1. Let $K/F$ be a degree 2 extension of fields.

   (a) If the characteristic of $F$ is not 2, prove that $K = F(a)$ for some $a \in K \setminus F$ with $a^2 \in F$.

   (b) Give a counterexample to (1a) if $F$ has characteristic 2.

   (c) Fix $F$ of characteristic not 2 and let $K_1, K_2$ be quadratic extensions of $F$ with $K_1 = F(a_1)$ and $K_2 = F(a_2)$ where $a_i^2 = b_i \in F$. Prove that $K_1 \simeq K_2$ as extensions of $F$ (i.e. that there exists an isomorphism of fields $K_1 \simeq K_2$ restricting to the identity on $F$) if and only if $b_1/b_2 \in (F^\times)^2$ is a square. Conclude that the isomorphism classes of quadratic extensions of $F$ are in bijection with the group $F^\times/(F^\times)^2$.

   (d) Using (1c), give a complete list (without repetition) of all isomorphism classes of quadratic extensions of $Q$.

Solution:

   (a) Fix $b \in K \setminus F$. Then $\{1, b\}$ is an $F$-basis of $K$, so $b$ satisfies a degree 2 polynomial $b^2 + ub + v = 0$ with $u, v \in F$. Since the characteristic of $F$ is not 2, $2 \in F^\times$ so $u/2$ makes sense and we have $(b + u/2)^2 = u^2/4 - v$ by completing the square. Thus, $a := b + u/2 \in K \setminus F$ has $a^2 \in F$ and clearly $K = F(a)$.

   (b) The extension $F_2[X]/(X^2 + X + 1)$ of $F_2$ gives a counterexample, since $(a + bX)^2 = (a^2 + b^2) + b^2X$ lies in $F$ if and only if $b = 0$.

   (c) If $K_1 \simeq K_2$ as extensions of $F$, then $b_1$ must be a square in $K_2$, say $b_1 = (u + va_2)^2$. This gives $b_1 = u^2 + v^2b_2 + 2uvb_2$ from which it follows (as $2 \neq 0$ in $F$) that either $u$ or $v$ must be zero. The second case cannot occur as otherwise $b_1$ would be a square in $F$ and $K_1 = F$. Thus, $b_1 = v^2b_2$ for some $v \in F$. Conversely, If $b_1 = v^2b_2$ then $b_1 = (va_2)^2$ is a square in $K_2$, and the map $F[X] \to K_2$ sending $X$ to $va_2$ is surjective and yields an isomorphism $F[X]/(X^2 - b_1) \simeq K_2$. As the source of this isomorphism is isomorphic to $K_1$, we get $K_1 \simeq K_2$ as extensions of $F$.

   (d) These are parameterized by $Q^\times/(Q^\times)^2 = \{2, 3, 5, 6, 7, 10, 11, 13, 14, 15, \ldots \}$ (the positive square-free integers).

2. For $a \in F_p$, set $f_a(x) := X^p - X - a \in F_p[X]$.

   (a) If $a = 0$, show that $f_a(X) = \prod_{u \in F_p} (X - u)$.

   (b) Suppose that $a \neq 0$ and let $E_a$ be a splitting field of $f_a(X)$. If $r_1, r_2 \in E_a$ are roots of $f_a$, prove that $r_1 - r_2 \in F_p$.

   (c) Show that $f_a(X)$ is irreducible for all $a \in F_p^\times$.

   (d) Prove that $f_b(X)$ splits completely over $E_a$ for each fixed $a \in F_p^\times$ and all $b \in F_p^\times$. Conclude that $E_a$ is independent of $a$.

Solution:
(a) Every $u \in \mathbb{F}_p$ satisfies $X^p - X = 0$ and this gives $p$ roots of the degree $p$ polynomial $X^p - X$ in the Euclidean domain $F[X]$, so we get the claimed factorization.

(b) Observe that $(r_1 - r_2)^p - (r_1 - r_2) = (r_1^p - r_1) - (r_2^p - r_2) = 0$ so $r_1 - r_2$ is a root of $X^p - X$ and hence an element of $\mathbb{F}_p$ by the first part.

(c) Certainly $f_a$ has no root in $\mathbb{F}_p$ for $a \in \mathbb{F}_p^\times$, by part 1. Over $E_a$, we have the factorization

$$f_a = \prod_{0 \leq i < p} (X - (r + i))$$

for a fixed root $b$ of $f_a$ in $E_a$ (by the previous part). If $f_a = gh$ in $\mathbb{F}_p[X]$ then $g = X^d + \alpha X^{d-1}$ for some $0 < d < p$. But $g$ is a product over certain integers $i$ of $(X - (r + i))$ in $E_a[X]$ so we must have $-\alpha = dr + u$ for some $u \in \mathbb{F}_p$. As $d \in \mathbb{F}_p^\times$, this gives $r \in \mathbb{F}_p$ (as $\alpha \in \mathbb{F}_p$), a contradiction as $f_a$ has no roots in $\mathbb{F}_p$. Hence $f_a$ is irreducible.

(d) If $r$ is any root of $f_a$ in $E_a$, then $(vr)^p - (vr) + va = 0$ for any $v \in \mathbb{F}_p^\times$. Thus, the roots of $f_{va}$ are precisely $vr, vr + 1, \ldots, vr + p - 1 \in E_a$ so $f_{va}$ splits completely over $E_a$. This shows that $E_a$ contains $E_{va}$ for all $a \in \mathbb{F}_p^\times$ and hence that $E_a$ is independent of $a$.

3. Find the minimal polynomials of $2 \cos(2\pi/5)$ and $2 \cos(2\pi/7)$ over $\mathbb{Q}$.

**Solution** We treat the case of $2 \cos(2\pi/7)$ as it is the harder of the two. Let $\zeta = e^{2\pi i/7}$ and set $K = \mathbb{Q}(\zeta)$, $G = \text{Gal}(K/\mathbb{Q})$. Put $\eta := \zeta + \zeta^{-1} = 2 \cos(2\pi/7)$. We know that $G \simeq (\mathbb{Z}/7\mathbb{Z})^\times$ is cyclic of order 6, generated by the automorphism $\sigma : \zeta \mapsto \zeta^3$ (since $3 \in (\mathbb{Z}/7\mathbb{Z})^\times$ is a generator of this cyclic group). The conjugates of $\eta$ are

$$\eta, \quad \sigma \eta = \zeta^3 + \zeta^{-3}, \quad \sigma^2 \eta = \zeta^2 + \zeta^{-2}.$$

Using the binomial theorem, we compute

$$\sigma^2 \eta = \eta^2 - 2, \quad \sigma \eta = \eta^3 - 3\eta$$

and hence we find that

$$\eta + \sigma \eta + \sigma^2 \eta = \eta^3 + \eta^2 - 2\eta - 2.$$

Using the fact that the minimal polynomial of $\zeta$ is $X^6 + X^5 + \cdots + X + 1$, the left hand side above is $-1$ whence $\eta$ is a root of the degree 3 polynomial

$$X^3 + X^2 - 2X - 1$$

which must therefore be the minimal polynomial of $\eta$ since $\eta$ has 3 distinct conjugates.

4. For each of the following extensions, determine $[K : F]$ and an $F$-basis of $K$.

(a) $F = \mathbb{Q}$, $L = \mathbb{Q}(a, b)$ with $a^2 = 6$ and $b^3 = 2$.

(b) $F = \mathbb{C}(T)$ and $L$ is the splitting field of $X^n - T$ over $F$, with $n$ a positive integer.

(c) $F = \mathbb{F}_p(T)$ and $L$ is the splitting field of $X^p - T$ over $F$, with $p$ a prime.

**Solution:**

(a) An $F$-basis is $\{1, b, b^2, a, ab, ab^2\}$

(b) $L$ is the splitting field of $X^n - T$ over $F$, with $n$ a positive integer.

(c) $L$ is the splitting field of $X^p - T$ over $F$, with $p$ a prime.
Let \( r \) be a root of \( X^n - T \) in \( L \). An \( F \)-basis is \( \{1, r, r^2, \ldots, r^{n-1}\} \) (note that this polynomial is irreducible by Eisenstein’s criterion, so \( F(r) \) is a degree \( n \) extension and since \( C \) contains all \( n \)-th roots of unity, \( X^n - T \) splits completely over \( F(r) \)).

Again, Eisenstein’s criterion gives irreducibility. If \( r \) the unique(!) root of \( X^p - T \) in \( L \), then an \( F \)-basis of \( L \) is \( 1, r, r^2, \ldots, r^{p-1} \).

5. Let \( K/F \) be a finite extension of fields and let \( \alpha \in K \). Then \( \alpha \) induces an \( F \)-linear map of finite-dimensional \( F \)-vector spaces
\[
m_{\alpha} : K \to K.
\]

(a) Prove that \( \alpha \) is a root of the characteristic polynomial of the linear map \( m_{\alpha} \). Hint: select a suitable \( F \)-basis of \( F(\alpha) \).

(b) Use (5a) to find a monic degree 3 polynomial with \( \mathbb{Q} \)-coefficients satisfied by \( 1 + \sqrt[3]{2} + \sqrt[3]{4} \).

(c) Prove that if \( K = F(\alpha) \), then the characteristic polynomial of \( m_{\alpha} \) as a linear map \( K \to K \) is in fact the minimal polynomial of \( \alpha \) over \( F \).

Solution:

(a) Let \( m(x) := x^d + a_{d-1}x^{d-1} + \cdots + a_0 \) be the minimal polynomial of \( \alpha \) over \( F \). Then \( 1, \alpha, \ldots, \alpha^{d-1} \) is an \( F \)-basis of \( F(\alpha) \). Let \( \{b_1, \ldots, b_e\} \) be an \( F(\alpha) \)-basis of \( K \) so \( \{\alpha^i b_j\} \) is an \( F \)-basis of \( K \). Then the matrix of multiplication by \( \alpha \) on \( K \) with respect to this basis is a block diagonal matrix, with blocks given by the matrix of multiplication by \( \alpha \) on \( F(\alpha) \), which is easily seen to be
\[
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & 0 \\
-a_0 & -a_1 & -a_2 & \cdots & -a_{d-1}
\end{pmatrix}
\]
This matrix has characteristic polynomial \( m(x) \) so the characteristic polynomial of \( m_{\alpha} \) is a power of \( m(x) \). This also handles part c).

(b) Let \( \alpha = \sqrt[3]{2} \) and \( \beta := 1 + \alpha + \alpha^2 \). The matrix of multiplication by \( \beta \) on \( \mathbb{Q}(\alpha) \) with respect to the basis \( 1, \alpha, \alpha^2 \) is
\[
\begin{pmatrix}
1 & 1 & 1 \\
2 & 1 & 1 \\
2 & 2 & 1
\end{pmatrix}
\]
and this has characteristic polynomial \( X^3 - 3X^2 - 3X - 1 \).

6. For each of the following algebraic elements \( \alpha \) of the given field extension \( K/\mathbb{Q} \), express \( 1/\alpha \) and \( 1/(\alpha + 1) \) as polynomials in \( \alpha \) with \( \mathbb{Q} \)-coefficients.

(a) \( K \) is the splitting field of \( f = X^3 - 3X + 1 \) and \( \alpha \) is a root of \( f \).

(b) \( K \) is the splitting field of \( f = X^4 + X^3 + X^2 + X + 1 \) and \( \alpha \) is a root of \( f \).

(c) \( K \) is the splitting field of \( f = X^5 - 3X + 3 \) and \( \alpha \) is a root of \( f \).

Solution:
(a) \(1/\alpha = 3 - \alpha^2\) and \(1/(\alpha + 1) = \frac{1}{3}(-\alpha^2 + \alpha + 2)\).
(b) \(1/\alpha = -a^3 - a^2 - a - 1\) and \(1/(\alpha + 1) = -a^3 - a\)
(c) \(1/\alpha = \frac{1}{3}(-\alpha^4 + 3)\) and \(1/(\alpha + 1) = \frac{1}{5}(-\alpha^4 + a^3 - a^2 + a + 2)\)

7. Prove that \(X^4 - 5\) is irreducible over \(\mathbb{Q}\) and has splitting field \(K\) of degree 8 over \(\mathbb{Q}\). Describe this splitting field explicitly as \(\mathbb{Q}(\alpha, b)\) where \(\alpha\) is a root of \(X^4 - 5\) and \(b^2 \in \mathbb{Q}\). In terms of \(\alpha\) and \(b\), write down a \(\mathbb{Q}\)-basis for \(K\).

**Solution:** Use Eisenstein with \(p = 5\). The splitting field is easily seen to be \(\mathbb{Q}(\alpha, b)\) where \(\alpha := \sqrt[4]{5}\) and \(b := i\), which has degree 8 since \(i\) is not in \(\mathbb{Q}(\alpha)\) as \(\mathbb{Q}(\alpha)\) is a subfield of \(\mathbb{R}\). A \(\mathbb{Q}\)-basis for \(K\) is \(\{1, \alpha, \alpha^2, \alpha^3, b, ba, ba^2, ba^3\}\).

8. Describe the splitting fields of \(f := X^3 - 5\) over \(\mathbb{F}_{11}\) and \(\mathbb{F}_7\) and factor \(f\) into linear factors over each extension.

**Solution:** Over \(\mathbb{F}_{11}\), the given polynomial has a root \(X = 3\) and factors as \((X - 3)(X^2 + 3X - 2)\) with irreducible quadratic. The splitting field is therefore degree 2, and is obtained by adjoining the square root of any nonsquare in \(\mathbb{F}_{11}\). Explicitly, the splitting field is \(\mathbb{F}_{11}(\alpha)\) where \(a^2 = -1\) and then \(X^3 - 5\) factors over \(\mathbb{F}_{11}(\alpha)\) as

\[X^3 - 5 = (X - 3)(X + 2a - 4)(X - 2a - 4)\]

The case of \(\mathbb{F}_7\) is similar and is left to the reader.