n.*

The field $\mathbb{Q}(\omega_n)$ is a splitting field for the polynomial $x^n - 1$ over $\mathbb{Q}$, since the roots of this polynomial are powers of ω_n. Any splitting field extension is both finite and normal.

The field $\mathbb{Q}(\omega_n, i)$ is a splitting field for the polynomial $(x^n - 1)(x^2 + 1)$ over $\mathbb{Q}$. Any splitting field extension is both finite and normal.

9. (a) *Let p be a prime number. The* cyclotomic polynomial $\Phi_p(x)$ *is defined by*

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}.$$

Show that

$$x\Phi_p(x + 1) = (x + 1)^p - 1,$$

and hence show that

$$\Phi_p(x) = \sum_{k=0}^{p-1} \left(\begin{array}{c} p \\ k+1 \end{array} \right) x^k,$$

where $\left(\begin{array}{c} p \\ k+1 \end{array} \right)$ *is the binomial coefficient whose value is the number of ways of choosing* $k+1$ *objects from a collection of* p *objects.*

The cyclotomic polynomial $\Phi_p(x)$ satisfies the identity $(x-1)\Phi_p(x) = x^p - 1$. On substituting $x+1$ for x, we find that $x\Phi_p(x) = (x+1)^p - 1$. On expanding $(x+1)^p$ using the Binomial Theorem, we find that

$$x\Phi_p(x) = \sum_{k=1}^{p} \binom{p}{k} x^k.$$

On substituting $k+1$ for k in this formula, we find that

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

(b) *If* p *be a prime number, then the binomial coefficient* $\left(\begin{array}{c} p \\ k+1 \end{array} \right)$ *is divisible by* p *for all integers* k *satisfying* $0 < k < p$. *By making use of this result or otherwise, show that the cyclotomic polynomial* $\Phi_p(x)$ *is irreducible over* $\mathbb{Q}$ *for all prime numbers* p.

The cyclotomic polynomial $\Phi_p(x)$ is a polynomial of degree $p-1$, and its leading coefficient $\left(\begin{array}{c} p \\ p \end{array} \right)$ is equal to 1. The remaining coefficients of this polynomial are divisible by the prime number p. The constant coefficient is $\left(\begin{array}{c} p \\ 1 \end{array} \right)$, and this coefficient has the value p. Therefore the constant coefficient of $\Phi_p(x)$ is not divisible by p^2. We have thus verified that the leading coefficient of $\Phi_p(x)$ is not divisible by the prime number p, the remaining coefficients are all divisible by p, and the constant coefficient is not divisible by p^2. The conditions of Eisenstein's criterion for irreducibility are therefore satisfied with respect to the prime number p. We conclude therefore that $\Phi_p(x)$ is an irreducible monic polynomial of degree $p-1$ over the field $\mathbb{Q}$ of rational numbers.

(c) *Let* p *be a prime number, and let* $\omega_p = \exp(2\pi i/p)$, *where* $i = \sqrt{-1}$. *Prove that the minimum polynomial of* ω_p *over* $\mathbb{Q}$ *is the* cyclotomic polynomial $\Phi_p(x)$, *where* $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$.

It was shown in (b) that, for each prime number p, the cyclotomic polynomial $\Phi_p(x)$ is an irreducible monic polynomial of degree $p-1$ over the field $\mathbb{Q}$ of rational numbers. It follows from this that it is the minimum polynomial of each of its roots. Those roots include ω_p.
Now the coefficient of x^k in $\Phi_p(x)$ is the binomial coefficient $\binom{p}{k+1}$. This coefficient is divisible by the prime number p for $0 \leq k < p-1$. Moreover the leading coefficient has the value 1, and constant coefficient has the value p. It follows from Eisenstein's Criterion, that the polynomial Φ_p is irreducible over $\mathbb{Q}$. Moreover it is a monic polynomial which has ω_p as a root. Therefore $\Phi_p(x)$ is the minimum polynomial of ω_p. It follows from a standard theorem concerning simple algebraic extensions that

$$[\mathbb{Q}(\omega_p)\colon\mathbb{Q}] = \deg \Phi_p = p-1,$$

as required.

(d) *Explain why* $[\mathbb{Q}(\omega_p)\colon\mathbb{Q}] = p-1$ *for all prime numbers* p*, where* $\omega_p = \exp(2\pi i/p)$.

The degree of the simple field extension $\mathbb{Q}(\omega_p)\colon\mathbb{Q}$ is equal to the degree of the minimum polynomial of ω_p over the ground field $\mathbb{Q}$. But the minimum polynomial of ω_p over $\mathbb{Q}$ is the cyclotomic polynomial $\Phi_p(x)$, and this polynomial has degree $p-1$. The result follows.

10. *Throughout this question, let* $\omega = \omega_5 = \exp(2\pi i/5)$ *and* $\xi = \sqrt[5]{2}$. *Also let* $\Phi_5(x)$ *denote the cyclotomic polynomial*

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

The field $\mathbb{Q}(\omega)$ *is a splitting field for the polynomial* $\Phi_5(x)$ *over the field of rational numbers. Note that it was shown in Question 9 that the cyclotomic polynomial* $\Phi_5(x)$ *is irreducible over the field* $\mathbb{Q}$ *of rational numbers, and that therefore* $[\mathbb{Q}(\omega)\colon\mathbb{Q}] = 4$.

(a) *Show that the field* $\mathbb{Q}(\xi,\omega)$ *is a splitting field for the polynomial* x^5-2 *over* $\mathbb{Q}$.

The roots of the polynomial x^5-2 in $\mathbb{C}$ are of the form $\xi\omega^r$ for $r = 0,1,2,3,4$. These roots all belong to the subfield $\mathbb{Q}(\xi,\omega)$ of $\mathbb{C}$. Let L be a subfield of $\mathbb{C}$ that contains all these roots. Then $\xi \in L$. Also L contains the ratio of the roots $\xi\omega$ and ξ, and therefore $\omega \in L$. Therefore $\mathbb{Q}(\xi,\omega) \in L$. Thus $\mathbb{Q}(\xi,\omega)$ is the smallest subfield of $\mathbb{C}$ that contains all rational numbers and also contains all the roots of the polynomial x^5-2. This field $\mathbb{Q}(\xi,\omega)$ is thus a splitting field for x^5-2 over $\mathbb{Q}$.

(b) *Show that* $[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}] = 20$ *and* $[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}(\omega)] = 5$. *Hence or otherwise, show that* $x^5 - 2$ *is the minimum polynomial of* $\xi\omega^s$ *over the field* $\mathbb{Q}(\omega)$ *for* $s = 0, 1, 2, 3, 4$.

The polynomial $x^5 - 2$ is irreducible, by Eisenstein's Criterion, with the prime number equal to 2, and therefore $[\mathbb{Q}(\xi)\colon\mathbb{Q}] = 5$.
Now it follows from the Tower Law that $[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}]$ is divisible by both $[\mathbb{Q}(\xi)\colon\mathbb{Q}]$ and $[\mathbb{Q}(\omega)\colon\mathbb{Q}]$, since $\mathbb{Q}(\xi)$ and $\mathbb{Q}(\omega)$ are both subfields of $\mathbb{Q}(\xi,\omega)$. Thus $[\mathbb{Q}(\xi)\colon\mathbb{Q}]$ is divisible by both 5 and 4, and is thus divisible by 20. But $\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}(\omega)$ is a simple algebraic extension, and the degree of this extension is equal to the degree of the minimum polynomial of ξ over $\mathbb{Q}(\omega)$. This minimum polynomial divides $x^5 - 2$. Therefore $[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}(\omega)] \leq 5$. Now an immediate application of the Tower Law shows that

$$[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}] = [\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}(\omega)][\mathbb{Q}(\omega)\colon\mathbb{Q}] \leq 20.$$

But we have already shown that this degree is divisible by 20. Therefore $[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}] = 20$. Moreover $[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}(\omega)] = 5$, and therefore the minimum polynomial of ξ over $\mathbb{Q}(\omega)$ is a monic polynomial of degree 5. We see from this that $x^5 - 2$ must be the minimum polynomial of ξ over $\mathbb{Q}(\omega)$. This polynomial is thus irreducible and is therefore the minimum polynomial of each of its roots over $\mathbb{Q}(\omega)$. These roots are of $\xi\omega^s$ over the field $\mathbb{Q}(\omega)$ for $s = 0, 1, 2, 3, 4$.

(c) *Prove that the Galois* $\Gamma(\mathbb{Q}(\xi,\omega)\colon\mathbb{Q})$ *consists of the automorphisms* $\theta_{r,s}$ *for* $r = 1, 2, 3, 4$ *and* $s = 0, 1, 2, 3, 4$, *where* $\theta_{r,s}(\omega) = \omega^r$ *and* $\theta_{r,s}(\xi) = \omega^s\xi$.

The elements ξ and $\xi\omega$ of $\mathbb{Q}(\xi,\omega)$ have the same minimum polynomial over the field $\mathbb{Q}(\omega)$. A basic theorem in Galois Theory then ensures that there exists an automorphism σ of $\mathbb{Q}(\xi,\omega)$ such that $\sigma(\xi) = \xi\omega$ and $\sigma(z) = z$ for all $z \in \mathbb{Q}(\omega)$. Note that $\sigma(\omega) = \omega$.
Now it also follows from the Tower Law that

$$[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}] = [\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}(\xi)][\mathbb{Q}(\xi)\colon\mathbb{Q}],$$

where $[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}] = 20$ and $[\mathbb{Q}(\xi)\colon\mathbb{Q}] = 5$. It follows that

$$[\mathbb{Q}(\xi,\omega)\colon\mathbb{Q}(\xi)] = 4.$$

Therefore the minimum polynomial Φ_5 of ω over $\mathbb{Q}$ is also the minimum polynomial of ω over $\mathbb{Q}(\xi)$. It follows that there exists an automorphism τ of $\mathbb{Q}(\xi,\omega)$ such that $\tau(\omega) = \omega^2$ and $\tau(z) = z$ for all

$z \in \mathbb{Q}(\xi)$. Note that $\tau(\xi) = \xi$. Moreover $\tau^2(\omega) = \tau(\tau(\omega)) = \omega^4$, and $\tau^3(\omega) = \tau(\tau^2(\omega)) = \omega^8 = \omega^3$. Let $\theta_{1,s} = \sigma^s$, $\theta_{2,s} = \sigma^s\tau$, $\theta_{3,s} = \sigma^s\tau^3$ and $\theta_{4,s} = \sigma^s\tau^2$. Then $\theta_{r,s}$ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\xi, \omega)$ for $r = 1, 2, 3, 4$ and $s = 0, 1, 2, 3, 4$. Also $\theta_{1,s}(\omega) = \sigma^s(\omega) = \omega$, $\theta_{2,s}(\omega) = \sigma^s(\tau(\omega))\sigma^s(\omega^2) = \omega^2$, $\theta_{3,s}(\omega) = \sigma^s(\tau^3(\omega))\sigma^s(\omega^3) = \omega^3$, and $\theta_{4,s}(\omega) = \sigma^s(\tau^2(\omega))\sigma^s(\omega^4) = \omega^4$ for $s = 0, 1, 2, 3, 4$. Also $\theta_{r,s}(\xi) = \sigma^s(\theta_{r,0}(\xi)) = \sigma^s(\xi) = \omega^s\xi$ for $r = 1, 2, 3, 4$ and $s = 0, 1, 2, 3, 4$. Thus we have 20 automorphisms $\theta_{r,s}$ that are distinct, and belong to the Galois Group $\Gamma(\mathbb{Q}(\xi, \omega) : \mathbb{Q})$. But this Galois Group is of order 20. Therefore any automorphism in this Galois group must be one of the automorphisms $\theta_{r,s}$.

11. *Let f be a monic polynomial of degree n with coefficients in a field K. Then*

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f in some splitting field L for f over K. The discriminant *of the polynomial f is the quantity δ^2, where δ is the product $\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$ of the quantities $\alpha_j - \alpha_i$ taken over all pairs of integers i and j satisfying $1 \le i < j \le n$.*

Show that the quantity δ changes sign whenever α_i is interchanged with α_{i+1} for some i between 1 and $n - 1$. Hence show that $\theta(\delta) = \delta$ for all automorphisms θ in the Galois group $\Gamma(L : K)$ that induce even permutations of the roots of f, and $\theta(\delta) = -\delta$ for all automorphisms θ in $\Gamma(L : K)$ that induce odd permutations of the roots.

The quantity δ satisfies

$$(\alpha_{i+1} - \alpha_i)\rho\sigma\tau,$$

where

$$\begin{aligned}
\rho &= \prod_{\substack{1 \le j < k \le n \\ j \notin \{i, i+1\} \\ k \notin \{i, i+1\}}} (\alpha_k - \alpha_j) \\
\sigma &= \prod_{1 \le k < i} ((\alpha_i - \alpha_k)(\alpha_{i+1} - \alpha_k)) \\
\tau &= \prod_{i+1 < k \le n} ((\alpha_k - \alpha_i)(\alpha_k - \alpha_{i+1}))
\end{aligned}$$

If α_i is interchanged with α_{i+1}, where $1 \leq i < n$, then the term $\alpha_{i+1} - \alpha_i$ changes sign, but the quantities ρ, σ and τ remain unchanged. Therefore the quantity δ changes sign when i is interchanged with $i+1$. Now any permutation of $\{1, 2, \ldots, n\}$ may be expressed as a composition of transpositions, and any transposition may be expressed as a composition of transpositions that swap adjacent integers in the list $1, 2, \ldots, n$. If a permutation is even, then it can be expressed as the composition of an even number of transpositions of this form; and if the permutation is odd, then it can be expressed as a composition of an odd number of transpositions of this form. Therefore δ is unchanged under an even permutation of the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, but changes sign under an odd permutation of these roots. Thus $\theta(\delta) = \delta$ for all $\theta \in \Gamma(L\colon K)$ that induce an even permutation of $\alpha_1, \alpha_2, \ldots, \alpha_n$, $\theta(\delta) = -\delta$ for all automorphisms θ in $\Gamma(L\colon K)$ that induce odd permutations of $\alpha_1, \alpha_2, \ldots, \alpha_n$.

It follows that $\theta(\delta^2) = (\theta(\delta))^2 = \delta^2$ for all $\theta\colon \Gamma(L\colon K)$. Therefore δ^2 belongs to the fixed field of $\Gamma(L\colon K)$.

12. *Let L be a splitting field for the polynomial f over the field K, where*

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

Suppose that the field extension $L\colon K$ is separable, and is thus a Galois extension. Apply the Galois correspondence to show that the discriminant δ^2 of the polynomial f belongs to the field K containing the coefficients of f, and the field $K(\delta)$ is the fixed field of the subgroup of $\Gamma(L\colon K)$ consisting of those automorphisms in $\Gamma(L\colon K)$ that induce even permutations of the roots of f. Hence show that $\delta \in K$ if and only if all automorphisms in the Galois group $\Gamma(L\colon K)$ induce even permutations of the roots of f.

The splitting field extension $L\colon K$ is a Galois extension, because $L\colon K)$ is separable, and therefore the fixed field of $\Gamma(L\colon K)$ is the ground field K. We conclude that $\delta^2 \in K$.

Let H be the subgroup of $\Gamma(L\colon K)$ consisting of those permutations that induce even permutations of the roots of f, and let M be the fixed field of H. Then $\delta \in M$, and $K \subset M \subset L$. Now either $H = \Gamma(L\colon K)$, in which case $M = K$, or else H is a subgroup of $\Gamma(L\colon K)$ of index 2, in which case $[M\colon K] = 2$. (Indeed either all elements of $\Gamma(L\colon K)$ induce even permutations of the roots, or else half of them induce even permutations and the other half induce odd permutations.) If $H = \Gamma(L\colon K)$ then $M = K$ and $\delta \in K$, and thus $M = K(\delta)$. On the other

hand, if H is a proper subgroup of $\Gamma(L\colon K)$ then $\theta(\delta) = -\delta$ for some element θ of $\Gamma(L\colon K)$ that induces an odd permutation of the roots of f, and therefore $\delta \notin K$. But in that case $1 < [K(\delta)\colon K] \leq [M\colon K] = 2$, and therefore $K(\delta) = M$. Thus $K(\delta)$ is the fixed field of H. So we see that $\delta \in K$ if and only if $H = \Gamma(L\colon K)$, as required.

13. (a) *Show that the discriminant of the quadratic polynomial $x^2 + bx + c$ is $b^2 - 4c$.*

Let $x^2 + bx + c = (x - \alpha)(x - \beta)$. Then the discriminant is δ^2, where $\delta = (\beta - \alpha)$. Now $\alpha + \beta = -b$ and $\alpha\beta = c$. Therefore

$$\delta^2 = \alpha^2 + \beta^2 - 2\alpha\beta = (\alpha + \beta)^2 - 4\alpha\beta = b^2 - 4c.$$

(b) *Show that the discriminant of the cubic polynomial $x^3 - px - q$ is $4p^2 - 27q^2$.*

Let

$$x^3 - px - q = (x - \alpha)(x - \beta)(x - \gamma).$$

Then

$$\alpha + \beta + \gamma = 0, \quad p = -(\beta\gamma + \alpha\gamma + \alpha\beta), \quad q = \alpha\beta\gamma.$$

Moreover the discriminant is δ^2, where

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

Let us eliminate γ using the equation $\alpha + \beta + \gamma = 0$. We find that

$$\begin{aligned}
p &= \alpha^2 + \alpha\beta + \beta^2 \\
q &= -\alpha^2\beta - \alpha\beta^2 \\
\delta^2 &= (\beta - \alpha)^2(\alpha + 2\beta)^2(\beta + 2\alpha)^2 \\
&= (\alpha^2 - 2\alpha\beta + \beta^2)(2\alpha^2 + 2\beta^2 + 5\alpha\beta)^2 \\
&= (\alpha^2 - 2\alpha\beta + \beta^2)(4\alpha^4 + 20\alpha^3\beta + 33\alpha^2\beta^2 + 20\alpha\beta^3 + 4\beta^4) \\
&= 4\alpha^6 + 12\alpha^5\beta - 3\alpha^4\beta^2 - 26\alpha^3\beta^3 - 3\alpha^2\beta^4 + 12\alpha\beta^5 + 4\beta^6 \\
p^3 &= (\alpha^2 + \alpha\beta + \beta^2)(\alpha^4 + 2\alpha^3\beta + 3\alpha^2\beta^2 + 2\alpha\beta^3 + \beta^4) \\
&= \alpha^6 + 3\alpha^5\beta + 6\alpha^4\beta^2 + 7\alpha^3\beta^3 + 6\alpha^2\beta^4 + 3\alpha\beta^5 + \beta^6 \\
q^2 &= \alpha^2\beta^2(\alpha + \beta)^2 \\
&= \alpha^4\beta^2 + 2\alpha^3\beta^3 + \alpha^2\beta^4
\end{aligned}$$

Therefore

$$\delta^2 - 4p^3 = -27\alpha^4\beta^2 - 54\alpha^3\beta^3 - 27\alpha^2\beta^4 = -27q^2,$$

and thus $\delta^2 = 4p^2 - 27q^2$, as required.

14. *Let $f(x) = x^3 - px - q$ be a cubic polynomial with complex coefficients p and q without repeated roots, and let the complex numbers α, β and γ be the roots of f.*

(a) *Give formulae for the coefficients p and q of f in terms of the roots α, β and γ of f, and verify that $\alpha + \beta + \gamma = 0$ and*

$$\alpha^3 + \beta^3 + \gamma^3 = 3\alpha\beta\gamma = 3q$$

The monic polynomial f has roots α, β and γ, and therefore

$$\begin{aligned} f(x) &= (x-\alpha)(x-\beta)(x-\gamma) \\ &= x^3 - (\alpha+\beta+\gamma)x^2 + (\beta\gamma+\alpha\gamma+\alpha\beta)x - \alpha\beta\gamma \end{aligned}$$

On comparing coefficients, we see that

$$\alpha + \beta + \gamma = 0, \quad p = -(\beta\gamma + \alpha\gamma + \alpha\beta), \quad q = \alpha\beta\gamma.$$

Then

$$\begin{aligned} 0 &= (\alpha+\beta+\gamma)^3 \\ &= \alpha^3 + 3\alpha^2(\beta+\gamma) + 3\alpha(\beta^2 + 2\beta\gamma + \gamma^2) \\ &\quad + \beta^3 + 3\beta^2\gamma + 3\beta\gamma^2 + \gamma^3 \\ &= \alpha^3 + \beta^3 + \gamma^3 \\ &\quad + 3(\alpha^2(\beta+\gamma) + \beta^2(\alpha+\gamma) + \gamma^2(\alpha+\beta)) \\ &\quad + 6\alpha\beta\gamma \end{aligned}$$

But

$$\alpha^2(\beta+\gamma) + \beta^2(\alpha+\gamma) + \gamma^2(\alpha+\beta) = -(\alpha^3 + \beta^3 + \gamma^3),$$

because $\alpha + \beta + \gamma = 0$. It follows that

$$0 = -2(\alpha^3 + \beta^3 + \gamma^3) + 6\alpha\beta\gamma,$$

and therefore

$$\alpha^3 + \beta^3 + \gamma^3 = 3\alpha\beta\gamma = 3q.$$

(b) *Let $\lambda = \alpha + \omega\beta + \omega^2\gamma$ and $\mu = \alpha + \omega^2\beta + \omega\gamma$, where ω is the complex cube root of unity given by $\omega = \frac{1}{2}(-1+\sqrt{3}i)$. Verify that $1 + \omega + \omega^2 = 0$, and use this result to show that*

$$\alpha = \frac{1}{3}(\lambda + \mu), \qquad \beta = \frac{1}{3}(\omega^2\lambda + \omega\mu), \qquad \gamma = \frac{1}{3}(\omega\lambda + \omega^2\mu).$$

Calculating ω^2, we find that

$$\omega^2 = \tfrac{1}{4}\left(1 - 3 - 2\sqrt{3}i\right) = \tfrac{1}{2}\left(-1 - \sqrt{3}i\right).$$

It follows that $\omega + \omega^2 = -1$. Then

$$\begin{aligned}
\lambda + \mu &= 2\alpha + (\omega + \omega^2)(\beta + \gamma) = (2 - \omega - \omega^2)\alpha = 3\alpha, \\
\omega^2\lambda + \omega\mu &= 2\beta + (\omega + \omega^2)(\alpha + \gamma) = (2 - \omega - \omega^2)\beta = 3\beta, \\
\omega\lambda + \omega^2\mu &= 2\gamma + (\omega + \omega^2)(\alpha + \beta) = (2 - \omega - \omega^2)\gamma = 3\gamma.
\end{aligned}$$

(c) *Let K be the subfield $\mathbb{Q}(p, q)$ of $\mathbb{C}$ generated by the coefficients of the polynomial f, and let M be a splitting field for the polynomial f over $K(\omega)$. Show that the extension $M\colon K$ is normal, and is thus a Galois extension. Show that any automorphism in the Galois group $\Gamma(M\colon K)$ permutes the roots α, β and γ of f and either fixes ω or else sends ω to ω^2.*

The field M is a splitting field for the polynomial $f(x)(x^2 + x + 1)$ over the field K. It follows from a standard theorem that the extension $M\colon K$ is finite and normal. It is also separable, since the field K has characteristic zero. If $\sigma \in \Gamma(M\colon K)$ then $\sigma(p) = p$ and $\sigma(q) = q$. It follows that

$$\sigma(z^3 - pz - q) = \sigma(z)^3 - \sigma(p)\sigma(z) - \sigma(q) = \sigma(z)^3 - p\sigma(z) - q.$$

Thus σ sends any root of the polynomial $x^3 - px - q$ to another root of this polynomial. Therefore the elements of $\Gamma(M\colon K)$ permute the roots α, β and γ of the polynomial f. Similarly an element σ of $\Gamma(M\colon K)$ permutes the roots of the polynomial $x^2 + x + 1$. These roots are ω and ω^2. Therefore either $\sigma(\omega) = \omega$ or else $\sigma(\omega) = \omega^2$.

(d) *Let $\theta \in \Gamma(M\colon K)$ be a K-automorphism of M. Suppose that*

$$\theta(\alpha) = \beta, \quad \theta(\beta) = \gamma, \quad \theta(\gamma) = \alpha.$$

Show that if $\theta(\omega) = \omega$ then $\theta(\lambda) = \omega^2\lambda$ and $\theta(\mu) = \omega\mu$. Show also that if $\theta(\omega) = \omega^2$ then $\theta(\lambda) = \omega\mu$ and $\theta(\mu) = \omega^2\lambda$. Hence show that $\lambda\mu$ and $\lambda^3 + \mu^3$ are fixed by any automorphism in $\Gamma(M\colon K)$ that cyclically permutes α, β and γ. Show also that the quantities $\lambda\mu$ and $\lambda^3 + \mu^3$ are also fixed by any automorphism in $\Gamma(M\colon K)$ that interchanges two of the roots of f whilst leaving the third root fixed. Hence prove that $\lambda\mu$ and $\lambda^3 + \mu^3$ belong to the field K generated by the coefficients of f and can therefore be expressed as rational functions of p and q.

Suppose that $\theta(\omega) = \omega$. Then

$$\begin{aligned}\theta(\lambda) &= \theta(\alpha) + \omega\theta(\beta) + \omega^2\theta(\gamma) = \beta + \omega\gamma + \omega^2\alpha = \omega^2\lambda. \\ \theta(\mu) &= \theta(\alpha) + \omega^2\theta(\beta) + \omega\theta(\gamma) = \beta + \omega^2\gamma + \omega\alpha = \omega\mu.\end{aligned}$$

(Here we have used the fact that $\omega^3 = 1$.) On the other hand, if $\theta(\omega) = \omega^2$ then $\theta(\omega^2) = \omega$, and therefore

$$\begin{aligned}\theta(\lambda) &= \theta(\alpha) + \omega^2\theta(\beta) + \omega\theta(\gamma) = \beta + \omega^2\gamma + \omega\alpha = \omega\mu. \\ \theta(\mu) &= \theta(\alpha) + \omega\theta(\beta) + \omega^2\theta(\gamma) = \beta + \omega^2\gamma + \omega^2\alpha = \omega^2\lambda.\end{aligned}$$

Thus if $\theta(\omega) = \omega$ then $\theta(\lambda^3) = \lambda^3$ and $\theta(\mu^3) = \mu^3$, and therefore $\theta(\lambda^3 + \mu^3) = \lambda^3 + \mu^3$. Similarly if if $\theta(\omega) = \omega^2$ then $\theta(\lambda^3) = \mu^3$ and $\theta(\mu^3) = \lambda^3$, and therefore $\theta(\lambda^3 + \mu^3) = \lambda^3 + \mu^3$. Also if $\theta(\omega) = \omega$ then $\theta(\lambda\mu) = (\omega^2\lambda)(\omega\mu) = \lambda\mu$. Similarly if $\theta(\omega) = \omega^2$ then $\theta(\lambda\mu) = (\omega\mu)(\omega^2\lambda) = \lambda\mu$. Now any element of the Galois group $\Gamma(M\colon K)$ that cyclicly permutes the roots α, β and γ of $f(x)$ is in the cyclic subgroup generated by the automorphism θ. We conclude that any element of the Galois group $\Gamma(M\colon K)$ that cyclicly permutes the roots α, β and γ of $f(x)$ must fix the quantities $\lambda\mu$ and $\lambda^3 + \mu^3$.

Now suppose that $\Gamma(M\colon K)$ contains a K-automorphism τ_α which fixes α and interchanges β and γ. If $\tau_\alpha(\omega) = \omega$ then $\tau_\alpha(\lambda) = \mu$ and $\tau_\alpha(\mu) = \lambda$, and therefore τ_α fixes $\lambda\mu$ and $\lambda^3 + \mu^3$. Similarly if $\tau_\alpha(\omega) = \omega^2$, then $\tau_\alpha(\lambda) = \lambda$ and $\tau_\alpha(\mu) = \mu$, and therefore τ_α fixes $\lambda\mu$ and $\lambda^3 + \mu^3$.

Next suppose that $\Gamma(M\colon K)$ contains a K-automorphism τ_β which fixes β and interchanges α and γ. If $\tau_\beta(\omega) = \omega$ then $\tau_\beta(\lambda) = \omega^2\mu$ and $\tau_\beta(\mu) = \omega\lambda$, and therefore τ_β fixes $\lambda\mu$ and $\lambda^3 + \mu^3$. Similarly if $\tau_\beta(\omega) = \omega^2$, then $\tau_\beta(\lambda) = \omega\lambda$ and $\tau_\beta(\mu) = \omega^2\mu$, and therefore τ_β fixes $\lambda\mu$ and $\lambda^3 + \mu^3$.

Next suppose that $\Gamma(M\colon K)$ contains a K-automorphism τ_γ which fixes γ and interchanges α and β. If $\tau_\gamma(\omega) = \omega$ then $\tau_\gamma(\lambda) = \omega\mu$ and $\tau_\gamma(\mu) = \omega^2\lambda$, and therefore τ_γ fixes $\lambda\mu$ and $\lambda^3 + \mu^3$. Similarly if $\tau_\gamma(\omega) = \omega^2$, then $\tau_\gamma(\lambda) = \omega^2\lambda$ and $\tau_\gamma(\mu) = \omega\mu$, and therefore τ_γ fixes $\lambda\mu$ and $\lambda^3 + \mu^3$.

We have thus shown that every element of the Galois group $\Gamma(M\colon K)$ must fix the quantities $\lambda\mu$ and $\lambda^3 + \mu^3$. These quantities must therefore belong to the fixed field of the Galois group. This fixed field is the field K. Therefore $\lambda\mu \in K$ and $\lambda^3 + \mu^3 \in K$. These quantities must therefore be expressible in terms of the formulae constructed out of rational numbers and the quantities p and q using only the operations of addition, subtraction, multiplication and division.

(e) *Show by direct calculation that* $\lambda\mu = 3p$ *and* $\lambda^3 + \mu^3 = 27q$. *Hence show that* λ^3 *and* μ^3 *are roots of the quadratic polynomial* $x^2 - 27qx + 27p^3$. *Use this result to verify that the roots of the cubic polynomial* $x^3 - px - q$ *are of the form*

$$\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}$$

where the two cube roots must be chosen so as to ensure that their product is equal to $\frac{1}{3}p$.

By direct calculation, using the identity $\omega^3 = 1$, we see that

$$\begin{aligned} \lambda\mu &= \alpha^2 + \beta^2 + \gamma^2 + (\omega + \omega^2)(\alpha\beta + \alpha\gamma + \beta\gamma) \\ &= (\alpha + \beta + \gamma)^2 + (\omega + \omega^2 - 2)(\alpha\beta + \alpha\gamma + \beta\gamma). \end{aligned}$$

But $\alpha + \beta + \gamma = 0$ and $\omega^2 + \omega + 1 = 0$. Therefore

$$\lambda\mu = -3(\alpha\beta + \alpha\gamma + \beta\gamma) = 3p.$$

Also

$$\begin{aligned} \lambda^3 &= \alpha^3 + \beta^3 + \gamma^3 \\ &\quad + 3\alpha^2(\omega\beta + \omega^2\gamma) + 3\beta^2(\omega^2\alpha + \omega\gamma) + 3\gamma^2(\omega\alpha + \omega^2\beta) \\ &\quad + 6\alpha\beta\gamma, \\ \mu^3 &= \alpha^3 + \beta^3 + \gamma^3 \\ &\quad + 3\alpha^2(\omega^2\beta + \omega\gamma) + 3\beta^2(\omega\alpha + \omega^2\gamma) + 3\gamma^2(\omega^2\alpha + \omega\beta) \\ &\quad + 6\alpha\beta\gamma. \end{aligned}$$

It follows that

$$\begin{aligned} \lambda^3 + \mu^2 &= 2\alpha^3 + \beta^3 + \gamma^3 \\ &\quad + 3(\omega + \omega^2)(\alpha^2(\beta + \gamma) + \beta^2(\alpha + \gamma) + \gamma^2(\alpha + \beta)) \\ &\quad + 12\alpha\beta\gamma, \end{aligned}$$

It follows that

$$\begin{aligned} \lambda^3 + \mu^2 &= (2 - 3\omega - 3\omega^2)(\alpha^3 + \beta^3 + \gamma^3) + 12\alpha\beta\gamma \\ &= 5(\alpha^3 + \beta^3 + \gamma^3) + 12\alpha\beta\gamma. \end{aligned}$$

Also $\alpha^3 + \beta^3 + \gamma^3 = 3\alpha\beta\gamma = 3q$. Therefore $\lambda^3 + \mu^3 = 27q$. Now λ^3 and μ^3 are the roots of the quadratic polynomial $g(x)$, where

$$g(x) = (x - \lambda^3)(x - \mu^3) = x^2 - 27qx + 27p^3.$$

Now the roots of this quadratic polynomial are $r_\pm$, where

$$r_\pm = 27\left(\frac{q}{2} \pm \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}\right).$$

One of these roots is λ^3, and the other is μ^3. The formula for the roots of the cubic polynomial are then given in terms of λ and μ by the formulae

$$\alpha = \frac{1}{3}(\lambda + \mu), \qquad \beta = \frac{1}{3}(\omega^2\lambda + \omega\mu), \qquad \gamma = \frac{1}{3}(\omega\lambda + \omega^2\mu).$$