Note: A random subset of these problems will be graded for credit.

(1) Recall that for an extension field $E$ of a field $F$, an element $a \in E$ is algebraic over $F$ if it is a root of some polynomial $f(x) \in F[X]$. Furthermore, the degree of an element $a \in E$ that is algebraic over $F$ is the degree of a polynomial of minimal degree such that $a$ is a root of the polynomial.

(a) Show $\sqrt{2} + \sqrt{3}$ algebraic over $\mathbb{Q}$. Find its degree over $\mathbb{Q}$. Prove your answer.

Proof: Consider that $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$ and hence
$$6 = (\sqrt{6})^2 = (0.5[(\sqrt{2} + \sqrt{3})^2 - 5])^2.$$Thus for $\alpha = \sqrt{2} + \sqrt{3}$ we get that $6 = (1/4)(\alpha^2 - 5)^2$ or equivalently,
$$24 = \alpha^4 - 10\alpha^2 + 25.$$So for
$$f(x) = x^4 - 10x^2 + 1,$$it follows that $f(\sqrt{2} + \sqrt{3}) = 0$. So $\sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$ of degree at most 4. Now let’s show the degree is 4. We do this by showing that $\sqrt{2} + \sqrt{3}$ is not the root of lower degree non-constant polynomial in $\mathbb{Q}[X]$.

Suppose $\sqrt{2} + \sqrt{3}$ is a root of a lower degree non-constant polynomial in $\mathbb{Q}[X]$. Let $g(x) \in \mathbb{Q}[X]$ be of minimal degree between 1 and 3 such that $g(\sqrt{2} + \sqrt{3}) = 0$. WLOG assume $g$ is monic. By the division algorithm, there exists unique polynomials $q(x), r(x) \in \mathbb{Q}[X]$ such that $f(x) = q(x)g(x) + r(x)$ and the degree of $r(x)$ is less than that of $g(x)$. Then since $f(\sqrt{2} + \sqrt{3}) = 0$ and $g(\sqrt{2} + \sqrt{3}) = 0$ it follows that $r(\sqrt{2} + \sqrt{3}) = 0$. By the minimality of the degree of $g(x)$ this implies that $r(x)$ is of degree zero, that is, $r(x) = C \in \mathbb{Q}$. But then $C = 0$. So $f(x) = q(x)g(x)$.

Hence $f(x)$ is reducible, as either a product of linear times a cubic, or the product of two quadratics. Suppose $f(x)$ is the product of a linear poly. and a cubic poly. WLOG assume $x - r$ for $r \in \mathbb{Q}$ is the linear poly. That would make $r$ a root of $f(x)$ and hence would have to be an integer factor of $f(0) = 1$. So $r = \pm 1$. But $f(\pm 1) = -8 \neq 0$. Now suppose $g(x)$ and $g(x)$ are quadratic. WLOG assume $g(x) = x^2 + ax + b$ for some $a, b \in \mathbb{Q}$. Then since $g(\sqrt{2} + \sqrt{3}) = 0$ we get
$$(\sqrt{2} + \sqrt{3})^2 + a(\sqrt{2} + \sqrt{3}) + b = (5 + b) + 2\sqrt{6} + a\sqrt{2} + a\sqrt{3},$$which cannot be 0 as there is no $a, b \in \mathbb{Q}$ such that the above is 0 (as 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ are linearly independent over $\mathbb{Q}$).

(b) Show $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a simple extension field of $\mathbb{Q}$.

Proof: Clearly $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We try to show the reverse. Consider that
$$\frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$But then $\sqrt{3} = (1/2) [(\sqrt{2} + \sqrt{3}) + (\sqrt{3} - \sqrt{2})]$ and $\sqrt{2} = (1/2) [(\sqrt{2} + \sqrt{3}) - (\sqrt{3} - \sqrt{2})]$. So $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is a simple extension field of $\mathbb{Q}$.
(2) Let $n \in \mathbb{N}$. Let $E$ be an extension field of $F$ that as a vector space over $F$ has dimension $n$. Let $a \in E$. Prove that $a$ is algebraic of degree at most $n$ over $F$.

**Proof:** To yield a contradiction suppose $a$ either has degree more than $n$ over $F$ or is transcendental over $F$. Then the only solution to $b_0 + b_1a + b_2a^2 + \cdots + b_na^n = 0$ where $b_0, b_1, b_2, \ldots, b_n \in F$ is the trivial solution $b_0 = b_1 = b_2 = \cdots = b_n = 0$, as otherwise $a$ would be the root of $f(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n \in F[x]$. That implies that $\{1, a, a^2, \ldots, a^n\}$ is linearly independent and thus spans a subspace of $E$ of dimension $(n + 1)$ over $F$. This contradicts that the dimension of $E$ is $n$. So $a$ is algebraic of degree at most $n$ over $F$. □

(3) Let $n \in \mathbb{N}$, $n \geq 2$, and $q \in \mathbb{N}$ be a positive integer power of a prime number. Let $\mathbb{F}_q$ be a field with $q$ elements.

(a) How many non-zero vectors does $(\mathbb{F}_q)^n$ contain?

$q^n$ total vectors, so $q^n - 1$.

(b) Let $x \in (\mathbb{F}_q)^n$ be a non-zero vector. How many vectors are there in $(\mathbb{F}_q)^n$ that DO NOT lie in the Span($x$)?

$q$ vectors in that span, so $q^n - q$.

(c) Let $x, y \in (\mathbb{F}_q)^n$ be a pair of linearly independent vectors. How many vectors are there in $(\mathbb{F}_q)^n$ that DO NOT lie in the Span($x, y$)?

$q^2$ vectors in that span, so $q^n - q^2$.

(d) Consider the group $G = \text{GL}_n(\mathbb{F}_q)$ consisting of invertible $n \times n$ matrices over a finite field with $q$ elements. Find the order of $G$.

Hint: Each column (after the first) of an invertible matrix must not lie in the span of the previous columns.

It would be $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) = \prod_{i=0}^{n-1} (q^n - q^i)$.
(4) We know that \( f(x) = x^3 + x^2 + 1 \) is irreducible over \( \mathbb{Z}_2 \). Let \( \alpha \) be a root of \( f(x) \) is some extension field \( E \) of \( \mathbb{Z}_2 \). Show that \( f(x) \) factors into the product of 3 linear factors in \( \mathbb{Z}_2(\alpha) \).

Hint: Every element of \( \mathbb{Z}_2(\alpha) \) looks like \( a_0 + a_1\alpha + a_2\alpha^2 \) where \( a_0, a_1, a_2 \in \mathbb{Z}_2 \). Divide \( x^3 + x^2 + 1 \) by \( x - \alpha \) using long division and show that the quadratic quotient has a root in \( \mathbb{Z}_2(\alpha) \).

**Proof**: By long division \( f(x) = (x + \alpha)g(x) \) where \( g(x) = x^2 + (\alpha + 1)x + (\alpha^2 + \alpha) \).

It suffices to show that \( g \) has a root in the field \( E \). Consider

\[
g(\alpha^2) = (\alpha^2)^2 + (\alpha + 1)(\alpha^2) + (\alpha^2 + \alpha) = \alpha^4 + \alpha^3 + \alpha = \alpha(\alpha^3 + \alpha^2 + 1) = 0 \quad □
\]

Incidentally, \( f(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^2 + \alpha + 1) \).

(5) Let \( F \) be a field. Let \( i, j, k \) satisfy \( i^2 = j^2 = k^2 = -1 \) and \( ij = k, jk = i, ki = j \), \( ji = -k, kj = -i \) and \( ik = -j \). Then assume that for any \( a \in F \), \( ab = ba \) for all \( b \in \{i, j, k\} \). Let \( Q_F = \{a + bi + cj + dk | a, b, c, d \in F \} \). Addition in \( Q_F \) is done by combining “like” terms (involving the linearly independent quantities \( 1, i, j, k \)) and multiplication is done with the distributive property and the rules given for multiplying \( i, j, k \) amongst themselves and with field elements. It turns out that \( Q_F \) is a noncommutative ring, called the *quaternions*.

(a) Compute \((1 + i + j + 2k)(1 + 2i + 2j + k)\) if \( F \) is of characteristic 3.

\[
(1 + i + j + 2k)(1 + 2i + 2j + k) = 1.
\]

(b) Compute \((1 + i + 2j + 3k)(1 - i - 2j - 3k)\) if \( F \) is of characteristic 0.

\[
(1 + i + 2j + 3k)(1 - i - 2j - 3k) = 15.
\]
(c) Show that \( \phi : Q_F \to M_2(\mathbb{C}) \) given by the rule below is a monomorphism.

\[
\phi(a + bi + cj + dk) = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + c \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} + d \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.
\]

**Proof:** To show that \( \phi \) is a homomorphism, since it is obvious that \( \phi(a + bi + cj + dk) = a\phi(1) + b\phi(i) + c\phi(j) + d\phi(k) \), it suffices to show that \( \phi(2^\beta) = \phi(2^\Gamma) = \phi(k^2) = \phi(-1) = -\phi(1) \). \( \phi(ij) = \phi(i)\phi(j) \), \( \phi(ji) = \phi(j)\phi(i) \), \( \phi(ik) = \phi(i)\phi(k) \), \( \phi(ki) = \phi(k)\phi(i) \), \( \phi(jk) = \phi(j)\phi(k) \), and \( \phi(ji) = \phi(j)\phi(i) \).

By the definition of \( \phi \), \( \phi(1) = I_2 \). We see that

\[
\phi(ij) = \phi(k) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \phi(i)\phi(j).
\]

Also

\[
\phi(ji) = \phi(-k) = -\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \phi(j)\phi(i).
\]

Also

\[
\phi(ij) = \phi(\alpha) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \phi(i)\phi(k).
\]

Also

\[
\phi(jk) = \phi(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \phi(j)\phi(k).
\]

Finally

\[
\phi(kj) = \phi(-i) = -\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \phi(j)\phi(k).
\]

Now it only remains to show that ker(\( \phi \)) is \{0\}. For that it suffices to show that the only solution to \( a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + c \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} + d \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = 0 \) is the trivial solution (in other terms, that the matrices are linearly independent).

From that equation we get 4 linear equations: \( a + di = 0 \), \( b + ci = 0 \), \( -b + ci = 0 \), and \( a - di = 0 \). Adding the first and last equations yields \( a = 0 \) and hence \( d = 0 \). Adding the other two yields \( c = 0 \) and hence \( b = 0 \). So \( \phi \) is a monomorphism. \( \Box \)

(d) If the characteristic of \( F \) is 5 then show that \( 1 + 2i + 3j - k \) is a zero divisor in \( Q_F \).

\[
(1 + 2i + 3j - k)(2 + i + j + 3k) = 0.
\]

(6) Let \( E \) be an extension field of \( F \). Let \( \alpha \in E \) be algebraic of odd degree over \( F \). Show that \( \alpha^2 \) is algebraic of odd degree over \( F \) and \( E(\alpha) = F(\alpha^2) \).

**Proof:** Let \( F \) be a field and \( E \) be an extension field of \( F \). Let \( \alpha \in E \) be algebraic of odd degree over \( F \). Then \( [E(\alpha) : F] \) is odd. Clearly \( F(\alpha^2) \subseteq F(\alpha) \). To yield a contradiction suppose \( F(\alpha) \not\subseteq F(\alpha^2) \). In particular, that means \( \alpha \not\in F(\alpha^2) \). Since \( \alpha \) is a root of \( x^2 - \alpha^2 \in F(\alpha^2)[x] \) it follows that \( [F(\alpha) : F(\alpha^2)] = 2 \). But then \( [F(\alpha) : F] = [F(\alpha) : F(\alpha^2)] [F(\alpha^2) : F] = 2 [F(\alpha^2) : F] \), implying that \( [F(\alpha) : F] \) is even, which is contradiction. Hence, \( F(\alpha) \subseteq F(\alpha^2) \), and thus \( F(\alpha) = F(\alpha^2) \). \( \Box \)
(7) Let $E$ be an extension field of a field $F$.

(a) If $[E : F]$ is a prime, show that $E = F(\alpha)$ for all $\alpha \in E \setminus F$.

Proof: Suppose $[E : F]$ is prime. Let $\alpha \in E \setminus F$. Then $E \geq F(\alpha) > F$. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ is prime and $[F(\alpha) : F] > 1$ it follows that $[E : F] = [F(\alpha) : F]$ and $[E : F(\alpha)] = 1$, which implies that $E = F(\alpha)$ □

(b) Show that if $a, b \in E$ are algebraic over $F$ of degrees $m, n$ respectively, and $m, n$ are relatively prime then $[F(a, b) : F] = mn$.

Proof: Let $F$ be a field and $E$ be an extension field. Let $a, b \in E$ be algebraic over $F$ of degrees $m, n$ respectively, where $m, n$ are relatively prime. Then $[F(a) : F] = m$ and $[F(b) : F] = n$. Then since $[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F] = [F(a, b) : F(a)][F(a) : F]$, it follows that $[F(a, b) : F]$ is divisible by $m$ and $n$, and hence $mn$ since $m$ and $n$ are relatively prime. So $[F(a, b) : F] \geq mn$. Since $a$ is algebraic of degree $m$ over $F$, it is algebraic of degree at most $m$ over $F(b)$. Hence $[F(a, b) : F] = [F(a, b) : F(b)][F(b) : F] \leq mn$. So we are done, as it must be the case that $[F(a, b) : F] = mn$ □

(8) Show that if $F$ is a finite field of odd characteristic then $F$ is not algebraically closed.

Proof: Let $F$ be a finite field of odd characteristic. Then $-1 \neq 1$. But $(-1)^2 = 1^2$, so \{$x^2 | x \in F$\} is a subset of $F$ with at most $|F| - 1$ elements. Thus there exists an element $\alpha \in F$ such that $\alpha^2 \neq \alpha$ for all $a \in F$. Hence for $f(x) = x^2 - \alpha \in F[X]$ we have that $f(x)$ has no root in $F$. Hence $F$ is not algebraically closed □

(9) Let $p \in \mathbb{N}$ be a prime. Construct a field of order $p^2$.

Proof: Suppose $p = 2$. $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$. So $I = (f(x))$ is a maximal ideal of $\mathbb{Z}_2[x]$ and thus $F = \mathbb{Z}_2[x]/I$ is a field. Every element in $F$ is expressible in the form $ax + b + I$, so there are $p^2 = 4$ elements in $F$. Now suppose $p$ is an odd prime. Then by the result of the previous exercise, $\exists \alpha \in \mathbb{Z}_p$ such that $f(x) = x^2 - \alpha$ is irreducible over $\mathbb{Z}_p$. So $I = (f(x))$ is a maximal ideal of $\mathbb{Z}_p[x]$ and thus $F = \mathbb{Z}_p[x]/I$ is a field. Every element in $F$ is expressible in the form $ax + b + I$, so there are $p^2$ elements in $F$ □

(10) Let $p \in \mathbb{N}$ be a prime and $F$ be a finite field of characteristic $p$. Show that every element of $F$ is algebraic over the subfield $\mathbb{Z}_p$.

Proof: Clearly $0$ is algebraic over $\mathbb{Z}_p$ as it’s a root of $x \in \mathbb{Z}_p[x]$. Let $\alpha \in F^\ast$. Since $F$ is a finite field, $F^\ast$ is a finite group under multiplication. So the order of $\alpha$ under multiplication is finite (and a divisor of $|F^\ast|$). Let $k \in \mathbb{N}$ be the order of $\alpha$. Then $\alpha^k = 1$, which implies that $\alpha$ is a root of $f(x) = x^k - 1 \in \mathbb{Z}_p[x]$. Hence every element of $F$ is algebraic over $\mathbb{Z}_p$ □