Justify your answers. The complex numbers, the real numbers and the finite field with \( p \) elements will be denoted by \( \mathbb{C} \), \( \mathbb{R} \) and \( \mathbb{F}_p \) respectively.

(1) Suppose that \( f(X) \in \mathbb{F}_2[X] \) is a square-free polynomial of degree 5 with coefficients in \( \mathbb{F}_2 \), and \( K \) is the splitting field of \( f(X) \). What are the possibilities for the Galois group of the field extension \( K/\mathbb{F}_2 \)?

(2) Suppose that \( V \) and \( W \) are nonzero finite dimensional \( \mathbb{R} \)-vector spaces. The vector space \( V \) is equipped with a symmetric bilinear form \((\cdot,\cdot)_V\) and \( W \) is equipped with a symmetric bilinear form \((\cdot,\cdot)_W\).
   (a) Show that there exists a symmetric bilinear form \((\cdot,\cdot)_{V \otimes W}\) on \( V \otimes W \) such that
   \[
   (v_1 \otimes w_1, v_2 \otimes w_2)_{V \otimes W} = (v_1, v_2)_V (w_1, w_2)_W
   \]
   for all \( v_1, v_2 \in V \) and \( w_1, w_2 \in W \).
   (b) Assume that \((\cdot,\cdot)_V\) and \((\cdot,\cdot)_W\) are positive definite. Show that \((\cdot,\cdot)_{V \otimes W}\) is positive definite as well.

(3) Let \( R \) be a commutative ring with 1 and \( M \) an ideal of \( R \).
   (a) Show that, if \( M \) is both maximal and principal, then there is no ideal \( I \) of \( R \) such that \( M \nsubseteq I \nsubseteq M^2 \).
   (b) Give an example of a commutative ring \( R \), a maximal ideal \( M \) (but not necessarily principal) of \( R \) and an ideal \( I \) with \( M \nsubseteq I \nsubseteq M^2 \).

(4) Define
   \[
   B = \begin{pmatrix}
   0 & 1 & 0 & 0 \\
   0 & 0 & 1 & 0 \\
   0 & 0 & 0 & 0 \\
   0 & 0 & 0 & 0 
   \end{pmatrix}.
   \]
   (a) Suppose that \( A \) is a complex \( 4 \times 4 \) matrix with \( AB = 0 \). Describe the possibilities for the Jordan normal form of \( A \).
   (b) Suppose that \( A \) is a complex \( 4 \times 4 \) matrix with \( AB = BA = 0 \). Describe the possibilities for the Jordan normal form of \( A \).

(5) Suppose that \( G \) is a finite group with whose order is divisible by the prime number \( p \) and \( \sigma \) is an automorphism of \( G \) such that \( \sigma^p \) is the identity. Show that \( G \) has an element \( g \) of order \( p \) with \( \sigma(g) = g \).
Justify your answers. The complex numbers, the real numbers and the finite field with \( p \) elements will be denoted by \( \mathbb{C} \), \( \mathbb{R} \) and \( \mathbb{F}_p \) respectively.

(1) Suppose that \( A \) is a complex \( 5 \times 5 \) matrix with minimal polynomial \( X^5 - X^3 \).
   (a) What is the characteristic polynomial of \( A^2 \)?
   (b) What is the minimal polynomial of \( A^2 \)?

(2) Let \( G = \text{GL}_n(\mathbb{F}_p) \) be the group of invertible \( n \times n \) matrices with coefficients in \( \mathbb{F}_p \), where \( p \) is prime. Then \( G \) acts by left multiplication on the \( \mathbb{F}_p \)-vector space \( (\mathbb{F}_p)^n \) consisting of all \( n \)-high column vectors with entries in \( \mathbb{F}_p \). This induces an action of \( G \) on the set \( S \) of chains of \( \mathbb{F}_p \)-vector spaces \( 0 \subseteq V_1 \subseteq V_2 \subseteq \cdots \subseteq V_n = (\mathbb{F}_p)^n \) in which \( \dim V_i = i \).
   (a) Determine the size of \( S \).
   (b) Describe the stabilizer in \( G \) of the chain in which \( V_i \) consists of all \( n \)-high column vectors whose bottom \( n - i \) entries are all zero.

(3) Let \( K = \mathbb{Q}(\sqrt{3}, i) \).
   (a) What is the degree of the field extension \( K/\mathbb{Q} \)?
   (b) Show that \( K/\mathbb{Q} \) is a Galois extension. What is the Galois group of this extension?

(4) For which nonnegative integers \( a, b \) is the ring \( \mathbb{Z}[X]/(bX - a) \) an integral domain?

(5) Let \( G \) be a finite group without any proper characteristic subgroup. This means that for every subgroup \( H \) with \( \{1\} \subsetneq H \subsetneq G \) there exists an automorphism \( \sigma \) of \( G \) such that \( \sigma(H) \neq H \). Show that there is a simple group \( L \) and a positive integer \( k \) such that \( G \cong \prod_{i=1}^{k} L \) is isomorphic to the direct product of \( k \) copies of \( L \).
(1) Let $d$ be the degree of the extension $K/F_2$. The Galois group is cyclic of order $d$. Note that there are two irreducible polynomials of degree 1 ($X$ and $X + 1$), one irreducible polynomial of degree 2 ($X^2 + X + 1$) and for each $d \geq 3$ there is at least 1 irreducible polynomial. The possibilities of the degrees of the factors of $f$ are

(a) 1, 1, 3;
(b) 2, 3;
(c) 1, 4;
(d) 5.

The value of $d$ is the least common multiple of the degrees of the factors, and has to be 3, 6, 4 or 5 respectively.

(2) (a) For fixed $v_2 \in V$ and $w_2 \in W$, the map
\[
(v_1, w_1) \mapsto (v_1, v_2)\cdot (w_1, w_2)
\]
is bilinear. By the universal property of tensor product, there exists a linear map
\[
\psi_{v_2, w_2} : V \otimes W \to \mathbb{R}
\]
such that
\[
\psi_{v_2, w_2}(v \otimes w) = (v, v_2)\cdot (w, w_2).
\]
The map $V \times W \to \text{Hom}(V \otimes W, \mathbb{R})$ given by $(v_2, w_2) \mapsto \psi_{v_2, w_2}$ is bilinear, so there exists a linear map $\psi' : V \otimes W \to \text{Hom}(V \otimes W, \mathbb{R})$ with
\[
\psi'(v_2 \otimes w_2) = \psi'_{v_2, w_2}.
\]
Now we define
\[
(a_1, a_2)_{V \otimes W} = \psi'(a_1)(a_2).
\]
Note that $(a_1, a_2)_{V \otimes W}$ is linear in $a_2$ because $\psi'(a_1)$ is linear, and it is linear in $a_1$ because $\psi'$ is linear. To show symmetry, note that
\[
\left( \sum_i v_i \otimes w_i, \sum_j v_j \otimes w_j \right)_{V \otimes W} = \sum_{i,j} (v_i \otimes w_i, v'_j \otimes w'_j)_{V \otimes W} = \sum_{i,j} (v_i, v'_j)_{V}(w_i, w'_j)_{W} = \sum_{i,j} (v'_j, v_i)_{V}(w'_j, w_i)_{W} = \left( \sum_j v'_j \otimes w'_j, v_i \otimes w_i \right)_{V \otimes W}.
\]

(b) We can choose a basis $v_1, v_2, \ldots, v_n$ of $V$ such that $(v_i, v_j)_V = \delta_{i,j}$ (Kronecker delta function) for all $i, j$. We can also choose a basis $w_1, \ldots, w_m$ of $W$ such that $(w_i, w_j)_W = \delta_{i,j}$. With respect to the basis $v_i \otimes w_j$ with $1 \leq i \leq n$ and $1 \leq j \leq m$, the bilinear form $(\cdot, \cdot)_{V \otimes W}$ is the usual inner product, so it is positive definite.

(3) (a) Since $A$ has rank at most 2, its Jordan normal form must also have rank at most 2. On the other hand, if $J$ is a matrix in Jordan normal form and $J$ has rank at most 2, then there exists an invertible matrix such that $C \text{im}(B) \subseteq \ker(J)$. So
The given page contains a continuation of a mathematical discussion. It begins with a statement about matrices and their transformations. Specifically, it mentions the conditions under which certain matrices can be expressed in a Jordan normal form. The page also details the possible forms of matrices with specific properties, such as rank conditions and the relationship between matrices and their transformations.

The text is structured in a way that suggests it is part of a larger mathematical exposition, likely in the field of linear algebra or matrix theory. The page includes examples of matrices in Jordan normal form, which are used to illustrate the concepts being discussed.

The bottom of the page appears to be cut off, indicating that there may be additional content or a continuation of the discussion not visible in the image.
with $\lambda_1 \in \mathbb{C}$ or

with $\lambda_1 \in \mathbb{C}$.

(c) case (i) appears when $b = c = 0$ and $a = 1$, case (ii) appears when $a = b = c = 0$ and case (iii) appears when $a = d = 0$ and $b = c = 1$.

(4) (a) Suppose that $M = (m)$. and $(m) = M \supseteq I \supseteq M^2 = (m^2)$. Let $I' = \{a \in R \mid am \in I\}$ and $M' = \{a \in R \mid am \in M^2\}$. We have $M \subseteq M' \subseteq I' \subseteq R$ so $I' = M$ or $I' = R$. If $I' = R$ then we have $m \in I$ and $I = M$. If $I' = M$ then for every $b \in I$ we can write $b = ma$ with $a \in I' = M$, so $b \in M^2$ and we conclude that $I = M^2$.

(b) For example $R = \mathbb{C}[X,Y]$, $M = (X,Y)$, $I = (X^2,Y)$ and $M^2 = (X^2,XY,Y^2)$.

(5) Let $H$ be the subgroup of all elements $g \in G$ with $\sigma(g) = g$. The group $\langle \sigma \rangle$ acts on $G$ and its orbits have 1 or $p$ elements (because the orbit size has to divide the order of $\langle \sigma \rangle$). So $G \setminus H$ is a union of orbits of size $p$, and $|G \setminus H| = |G| - |H|$ is divisible by $p$. Since $|G|$ is divisible by $p$, we conclude that $|H|$ is divisible by $p$. By Cauchy's theorem, $H$ has an element of order $p$. 
(1) The minimum polynomial is equal to the characteristic polynomial. The matrix $A$ must be conjugate to
\[
B = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & -1
\end{pmatrix}
\]
and $A^2$ is conjugate to
\[
B^2 = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}
\]
(a) The characteristic polynomial of $A^2$ (and $B^2$) is $X^3(X - 1)^2$.
(b) The minimum polynomial of $A^2$ (and $B^2$) is $X^2(X - 1)$.

(2) (a) For every $i V_i/V_{i-1}$ is a 1-dimensional subspace of $\mathbb{F}_p^n/V_{i-1} \cong \mathbb{F}_p^{n-i+1}$ and the number of choices for this is $(p^n-i+1)/(p-1)$. These one dimensional subspaces uniquely determine the chain, so the total number of chains is
\[
p^{i-1} \cdot p^{i-2} \cdot \ldots \cdot p - 1.
\]

(b) The stabilizer consists of the invertible upper triangular matrices.

(3) (a) Let $L = \mathbb{Q}(\sqrt[6]{3})$. The field extension $L/\mathbb{Q}$ has degree 6 because the minimum polynomial $X^6 - 3$ is irreducible by Eisenstein’s criterion. The extension $K/L$ has degree 2 because $i^2 \in L$ and $i \notin L$. So $[K : \mathbb{Q}] = [K : L] \cdot [L : \mathbb{Q}] = 2 \cdot 6 = 12$.
(b) Let $\zeta = (1 + \sqrt[6]{3}i)/2$ be the primitive 6-th root of unity and let $M$ be the splitting field of $X^6 - 3$. Then $M$ contains $\sqrt[3]{3}$ and $\zeta \sqrt[3]{3}$ and therefore $\zeta$. Now $M$ also contains $\sqrt[3]{3}$ and $i = (2\zeta - 1)/\sqrt[3]{3}$. So $M$ contains $K$. On the other hand, $K$ contains $\zeta$ and $\sqrt[3]{3}$ and therefore it contains $M$. We conclude that $K = M$. So $K = M$ is a splitting field and this implies that $K/\mathbb{Q}$ is Galois. The Galois group is the dihedral group $D_6$ with 12 element. More precisely, the Galois group $K/\mathbb{Q}(\zeta)$ is generated by an automorphism $\sigma$ of order 6 that sends $\sqrt[3]{3}$ to $\zeta \sqrt[3]{3}$. Let $\tau$ be complex conjugation. This is another automorphism of $K/\mathbb{Q}$. Note that $\tau \sigma \tau^{-1} = \sigma^{-1}$. Now $\tau$ and $\sigma$ generate the dihedral group $D_6$.

(4) Let $R = \mathbb{Z}[X]/(bX - a)$. We distinguish the following cases:
(a) If $a = b = 0$ then $R = \mathbb{Z}[X]$ which is an integral domain.
(b) If $b = 0$ and $a = 1$ then $R = 0$ is not an integral domain. ( because in an integral domain 1 $\neq 0$).
(c) If $b = 0$ and $a = p$ is prime, then $R = \mathbb{F}_p[X]$ is an integral domain.
(d) If $b = 0$ and $a$ is not prime then $R$ has zero divisors and is not an integral domain.

(e) Suppose that $b > 0$ and $d = \gcd(a, b) \neq 1$. We can write $a = a'd$ and $b = b'd$. In $R$ we have $d(b'X - a') = 0$ and $d, b'X - a' \neq 0$. So $R$ has zero divisors and is not an integral domain.

(f) Suppose that $b > 0$ and $\gcd(a, b) = 1$. Define a ring homomorphism $\varphi : \mathbb{Z}[X] \to \mathbb{Q}$ by $\varphi(f(X)) = f(a/b)$. The kernel is generated by $bX - a$. Indeed if $f(X)$ is a polynomial in the kernel, then $f(a/b) = 0$ so we can factor $f(X) = g(X)(bX - a)$ with $g(X) \in \mathbb{Q}[X]$. By Gauß’ Lemma, $g(X)$ has integer coefficients and $f(X)$ lies in the ideal $(bX - a)$. By the first isomorphism theorem, $R = \mathbb{Z}[X]/(bX - a)$ is isomorphic to the image of $\varphi$, which is an integral domain because it is a subring of the integral domain $\mathbb{Q}$.

(5) Suppose that $G$ is not trivial. Let $L$ be a nontrivial normal subgroup of $G$. We may assume that $L$ does not have a nontrivial subgroup that is normal in $G$ and properly contained in $L$. For every automorphism $\sigma$ of $G$, $\sigma(L)$ is also a normal subgroup. Suppose that

$$\{\sigma(L) \mid \sigma \text{ is an automorphism of } G\} = \{L_1, L_2, L_3, \ldots, L_d\},$$

where $L_1, L_2, \ldots, L_d$ are distinct normal subgroups of $G$. By induction on $r$ we show that $L_1L_2 \cdots L_r$ is isomorphic to $L^s$ for some $s$. The case $r = 1$ is clear. Suppose that $L_1L_2 \cdots L_r \cong L^s$. Then $(L_1L_2 \cdots L_r) \cap L_{r+1}$ is a normal subgroup of $L_{r+1}$ and must be isomorphic to $L_{r+1}$ or $\{1\}$. In the first case, we have $L_1L_2 \cdots L_{r+1} = L_1L_2 \cdots L_r \cong L^s$. In the second case, $L_1L_2 \cdots L_r$ and $L_{r+1}$ are normal subgroups of $L_1L_2 \cdots L_{r+1}$ with a trivial intersection, so $L_1L_2 \cdots L_{r+1} = (L_1L_2 \cdots L_{r}) \times L_{r+1} \cong L^s \times L = L^{s+1}$. Suppose that $N$ is a normal subgroup of $L$ that is not equal to $L$. Then $N \times \{0\} \subset L^s$ is a normal subgroup. By minimality of $L$, we see that $N$ must be trivial. This proves that $L$ is simple.