1. (15 points) Prove or disprove $\mathbb{Q}(\sqrt{3} + i) = \mathbb{Q}(\sqrt{3}, i)$. Here $i = \sqrt{-1}$ and $\mathbb{Q}$ denotes the field of rationals.

**Answer:** The set $\mathbb{Q}(\sqrt{3}, i)$ is given by

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

$$= \left\{ p(\sqrt{3}) \mid p(x) \in \mathbb{Q}(i)[x] \right\}$$

$$= \left\{ \sum_{k=0}^{n} a_k (\sqrt{3})^k \mid a_k \in \mathbb{Q}(i) \right\}$$

$$= \left\{ A_1 + A_2 \sqrt{3} \mid A_1, A_2 \in \mathbb{Q}(i) \right\}$$

$$= \left\{ a + b i + c \sqrt{3} + d i \sqrt{3} \mid a, b, c, d \in \mathbb{Q} \right\}$$

Similarly, we get

$$\mathbb{Q}(\sqrt{3} + i) = \left\{ p(\sqrt{3} + i) \mid p(x) \in \mathbb{Q}[x] \right\}$$

$$= \left\{ \sum_{k=0}^{n} a_k (\sqrt{3} + i)^k \mid a_k \in \mathbb{Q} \right\}$$

$$= \left\{ a + \beta i + \gamma \sqrt{3} + \delta i \sqrt{3} \mid a, \beta, \gamma, \delta \in \mathbb{Q} \right\}$$

Hence $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3} + i)$.

2. (15 points) Find the splitting fields of the following polynomials in $\mathbb{Q}[x]$:

(a) $f(x) = x^4 - 9$,

**Answer:** Since $f(x) = x^4 - 9$ can be factored as

$$f(x) = (x - \sqrt{3})(x + \sqrt{3})(x - i \sqrt{3})(x + i \sqrt{3}),$$
the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{3}, i)$.

(b) $f(x) = x^4 - 10x^2 + 1$,  
**Answer:** Since $f(x) = x^4 - 10x^2 + 1$ can be factored as  
\[ f(x) = (x - \sqrt{3} - \sqrt{2})(x - \sqrt{3} + \sqrt{2})(x + \sqrt{3} - \sqrt{2})(x + \sqrt{3} + \sqrt{2}), \]
the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{3}, \sqrt{2})$.

(c) $f(x) = x^2 + 2x + 2$,  
**Answer:** Since $f(x) = x^2 + 2x + 2$ can be factored as  
\[ f(x) = (x + i - 1)(x - i + 1), \]
the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$.

(d) $f(x) = x^5 - 1$  
**Answer:** Since $f(x) = x^5 - 1$ can be factored as  
\[ f(x) = (x - w^0)(x - w)(x - w^2)(x - w^3)(x - w^4) \]
where $w = e^{\frac{2\pi i}{5}}$ (the 5th root of unity), the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(w)$.

3. (15 points) Find the basis for each of the given vector spaces over the given field. What is the degree of each field extension?

(a) $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$  
**Answer:** The basis of the vector space $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$. The degree of extension of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, that is $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

(b) $\mathbb{Q}(i\sqrt{3})$ over $\mathbb{Q}$  
**Answer:** The basis of the vector space $\mathbb{Q}(i\sqrt{3})$ over $\mathbb{Q}$ is $\{1, i\sqrt{3}\}$. The degree of extension of $\mathbb{Q}(i\sqrt{3})$ over $\mathbb{Q}$, that is $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$.

(c) $\mathbb{Q}(\sqrt{3}, i)$ over $\mathbb{Q}$  
**Answer:** The basis of the vector space $\mathbb{Q}(\sqrt{3}, i)$ over $\mathbb{Q}$ is $\{1, i, \sqrt{3}, i\sqrt{3}\}$. The degree of extension of $\mathbb{Q}(\sqrt{3}, i)$ over $\mathbb{Q}$, that is $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$. 


(d) \(Q(\sqrt{3} + i)\) over \(Q(\sqrt{3})\)

**Answer:** Recall that \(Q(\sqrt{3} + i) = Q(\sqrt{3}, i)\). The basis of the vector space \(Q(\sqrt{3} + i)\) over \(Q(\sqrt{3})\) is \(\{1, i\}\). The degree of extension of \(Q(\sqrt{3} + i)\) over \(Q(\sqrt{3})\), that is \([Q(\sqrt{3} + i) : Q(\sqrt{3})] = 2\).

(c) \(Q(\pi)\) over \(Q(\pi^2)\)

**Answer:** Since \(\pi\) is transcendental over \(Q\), then \(\pi^2\) is also transcendental over \(Q\). Therefore \(Q(\pi) \simeq Q(\pi^2) \simeq Q(x)\). Moreover, since \(Q(\pi^2) \subseteq Q(\pi)\), therefore \(Q(\pi^2) = Q(\pi)\). Hence, the basis of the vector space \(Q(\pi)\) over \(Q(\pi^2)\) is \(\{1\}\). The degree of extension of \(Q(\pi)\) over \(Q(\pi^2)\), that is \([Q(\pi) : Q(\pi^2)] = 1\).

4. (15 points) Which of the following polynomials are irreducible in \(Q[x]\) (You must justify your answer to receive full credit):

(a) \(f(x) = x^3 + 4x^2 - 3x + 5\)

**Answer:** We will use the irreducibility test mod 2. Since \(f(x) = x^4 + 4x^2 - 3x + 5\), we get \(\tilde{f}(x) = x^3 + x + 1\) in \(Z_2[x]\). Moreover, since \(\tilde{f}(0) = 1 = \tilde{f}(1)\) and \(\text{deg}(\tilde{f}(x)) = 3\), the polynomial \(\tilde{f}(x)\) is irreducible in \(Z_2[x]\) and therefore \(f(x)\) is irreducible in \(Q[x]\).

(b) \(f(x) = 4x^4 - 6x^2 + 6x - 12\)

**Answer:** Take \(p = 3\) and apply Eisenstein’s test to conclude \(f(x)\) is irreducible in \(Q[x]\).

(c) \(f(x) = x^5 + x^3 + x^2 + 1\)

**Answer:** Since \(f(x) = x^5 + x^3 + x^2 + 1 = (x^2 + 1)(x^3 + 1)\), the polynomial \(f(x)\) is not irreducible in \(Q[x]\).

(d) \(f(x) = x^4 + 2x^3 - 6x^2 + 7x - 13\)

**Answer:** We will use the irreducibility test mod 2. Since \(f(x) = x^4 + 2x^3 - 6x^2 + 7x - 13\), we get \(\tilde{f}(x) = x^4 + x + 1\) in \(Z_2[x]\). Moreover, since \(\tilde{f}(0) = 1 = \tilde{f}(1)\) so \(\tilde{f}(x)\) has no linear factor. Since \(\tilde{f}(x)\) has no linear factor, therefore the possible quadratic factors are: \(x^2 + x + 1\) and \(x^2 + 1\). But \(x^4 + x + 1 \neq (x^2 + x + 1)(x^2 + x + 1)\) or \(x^4 + x + 1 \neq (x^2 + x + 1)(x^2 + 1)\) or \(x^4 + x + 1 \neq (x^2 + 1)(x^2 + 1)\). Hence the polynomial \(\tilde{f}(x)\) is irreducible in \(Z_2[x]\) and therefore \(f(x)\) is irreducible in \(Q[x]\).
5. (15 points) Draw the subfield lattice of $GF(3^{18})$ and of $GF(3^{30})$. Make sure that your lattice diagram is eye-pleasing.

**Answer:** The subfield lattice of $GF(3^{18})$ and of $GF(3^{30})$ are shown below.

![Subfield Lattice Diagrams](image)

6. (15 points) Suppose $F$ is an arbitrary field and let $F^3 = \{(a, b, c) \mid a, b, c \in F\}$. Prove that $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$ is a basis of the vector space $F^3$ over $F$ provided the characteristic of $F$ is not 2. When the characteristic of $F$ is 2, show that the set is not a basis.

**Answer:** Suppose $\text{char}(F) \neq 2$. Let $B = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$. We want to show that $B$ is a basis of the vector space $F^3$ over $F$. Suppose there exist $a, b, c \in F$ such that

$$a (1, 1, 0) + b (1, 0, 1) + c (0, 1, 1) = (0, 0, 0).$$

From the last equation, we get $(a + b, a + c, b + c) = (0, 0, 0)$. Solving this, we have $a = b = c$ and $2a = 0$. Since characteristic of $F$ is not 2, therefore $2a = 0$ yields $a = 0$ and hence we have $a = b = c = 0$. Thus we see that $B$ consists of a set of linearly independent vectors.
Let \((\alpha, \beta, \gamma) \in \mathbb{F}^3\). Then we can find constants \(a, b, c \in \mathbb{F}\) such that
\[a(1,1,0) + b(1,0,1) + c(0,1,1) = (\alpha, \beta, \gamma).\]

Writing the above in matrix notation, we have
\[
\begin{pmatrix}
1 & 1 & 0 \\
1 & 0 & 1 \\
0 & 1 & 1
\end{pmatrix}
\begin{pmatrix}
a \\
b \\
c
\end{pmatrix}
= \begin{pmatrix}
\alpha \\
\beta \\
\gamma
\end{pmatrix}.
\]

The determinant of the above 3 \(\times\) 3 matrix is nonzero, therefore it is invertible and we have
\[
\begin{pmatrix}
a \\
b \\
c
\end{pmatrix}
= 2^{-1}
\begin{pmatrix}
1 & 1 & -1 \\
1 & -1 & 1 \\
-1 & 1 & 1
\end{pmatrix}
\begin{pmatrix}
\alpha \\
\beta \\
\gamma
\end{pmatrix}.
\]

Hence any arbitrary vector \((\alpha, \beta, \gamma) \in \mathbb{F}^3\) can be uniquely represented as a linear combination of vectors in \(B\).

Hence \(B\) is a basis of the vector space \(\mathbb{F}^3\) over \(\mathbb{F}\).

If \(\text{char}(\mathbb{F}) = 2\), then \((1,1,0) + (1,0,1) = (0,1,1)\). Therefore the vectors in \(B\) are not linearly independent.

7. (15 points) Given that \(a\) belongs to some field extension of \(\mathbb{Q}\) and that \([\mathbb{Q}(a) : \mathbb{Q}] = 5\), prove that \(\mathbb{Q}(a^3) = \mathbb{Q}(a)\).

**Answer:** It is easy to see that \(\mathbb{Q} \subseteq \mathbb{Q}(a^3) \subseteq \mathbb{Q}(a)\). Hence we have
\[\left[\mathbb{Q}(a) : \mathbb{Q}\right] = \left[\mathbb{Q}(a) : \mathbb{Q}(a^3)\right]\left[\mathbb{Q}(a^3) : \mathbb{Q}\right] = 5.\]
The last equality implies that either \([\mathbb{Q}(a) : \mathbb{Q}(a^3)] = 1\) or \([\mathbb{Q}(a^3) : \mathbb{Q}] = 1\). If the first case is true, we are done, so let us assume that \([\mathbb{Q}(a^3) : \mathbb{Q}] = 1\) that is, \(\mathbb{Q} = \mathbb{Q}(a^3)\). Then, \(a^3 \in \mathbb{Q}\) and \(p(x) = x^3 - a^3 \in \mathbb{Q}[x]\) is such that \(p(a) = 0\). But this implies that \([\mathbb{Q}(a) : \mathbb{Q}] \leq 3\) which is a contradiction to the fact that \([\mathbb{Q}(a) : \mathbb{Q}] = 5\). Therefore, \(\mathbb{Q}(a^3) = \mathbb{Q}(a)\).

8. (15 points) Find a polynomial \(p(x)\) in \(\mathbb{Q}[x]\) so that \(\mathbb{Q}\left(\sqrt{1 + 2\sqrt{2}i}\right)\) is isomorphic to \(\mathbb{Q}[x]/\langle p(x) \rangle\).

**Answer:** Let \(x = \sqrt{1 + 2\sqrt{2}i}\). Then squaring both sides, we get \(x^2 = 1 + 2\sqrt{2}i\). Hence \(x^2 - 1 = 2\sqrt{2}i\). Again squaring both sides of the last equation, we have \(x^4 - 2x^2 + 9 = 0\). Therefore \(p(x) = x^4 - 2x^2 + 9 \in \mathbb{Q}[x]\) satisfies \(p\left(\sqrt{1 + 2\sqrt{2}i}\right) = 0\). It is easy to check that \(p(x) = x^4 - 2x^2 + 9\) is irreducible in \(\mathbb{Q}[x]\).
9. (15 points) Suppose that \( p(x) \) is irreducible over \( \mathbb{F} \) and \( a \) and \( a^2 \) are elements of some extension field of \( \mathbb{F} \) and both are zeros of \( p(x) \). Prove that \( \mathbb{F}(a) = \mathbb{F}(a^2) \).

**Answer:** Since \( a^2 \in \mathbb{F}(a) \) we have that \( \mathbb{F}(a^2) \subseteq \mathbb{F}(a) \). By the Corollary to Theorem 20.3, we obtain \( \mathbb{F}(a) \cong \mathbb{F}(a^2) \) as fields and therefore as vector spaces over \( \mathbb{F} \). Thus \( [\mathbb{F}(a) : \mathbb{F}] = [\mathbb{F}(a^2) : \mathbb{F}] \).

From
\[
[\mathbb{F}(a) : \mathbb{F}] = [\mathbb{F}(a) : \mathbb{F}(a^2)] [\mathbb{F}(a^2) : \mathbb{F}]
\]
we see that \( [\mathbb{F}(a) : \mathbb{F}(a^2)] = 1 \). Hence we have \( \mathbb{F}(a) = \mathbb{F}(a^2) \).

10. (15 points) Construct a field of order 9 and carry out the analysis done in Example 1 (on page 383), including the conversion table.

**Answer:** The polynomial \( p(x) = x^9 - x \) has 9 distinct roots since \( p(x) = x^9 - x \) and \( p'(x) = -1 \) have no common factors of positive degree. The finite field \( \mathbb{GF}(3^2) \) consists of these nine roots of the polynomial \( p(x) \).

The polynomial \( p(x) = x^9 - x \) is not irreducible in \( \mathbb{Z}_3[x] \). In fact using maple command \( \text{"Factor}(x^9 - x) \mod 3;" \) we see that
\[
p(x) = x (x + 1) (x + 2) (x^2 + 1) (x^2 + x + 2) (x^2 + 2x + 2).
\]
We can check using maple command \( \text{"Irreduc}(x^2+2x+2) \mod 3;" \) that the factor \( x^2+2x+2 \) is irreducible in \( \mathbb{Z}_3[x] \). Similarly the factors \( x^2+1 \) and \( x^2+x+2 \) can be verified to be irreducible in \( \mathbb{Z}_3[x] \). Each of the irreducible factor gives rise to a finite field with \( 3^2 \) elements. Hence we have the following additional finite fields \( \mathbb{Z}_3[x]/ < x^2 + 1 >, \mathbb{Z}_3[x]/ < x^2 + x + 2 > \) and \( \mathbb{Z}_3[x]/ < x^2 + 2x + 2 > \). However each one is isomorphic to \( GF(3^2) \).

Not that \( GF(3^2) \cong \mathbb{Z}_3[x]/ < x^2 + 1 > \) but \( x \) is not a generator of \( GF(3^2)^\# \). So we use \( GF(3^2) \cong \mathbb{Z}_3[x]/ < x^2 + x + 2 > \). This time \( x \) is a generator of \( GF(3^2)^\# \). The conversion table is the given below:

<table>
<thead>
<tr>
<th>Multiplicative</th>
<th>Additive</th>
<th>Additive</th>
<th>Multiplicative</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( x )</td>
<td>( x )</td>
<td>( 2 )</td>
<td>( x^4 )</td>
</tr>
<tr>
<td>( x^2 )</td>
<td>( 2x+1 )</td>
<td>( x )</td>
<td>( x )</td>
</tr>
<tr>
<td>( x^3 )</td>
<td>( 2x+2 )</td>
<td>( x+1 )</td>
<td>( x^7 )</td>
</tr>
<tr>
<td>( x^4 )</td>
<td>( 2 )</td>
<td>( x+2 )</td>
<td>( x^6 )</td>
</tr>
<tr>
<td>( x^5 )</td>
<td>( 2x )</td>
<td>( 2x )</td>
<td>( x^5 )</td>
</tr>
<tr>
<td>( x^6 )</td>
<td>( x+2 )</td>
<td>( 2x+1 )</td>
<td>( x^2 )</td>
</tr>
<tr>
<td>( x^7 )</td>
<td>( x+1 )</td>
<td>( 2x+2 )</td>
<td>( x^3 )</td>
</tr>
</tbody>
</table>
**Bonus Problem. (15 points)** (a) Let $\beta$ be a zero of $x^3 + x + 1$ in some extension field of $\mathbb{Z}_2$. Show that $\beta + 1$ is a zero of $x^3 + x^2 + 1$.

**Answer:** Since $\beta$ is a zero of $x^3 + x + 1$, therefore $\beta^3 + \beta + 1 = 0$. We show that $\beta + 1$ is zero of $p(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$. Since

$$p(\beta + 1) = (\beta + 1)^3 + (\beta + 1)^2 + 1$$
$$= \beta^3 + \beta^2 + \beta + 1 + \beta^2 + 1 + 1$$
$$= \beta^3 + \beta + 1$$
$$= 0,$$

therefore $\beta + 1$ is a zero of $x^3 + x^2 + 1$.

(b) Let $K$ be a splitting field of $x^2 + 2x + 2$ over $\mathbb{Z}_3$. Determine order of $K$ (that is, the number of elements in $K$).

**Answer:** Since $f(x) = x^2 + 2x + 2 = (x + 1 - i)(x + 1 + i)$. Hence $K = \mathbb{Z}_3(i)$. Since $\mathbb{Z}_3(i) = \{a + bi \mid a, b \in \mathbb{Z}_3\}$, therefore $|K| = 9$.

(c) Let $p$ be a any prime number. Write $x^p - x$ as a product of linear factors over $\mathbb{Z}_p$.

**Answer:** Since by Fermat’s Little theorem, we have $a^{p-1} - 1 \equiv 0 \mod p$ for $\gcd(a, p) = 1$, therefore $a^p - a = 0 \mod p$. Hence every element $a \in \mathbb{Z}_p$ is a root of the polynomial $x^p - x$. Therefore $x^p - x = x(x - 1)(x - 2)(x - 3)\cdots(x - (p - 1))$. 