1. Let $\mathbb{F}_q$ be a field with $q \neq 9$ elements and $a$ be a generator of the cyclic group $\mathbb{F}_q^*$. Show that $\text{SL}_2(\mathbb{F}_q)$ is generated by
\[
\begin{pmatrix}
1 & 1 \\
0 & 1 \\
\end{pmatrix},
\begin{pmatrix}
1 & 0 \\
a & 1 \\
\end{pmatrix}.
\]

2. Let $p, q$ be two prime numbers such that $p|q - 1$. Prove that
(a) there exists an integer $r \not\equiv 1 \mod q$ such that $r^p \equiv 1 \mod q$;
(b) there exists (up to an isomorphism) only one noncommutative group of order $pq$.

3. Let $F, L$ be extensions of a field $K$. Suppose that $F/K$ is finite. Show that there exists an extension $E/K$ such that there are monomorphisms of $F$ into $E$ and of $L$ into $E$ which are identical on $K$.

4. Find all irreducible representations of a finite $p$-group over a field of characteristic $p$.

5. How many two-sided ideals has the group algebra $\mathbb{C}[S_3]$, where $S_3$ is the group of permutations of $\{1, 2, 3\}$?
1. Show that any transitive subgroup of $A_5$ is isomorphic to one of the following groups: (a) the cyclic group $\mathbb{Z}/5\mathbb{Z}$, (b) the dihedral group $D_5$, (c) $A_5$.

2. Let $f(x) = x^5 - 5x + 12$. Verify that $f(x)$ is irreducible in $\mathbb{Q}[x]$ and its discriminant is $d(f) = (2^65^3)^2$. If $r_1, \ldots, r_5$ are the roots of $f$, let

$$P(x) = \prod_{1 \leq i < j \leq 5} (x - (r_i + r_j)).$$

Show that $P(x)$ is a product of two monic irreducible polynomials in $\mathbb{Q}[x]$:

$$P(x) = (x^5 - 5x^3 - 10x^2 + 30x - 36)(x^5 + 5x^3 + 10x^2 + 10x + 4).$$

Use this information, Problem 1 and properties of $f_3 \in \mathbb{F}_3[x]$, the reduction of $f$ modulo 3, to show that the Galois group $G_f$ of $f$ is isomorphic to $D_5$.

3. Let $D$ be an algebra over a field $k$, $\text{char } k \neq 2$, generated by elements $i, j$ and satisfies relations

$$i^2 = \alpha, j^2 = 1, ij = -ji \quad (\alpha \in k^\times).$$

Verify that $D$ is isomorphic to the algebra $M_2(k)$ of $2 \times 2$ matrices.

4. Let $f$ be a polynomial with $n$ variables and put

$$\text{Sym } f = \{ \sigma \in S_n \mid f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n) \}. $$

Prove that $\text{Sym } f$ is a subgroup of $S_n$. 

Prove that the group $D_4$ (of symmetries of the square) is isomorphic to $\text{Sym } (x_1x_2 + x_3x_4)$. 
All questions are equally weighted. Explain clearly how you arrive at your solutions. You have three hours in which to complete the exam.

Question 1. Let $V$ be an $n$-dimensional vector space over a field $k$ and let $\alpha: V \to V$ be a linear endomorphism. Prove that the minimal and characteristic polynomials of $\alpha$ coincide if and only if there is a vector $v \in V$ so that:

$$\{v, \alpha(v), \ldots, \alpha^{n-1}(v)\}$$

is a basis for $V$.

Question 2. Let $G$ be a group of order 24. Assume that no Sylow subgroup of $G$ is normal in $G$. Show that $G$ is isomorphic to the symmetric group $S_4$.

Question 3. (a) Fix a positive integer $n$ and classify all finite modules over the ring $\mathbb{Z}/n$.

(b) Prove, either using (a) or from first principles, for a fixed prime $p$ that all finite modules over $\mathbb{Z}/p$ are free.

Question 4. In this question all modules are left modules.

Let $k$ be a field of characteristic different from 2 and let $G = \{e, g\}$ be the multiplicative group with two elements. Consider the group ring $A = k[G]$.

(a) Show that the $A$-module $A$ is a direct sum of two ideals of $A$.
List all proper ideals of $A$.
Is $A$ a principal ideal domain?

(b) Show that every $A$-module decomposes into a direct sum of simple $A$-modules.

Assume now that the characteristic of the field $k$ is 2.

(c) Give an example of an $A$-module that cannot be decomposed into a direct sum of two simple $A$-modules.

Question 5. Let $t$ be transcendental over $\mathbb{Q}$. Set $K = \mathbb{Q}(t)$, $K_1 = \mathbb{Q}(t^2)$ and $K_2 = \mathbb{Q}(t^2 - t)$.
Show that $K$ is algebraic over $K_1$ and over $K_2$ and that $K$ is not algebraic over $K_1 \cap K_2$.

Question 6. Determine the Galois group over $\mathbb{Q}$ of the polynomial

$$X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15.$$
1. Let $F$ be a field of characteristic not equal to 2. Let $D$ be the non-commutative algebra over $F$ generated by elements $i, j$ that satisfy the relations

$$i^2 = j^2 = 1, \quad ij = -ji.$$ 

Define $k = ij$.

(a) Verify that $D$ is isomorphic to the algebra $M_2(F)$ of $2 \times 2$ matrices in such a way that

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad k \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$ 

(b) Write $q = x + yi + zj + uk$ for $x, y, z, u \in F$. Verify that the norm

$$N(q) = x^2 - y^2 - z^2 + u^2$$

corresponds to the determinant under the isomorphism of part (a).

(c) What does the involution $q \mapsto \overline{q} = x - yi - zj - uk$ on $D$ correspond to on the matrix side?

2. Let $R$ be a commutative ring. An $R$-module $M$ is said to be finitely presented if there exists a right-exact sequence

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

for some non-negative integers $m, n$. Prove that any finitely generated projective $R$-module $P$ is finitely presented.

3. Let $R$ be the ring $\mathbb{Z}[\zeta_p]$, where $p$ is a prime number and $\zeta_p$ denotes a primitive $p$th root of unity in $\mathbb{C}$. Prove that if an integer $n \in \mathbb{Z}$ is divisible by $1 - \zeta_p$ in $R$, then $p$ divides $n$.

4. Is $S_4$ isomorphic to a subgroup of $GL_2(\mathbb{C})$?

5. Let $n$ be a positive integer and $A$ an abelian group. Prove that

$$\text{Ext}^1(\mathbb{Z}/n\mathbb{Z}, A) \cong A/nA.$$
Each problem is worth 10 points.

(1) Show that there is no simple group of order 30.

(2) Let \( \Lambda \) be a free abelian group of finite rank \( n \), and let \( \Lambda' \subset \Lambda \) be a subgroup of the same rank. Let \( x_1, \ldots, x_n \) be a \( \mathbb{Z} \)-basis for \( \Lambda \), and let \( x'_1, \ldots, x'_n \) be a \( \mathbb{Z} \)-basis for \( \Lambda' \). For each \( i \), write \( x'_i = \sum_{j=1}^{n} a_{ij} x_j \), and let \( A := (a_{ij}) \in \text{Mat}_{n \times n}(\mathbb{Z}) \). Show that the index \([\Lambda : \Lambda']\) equals \(|\det A|\).

(3) In this problem all rings are commutative.

(a) Let \( R \) be a local ring with maximal ideal \( m \), let \( N \) and \( M \) be finitely generated \( R \)-modules, and let \( f: N \to M \) be an \( R \)-linear map. Show that \( f \) is surjective if and only if the induced map \( N/mN \to M/mM \) is.

(b) Recall that a module \( M \) over a ring \( R \) is projective if the functor \( \text{Hom}_R(M, -) \) is exact. Show that if \( R \) is local and \( M \) is finitely generated projective, then \( M \) is free.

(4) Compute the Galois group of \( x^5 - 10x + 5 \) over \( \mathbb{Q} \).

(5) Let \( K/k \) be an extension of finite fields with \( \#k = q \), let \( \Phi: x \mapsto x^q \) denote the \( q \)th power Frobenius map on \( K \), and let \( G := \text{Gal}(K/k) \).

(a) Compute the minimal polynomial of \( \Phi \) as a \( k \)-linear endomorphism of \( K \).

(b) Use (a) to prove the normal basis theorem in the case of the extension \( K/k \); there exists \( x \in K \) such that the set \( \{sx \mid s \in G\} \) is a \( k \)-basis for \( K \). (According to taste, it may be helpful to note that this is equivalent to the statement that \( K \cong k[G] \) as \( k[G] \)-modules.)

(6) Let \( G \) be a finite group with center \( Z \subset G \). Show that if \( G \) admits a faithful irreducible representation \( G \to \text{GL}_n(k) \) for some positive integer \( n \) and some field \( k \), then \( Z \) is cyclic.

---

1 In fact, the normal basis theorem holds for an arbitrary finite Galois field extension \( K/k \), but a different proof is required when \( k \) is infinite.
Each problem is worth 10 points.

(1) Let $A$ be a commutative ring, and define the nilradical $\sqrt{0}$ to be the set of nilpotent elements in $A$. Show that $\sqrt{0}$ is equal to the intersection of all prime ideals in $A$. Show that if $A$ is reduced, then $A$ can be embedded into a product of fields.

(2) Write down the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ and prove that it is reducible over $\mathbb{F}_p$ for every prime number $p$.

(3) Let $K/k$ be a finite separable field extension, and let $L/k$ be any field extension. Show that $K \otimes_k L$ is a product of fields.

(4) Let $M$ be an invertible $n \times n$ matrix with entries in an algebraically closed field $k$ of characteristic not 2. Show that $M$ has a square root, i.e. there exists $N \in \text{Mat}_{n\times n}(k)$ such that $N^2 = M$.

(5) Prove directly from the definition of (left) semisimple ring that every such ring is (left) Noetherian and Artinian. (You may freely use facts about semisimple, Noetherian, and Artinian modules.)

(6) Let $G$ be a finite group and $H$ an abelian subgroup. Show that every irreducible representation of $G$ over $\mathbb{C}$ has dimension $\leq [G : H]$. 
1. Determine $\text{Aut}(S_3)$.

2. A group $G$ is a semidirect product of subgroups $N, H \subset G$ if $N$ is normal and every element of $G$ has a unique presentation $nh$, $n \in N$, $h \in H$. Find all semidirect products (up to isomorphism) of $N = \mathbb{Z}/11\mathbb{Z}$, $H = \mathbb{Z}/5\mathbb{Z}$.

3. Let $F$ be a finite field of order $2^n$. Here $n > 0$. Determine all values of $n$ such that the polynomial $x^2 - x + 1$ is irreducible in $F[x]$.

4. (1). Determine the Galois group of $x^4 - 4x^2 - 2$ over $\mathbb{Q}$.
   (2). Let $G$ be a group of order 8 such that $G$ is the Galois group of a polynomial of degree 4 over $\mathbb{Q}$. Show that $G$ is isomorphic to the Galois group in part (1).

5. Let $A$ be a linear transformation of a finite dimensional vector space over a field of characteristic $\neq 2$.
   (1). Define the wedge product linear transformation $\wedge^2 A = A \wedge A$.
   (2). Prove that
   \[
   \text{tr}(\wedge^2 A) = \frac{1}{2}(\text{tr}(A)^2 - \text{tr}(A^2)).
   \]

6. Find a table of characters for the alternating group $A_5$. 
1. Classify all groups of order 66, up to isomorphism.

2. Let $F \subset K$ be an algebraic extension of fields. Let $F \subset R \subset K$ where $R$ is a $F$-subspace of $K$ with the property such that $\forall a \in R$, $a^k \in R$ for all $k \geq 2$.
   
   (1). Assume that $char(F) \neq 2$. Show that $R$ is a subfield of $K$.
   
   (2). Give an example such that $R$ may not be a field if $char(F) = 2$.

3. Determine the Galois group of $x^6 - 10x^3 + 1$ over $\mathbb{Q}$.

4. Let $V$ and $W$ be two finite dimensional vector spaces over a field $K$. Show that for any $q > 0$,
   
   \[
   \bigwedge^q(V \oplus W) \cong \sum_{i=0}^{q} \left( \bigwedge^i (V) \otimes_K \bigwedge^{q-i} (W) \right).
   \]

5. Prove that a finite dimensional algebra over a field is a division algebra if and only if it does not have zero divisors.

6. Let $A$ be a semi-simple finite dimensional algebra over $\mathbb{C}$, and let $V$ be a direct sum of two isomorphic simple $A$-modules. Find the automorphism group of the $A$-module $V$. 
All five problems are equally weighted. (The problem parts need not be equally weighted.) Explain clearly how you arrive at your solutions, or you risk losing credit. You will be given three hours in which to complete the exam.

1. Prove that every group of order 15 is cyclic.

2. The dihedral group $D_{2n}$ is the group on two generators $r$ and $s$, with respective orders $o(r) = n$ and $o(s) = 2$, subject to the relation $rsr = s$.
   (a) Calculate the order of $D_{2n}$.
   (b) Let $K$ be the splitting field of the polynomial $x^8 - 2$. Determine whether the Galois group $\text{Gal}(K/\mathbb{Q})$ is dihedral (i.e., isomorphic to $D_{2n}$ for some $n$).

3. Let $G = S_4$ (the symmetric group on four letters).
   (a) Prove that $G$ has two non-equivalent irreducible complex representations of dimension 3; call them $\rho_1$ and $\rho_2$.
   (b) Decompose $\rho_1 \otimes \rho_2$ (as a representation of $G$) into a direct sum of irreducible representations.

4. Let $H = S_3 \times S_5$.
   (a) Determine all normal subgroups of $H$. Make sure you have them all! What would be different if $H$ were replaced by $S_2 \times S_5$?
   (b) Describe, in full detail, the construction of a polynomial with rational coefficients, whose Galois group is isomorphic to $H$.

5. Let $L$ be a finite field. Let $a$ and $b$ be elements of $L^\times$ (the multiplicative group of $L$) and $c \in L$. Show that there exist $x$ and $y$ in $L$ such that $ax^2 + by^2 = c$.

6. Let $K$ be a finite algebraic extension of $\mathbb{Q}$.
   (a) Give the definition of an integral element of $K$.
   (b) Show that the set of integral elements in $K$ form a sub-ring of $K$. 
(c) **Determine** the ring of integers in each of the following two fields *No credit for memorized answers:* $\mathbb{Q}(\sqrt{13})$, and $\mathbb{Q}(\sqrt{2})$. 
1. Let $K$ be a field of characteristic $p > 0$. Prove that a polynomial $f(x) = x^p - x - a \in K[x]$ either irreducible, or is a product of linear factors. Find this factorization if $f$ has a root $x_0 \in K$.

2. Let $A, B$ be two commuting operators on a finite dimensional space $V$ over $\mathbb{C}$ such that $A^n = B^m$ is the identity operator on $V$ for some positive integers $n, m$. Prove that $V$ is a direct sum of 1-dimensional invariant subspaces with respect to $A$ and $B$ simultaneously.

3. Let $G$ be a finite $p$-group. Determine all irreducible representations of $G$ over a field $K$ of characteristic $p$.

4. Prove that the polynomial $x^4 + 1$ is not irreducible over any field of positive characteristic.

5. Prove that a tensor product of irreducible representations over an algebraically closed field is irreducible.

6. Let $D$ be an algebra over a field $K$ of characteristic $\neq 2$ generated by two elements $i, j$ satisfying relations

$$i^2 = 1, j^2 = 1, ij = -ji.$$  

Prove, that $D \simeq GL_2(K)$.
All five problems are equally weighted. (The problem parts need not be equally weighted.) Explain clearly how you arrive at your solutions, or you risk losing credit. You will be given three hours in which to complete the exam.

1. (a) Let $S_n$ be the symmetric group (permutation group) on $n$ objects. Prove that if $\sigma \in S_n$ is an $n$-cycle and $\tau \in S_n$ is a transposition (i.e., a 2-cycle), then $\sigma$ and $\tau$ generate $S_n$.

(b) Let $f_a(x)$ be the polynomial $x^5 - 5x^3 + a$. Determine an integer $a$ with $-4 \leq a \leq 4$ for which $f_a$ is irreducible over $\mathbb{Q}$, and the Galois group of [the splitting field of] $f_a$ over $\mathbb{Q}$ is $S_5$. Then explain why the equation $f_a(x) = 0$ is not solvable in radicals.

2. Let $R = \mathbb{Q}[X]$, $I$ and $J$ the principal ideals generated by $X^2 - 1$ and $X^3 - 1$ respectively. Let $M = R/I$ and $N = R/J$. Express in simplest terms [the isomorphism type of] the $R$-modules $M \otimes_R N$ and $\text{Hom}_R(M, N)$. Explain.


(a) Prove that $G$ has an irreducible complex representation of dimension 2, — call it $\rho$ — but none of higher dimension.

(b) Decompose $\rho \otimes \rho \otimes \rho$ (as a representation of $G$) into a direct sum of irreducible representations.

4. (a) Let $G$ be a group of order $p^2q^2$, where $p$ and $q$ are distinct odd primes, with $p > q$. Show that $G$ has a normal subgroup of order $p^2$.

(b) Can a solvable group contain a non-solvable subgroup? Explain.

5. (a) Prove that every group of order $p^2$ ($p$ a prime) is abelian. Then classify such groups up to isomorphism.

(b) Give an example of a non-abelian group of order $p^3$ for $p = 3$. Suggestion: Represent the group as a group of matrices.
1. Find the number of colouring of faces of a cube in 3 colours. Two colourings are equal if they are the same after a rotation of the cube. [Hint Use the Burnside formula]

\[
|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,
\]

where a group \( G \) acts on a set \( X \), \( X/G \) is the set of orbits, and, for every \( g \in G \), \( X^g \) is the fixed subset of \( g \) in \( X \).

2. Proof that all groups of order < 60 are solvable.

3. Let \( L/K \) be a Galois extension of degree \( p \) with \( \text{char} K = p \). Show that \( L = K(\theta) \), where \( \theta \) is a root of \( x^p - x - a, a \in K \), and, conversely, any such extension is Galois of degree 1 or \( p \).

4. Proof that a finite dimensional associative algebra over a field is a division algebra if and only if it has no zero divisors.

5. Find the table of characters for \( S_4 \).
Student’s Name:

To receive full credit, show all of your work.

1. Let \( p > 2 \) be a prime. Classify groups of order \( p^3 \) up to isomorphism.

2. Let \( a \) be an integral algebraic number such that its norm is 1 for any imbedding into \( \mathbb{C} \), the field of complex numbers. Prove that \( a \) is a root of unity.

3. Let \( R \) be a commutative ring with unity. Given an \( R \)-module \( A \) and an ideal \( I \subset R \), there is a natural \( R \)-module homomorphism \( A \otimes_R I \to A \otimes_R \mathbb{R} \) induced by the inclusion \( I \subset R \). In the following three steps you shall prove the flatness criterion: \( A \) is flat if and only if for every finitely generated ideal \( I \subset R \) the natural map \( A \otimes_R I \to A \otimes_R \mathbb{R} \) is injective.
   (a) Prove that if \( A \) is flat and \( I \subset R \) is a finitely generated ideal then \( A \otimes_R I \to A \otimes_R \mathbb{R} \) is injective.
   (b) If \( A \otimes_R I \to A \otimes_R \mathbb{R} \) is injective for every finitely generated ideal \( I \), prove that \( A \otimes_R I \to A \otimes_R \mathbb{R} \) is injective for every ideal \( I \). Show that if \( K \) is any submodule of a free module \( F \) then the natural map \( A \otimes_R K \to A \otimes_R \mathbb{R} \) is injective (\( \text{Hint: the general case reduces to the case when } F \text{ has finite rank} \)).
   (c) Let \( \psi: L \to M \) be an injective homomorphism of \( R \)-modules. Prove that the induced map \( 1 \otimes \psi: A \otimes_R L \to A \otimes_R M \) is injective (\( \text{Hint: Write } M \text{ as a quotient } f: F \to M \text{ of a free module } F, \text{ giving a short exact sequence } 0 \to K \to F \to M \to 0 \text{ and consider the commutative diagram} \)).

4. (a) Let \( R \) be a P.I.D. Prove that a finitely generated \( R \)-module \( M \) is flat if and only if \( M \) is torsion-free (hence, free by the structure theorem).
   (b) Give an example of an integral domain \( R \) and a torsion-free \( R \)-module \( M \) such that \( M \) is not free.

5. Compute the Galois group of \( f(x) = x^4 + 1 \) over \( \mathbb{Q} \).

6. Let \( p \) be a prime and let \( F \) be a field of characteristic \( p \).
   (a) Prove that the map \( \varphi: F \to F, \varphi(a) = a^p \) is a field homomorphism.
   (b) \( F \) is said to be perfect if the above homomorphism \( \varphi \) is an automorphism. Prove that every finite field is perfect.
   (c) If \( x \) is an indeterminate and \( F \) is any field of characteristic \( p \), prove that the field \( F(x) \) is not perfect.
1. Prove that, as a \( \mathbb{Z} \)-module, \( \mathbb{Q} \) is flat but not projective.

2. Let \( p \) and \( q \) be primes with \( p < q \). Let \( G \) be a group of order \( pq \). Prove the following statements:
   
   (a) If \( p \) does not divide \( q - 1 \) then \( G \) is cyclic.
   
   (b) If \( p \) divides \( q - 1 \) then \( G \) is either cyclic or isomorphic to a non-abelian group on two generators. Give the presentation of this non-abelian group.

3. Prove that every group of order \( p^2q \) where \( p \) and \( q \) are primes is solvable.

4. Prove that the group of automorphisms \( \text{Aut}_\mathbb{Q}(\mathbb{R}) \) of the field \( \mathbb{R} \) that fix \( \mathbb{Q} \) pointwise is trivial (Hint: Prove that every such automorphism is continuous).

5. Let \( A \) and \( B \) be \( n \times n \) matrices with complex coefficients. Assume that \( (A - I)^n = 0 \) and \( A^kB = BA^k \) for some natural number \( k \). Prove that \( AB = BA \) (Hint: Prove that \( A \) can be expressed as a function of \( A^k \)).

6. Let \( K \) be the splitting field of \( x^6 - 5 \) over \( \mathbb{Q} \).
   
   (a) Prove that \( x^6 - 5 \) is irreducible over \( \mathbb{Q} \).
   
   (b) Compute the Galois group of \( K \) over \( \mathbb{Q} \).
   
   (c) Describe an intermediate field \( F \) such that \( F \) is not \( \mathbb{Q} \) or \( K \) and \( F/\mathbb{Q} \) is Galois.
1. Let $G$ be a group of order $p^3q^2$, where $p$ and $q$ are prime integers. Show that for $p$ sufficiently large and $q$ fixed, $G$ contains a normal subgroup other than $\{1\}$ and $G$.

2. (a) Prove that if $M$ is an abelian group and $n$ is a positive integer, the tensor product $M \otimes \mathbb{Z}/n\mathbb{Z}$ can be naturally identified with $M/nM$.

(b) Compute the tensor product over $\mathbb{Z}$ of $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$. Also compute the tensor products $\mathbb{Q} \otimes \mathbb{Q}$, $\mathbb{Q} \otimes (\mathbb{Q}/\mathbb{Z})$, and $(\mathbb{Q}/\mathbb{Z}) \otimes (\mathbb{Q}/\mathbb{Z})$.

(c) Let $\mathbb{Z}^N$ denote the (abelian) group of sequences $(a_i)_{i \in \mathbb{N}}$ in $\mathbb{Z}$ under termwise addition, and $\mathbb{Z}^{(N)}$ the subgroup of sequences for which $a_i = 0$ for all but finitely many $i$. Define $\mathbb{Q}^N$ and $\mathbb{Q}^{(N)}$ analogously. Compare $\mathbb{Z}^{(N)} \otimes \mathbb{Q}$ to $\mathbb{Q}^{(N)}$, and $\mathbb{Z}^N \otimes \mathbb{Q}$ to $\mathbb{Q}^N$.

3. In this problem, $G$ denotes the group $S_5 \times C_2$, where $S_5$ is the symmetric group on five letters and $C_2$ is the cyclic group of order 2.

(a) Determine all normal subgroups of $G$.

(b) Give an example of a polynomial with rational coefficients whose Galois group is $G$, deducing that from basic principles.

4. Let $Q$ denote the finite group of quaternions, with presentation

$$Q = \{t, s_i, s_j, s_k \mid t^2 = 1, s_i^2 = s_j^2 = s_k^2 = s_i s_j s_k = t\}.$$ 

(a) Determine four non-isomorphic representations of $Q$ of dimension 1 over $\mathbb{R}$.

(b) Show that the natural embedding of $Q$ into the algebra $\mathbb{H}$ of real quaternions ($t \mapsto -1$, $s_i \mapsto i$, $s_j \mapsto j$, $s_k \mapsto k$) defines an irreducible real representation of $Q$, of dimension 4 over $\mathbb{R}$.

(c) Determine all irreducible representations of $Q$ over $\mathbb{C}$ (up to isomorphism).

5. (a) Give the definition of a Dedekind domain.

(b) Give an example of a Dedekind domain that is not a principal ideal domain. Verify from the definition that it is a Dedekind domain, and also that it isn’t a principal ideal domain.
1. a) Let $G$ be a group of order 5046. Show that $G$ cannot be a simple group. You may not appeal to the classification of finite simple groups.

b) Let $p$ and $q$ be prime numbers. Show that any group of order $p^2q$ is solvable.

2. Consider the special orthogonal group $G = SO(3, \mathbb{R})$, namely,

$$G = \{ A \in GL(3, \mathbb{R}) : A^T A = I_3, \ det(A) = 1 \}$$

(a) Show that for any element $A$ in $G$, there exists a real number $\alpha$ with $-1 \leq \alpha \leq 3$ such that

$$A^3 - \alpha A^2 + \alpha A - I_3 = 0.$$

(b) For which real numbers $\alpha$ with $-1 \leq \alpha \leq 3$ does there exist an element $A$ in $G$ whose minimal polynomial is $x^3 - \alpha x^2 + \alpha x - 1$? Explain your answer.

3. Let $G$ be a cyclic group of order 100. Let $K = \mathbb{Q}$, the field of rational numbers, or $K = F_p$, the finite field with $p$ elements, $p$ being a prime number. For each such $K$, construct a Galois extension $L/K$ whose Galois group $Gal(L/K)$ is isomorphic to $G$. Explain your construction in detail.

4. Let $\rho : S_3 \to \mathbb{C}^2$ be a two-dimensional irreducible representation of the symmetric group $S_3$. Decompose $\rho^\otimes 2$ and $\rho^\otimes 3$ into a direct sum of irreducible representations of $S_3$.

5. Let $A$ be a finite-dimensional semisimple algebra over $\mathbb{C}$, and $V$ an $A$-module of finite type (i.e., finitely-generated as an $A$-module). Prove that $V$ has only finitely many $A$-submodules if and only if $V$ is a direct sum of pairwise non-isomorphic irreducible (i.e., simple) $A$-modules.
1. (a) Let $H$ be a subgroup of a finite group $G$ with $H \neq \{1\}$ and $H \neq G$. Prove that $G$ is not the union of all the conjugates of $H$ in $G$.

(b) Give an example of an infinite group $G$ for which the assertion in part (a) is false.

2. Let $p$ be a prime, $F$ a finite field with $p$ elements and $K$ a finite extension of $F$. Denote by $F^\times$ and $K^\times$ the multiplicative groups of nonzero elements of fields $F$ and $K$, respectively. Prove that the norm homomorphism $N : K^\times \to F^\times$ is surjective.

3. Determine the Galois group [up to isomorphism] of the splitting field of each of the following polynomials over $\mathbb{Q}$:

(a) $f(x) = x^4 - 9x^3 + 9x + 4$,

(b) $g(x) = x^5 - 6x^2 + 2$.

4. Let $F$ be a field, and $V$ a finite-dimensional vector space over $F$, with $\dim_F V = n$.

(a) Prove that if $n > 2$, the spaces $\Lambda^2(\Lambda^2(V))$ and $\Lambda^4(V)$ are not isomorphic.

(b) Let $k$ be a positive integer. Prove that when $v \in \Lambda^k(V)$ and $0 \neq x \in V$, $v \wedge x = 0$ holds if and only if $v = x \wedge y$ for some $y \in \Lambda^{k-1}(V)$.

5. Let $K$ be a field, and $\Phi : G \to GL_n(K)$ an $n$-dimensional matrix representation of the group $G$. Define an action of $G$ on the full matrix ring $M_n(K)$ by $(g, A) \mapsto \Phi(g) \cdot A$ when $g \in G$ and $A \in M_n(K)$ (that’s a matrix product on the right-hand side). This in turn induces a group homomorphism $\Psi : G \to GL(M_n(K))$. Express the character $\chi(\Psi)$ of $\Psi$ in terms of $\chi(\Phi)$.
Algebra Qualifying Exam   Fall 2010

September 6, 2010   (150 minutes)

Do all problems. All problems are equally weighted. Show all work.

1. Let $G$ be a group. Let $H$ be a subset of $G$ that is closed under group multiplication. Assume that $g^2 \in H$ for all $g \in G$. Show that $H$ is a normal subgroup of $G$ and $G/H$ is abelian.

2. (a) Find the complete factorization of the polynomial $f(x) = x^6 - 17x^4 + 80x^2 - 100$ in $\mathbb{Z}[x]$.
   (b) For which prime numbers $p$ does $f(x)$ have a root in $\mathbb{Z}/p\mathbb{Z}$ (i.e, $f(x)$ has a root modulo $p$)? Explain your answer.

3. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$ and $F = \mathbb{Q}(\sqrt{-2})$. Show that $K$ is Galois over $F$ and determine the Galois group $\text{Gal}(K/F)$.

4. Let $A$ be a commutative Noetherian local ring with maximal ideal $m$. Assume $m^n = m^{n+1}$ for some $n > 0$. Show that $A$ is Artinian.

5. Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements. Here $p$ is a prime number. Let $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ be given by $\varphi(x) = x^p$.
   (a) Show that $\varphi$ is a linear transformation on $\mathbb{F}_q$ (as vector space over $\mathbb{F}_p$), then determine its minimal polynomial.
   (b) Supposed that $\varphi$ is diagonalizable over $\mathbb{F}_p$. Show that $n$ divides $p - 1$.

6. Let $G$ be a non-abelian group of order $p^3$. Here $p$ is a prime number.
   (a) Determine the number of (isomorphic classes of) irreducible complex representations of $G$, and find their dimensions.
   (b) Which of the irreducible complex representations of $G$ are faithful? Explain your answer.
Do all problems. All problems are equally weighted. Show all work.

1. Let \( G \) be a non-abelian group of order \( p^3 \), here \( p \) is prime. Determine the number of distinct conjugacy classes in \( G \).

2. Let \( R \) be a ring such that \( r^3 = r \) for all \( r \in R \). Show that \( R \) is commutative. (Hint: First show that \( r^2 \) is central for all \( r \in R \).)

3. Compute Galois groups of the following polynomials.
   (a). \( x^3 + t^2 x - t^3 \) over \( k \), where \( k = \mathbb{C}(t) \) is the field of rational functions in one variable over complex numbers \( \mathbb{C} \).
   (b). \( x^4 - 14x^2 + 9 \) over \( \mathbb{Q} \).

4. Let \( V \) be a \( n \)-dimensional vector space over a field \( k \). Let \( T \in End_k(V) \).
   (a). Show that \( tr(T \otimes T \otimes T) = (tr(T))^3 \). Here \( tr(T) \) is the trace of \( T \).
   (b). Find a similar formula for the determinant \( det(T \otimes T \otimes T) \).

5. Classify all non-commutative semi-simple rings with 512 elements. (You can use the fact that finite division rings are fields.)

6. Let \( G \) be a group with 24 elements. Use representation theory to show that \( G \neq [G, G] \). (Here \( [G, G] \) is the commutator subgroup of \( G \).)
Algebra Qualifying Exam  Fall 2009
September 9, 2009  (150 minutes)

Do all problems. All problems are equally weighted. Show all work.

1. Let $G$ be a finite group. Let $Aut(G)$ be the group of automorphisms of $G$. Consider the group action $\phi : Aut(G) \times G \to G$ where $\phi(\sigma, g) = \sigma(g)$. Assume $G$ has exactly two orbits under the action of $Aut(G)$.
   (a). Determine all such $G$, up to isomorphism.
   (b). List all cases in which $Aut(G)$ is a solvable group.

2. Consider $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} | a, b \in \mathbb{Q}\}$. Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{5}]$.

3. Determine the Galois group of $x^4 - 4x^2 + 7x - 3$ over $\mathbb{Q}$.

4. Let $E$ and $F$ be finite field extensions of a field $k$ such that $E \cap F = k$, and that $E$ and $F$ are both contained in a larger field $L$. Assume that $E$ is Galois over $k$. Show that $E \otimes_k F \cong EF$.

5. Let $A, B$ be two Noetherian local rings with maxima ideals $m_A, m_B$, respectively. Let $f : A \to B$ be a ring homomorphism such that $f^{-1}(m_B) = m_A$. Assume that:
   1. $A/m_A \to B/m_B$ is an isomorphism.
   2. $m_A \to m_B/m_B^2$ is surjective.
   3. $B$ is a finitely generated $A$-module (via $f$).
   Show that $f$ is surjective.

6. Let $\rho : G \to GL_n(\mathbb{C})$ be a complex irreducible representation of a finite group $G$. Let $\chi$ be its associated character and let $C$ be the center of $G$.
   (a). Show that, for all $s \in C$, $\rho(s)$ is a scalar multiple of the identity matrix $I_n$.
   (b). Use (a) to show that $|\chi(s)| = n$, for all $s \in C$.
   (c). Prove the inequality $n^2 \leq [G : C]$, where $[G : C]$ denotes the index of $C$ in $G$.
   (d). Show that, if $\rho$ is faithful (i.e., an injective group homomorphism), then $C$ is cyclic.
1. Let $H$ and $K$ be two solvable subgroups of a group $G$ such that $G = HK$.
   (a). Show that if either $H$ or $K$ is normal in $G$, then $G$ is solvable.
   (b). Give an example that $G$ may not be solvable without the assumption in (a).

2. Consider $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where $\omega$ is a non-trivial cube root of 1. Show that $\mathbb{Z}[\omega]$ is an Euclidean domain.

3. Consider the field $K = \mathbb{Q}(\sqrt{a})$ where $a \in \mathbb{Z}$, $a < 0$. Show that $K$ cannot be embedded in a cyclic extension whose degree over $\mathbb{Q}$ is divisible by 4.

4. Let $E$ be a finite-dimensional vector space over an algebraically closed field $k$. Let $A, B$ be $k$-endomorphisms of $E$. Assume $AB = BA$. Show that $A$ and $B$ have a common eigenvector.

5. Consider the $\mathbb{Z}$-modules $M_i = \mathbb{Z}/2^i\mathbb{Z}$ for all positive integers $i$. Let $M = \prod_{i=1}^{\infty} M_i$. Let $S = \mathbb{Z} - \{0\}$.
   (a). Show that $\mathbb{Q} \otimes_{\mathbb{Z}} M \cong S^{-1}M$.
   Here $S^{-1}M$ is the localization of $M$.
   (b). Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{i=1}^{\infty} M_i \neq \prod_{i=1}^{\infty} (\mathbb{Q} \otimes_{\mathbb{Z}} M_i)$.

   (a). How many simple characters over $\mathbb{C}$ does $H$ have?
   (b). Choose a non-trivial simple character $\psi$ of $H$ over $\mathbb{C}$ such that $\psi((12)(34)) = -1$. Compute the values of the induced character $\text{ind}^G_H(\psi)$ on conjugacy classes of $G$, then write the induced character as sum of simple characters.
Do all problems. All problems are equally weighted. Show all work.

1. Show that no group of order 36 is simple.

2. Show that the polynomial \( x^5 - 5x^4 - 6x - 2 \) is irreducible in \( \mathbb{Q}[x] \).

3. Let \( k \) be a finite field and \( K \) be a finite extension of \( k \). Let \( \text{Tr} = Tr_k^K \) be the trace function from \( K \) to \( k \). Determine the image of \( \text{Tr} \) and prove your answer.

4. A differentiation of a ring \( R \) is a mapping \( D : R \to R \) such that, for all \( x, y \in R \),
   \begin{enumerate}
   
   \item \( D(x + y) = D(x) + D(y) \); and
   \item \( D(xy) = D(x)y + xD(y) \).
   \end{enumerate}

   If \( K \) is a field and \( R \) is a \( K \)-algebra, then its differentiation are supposed to be over \( K \), that is,

   \begin{enumerate}
   \item \( D(x) = 0 \) for any \( x \in K \).
   \end{enumerate}

   Let \( D \) be a differentiation of the \( K \)-algebra \( M_n(K) \) of \( n \times n \)-matrices. Prove that there exists a matrix \( A \in M_n(K) \) such that \( D(X) = AX -XA \) for all \( X \in M_n(K) \).

5. For each \( n \in \mathbb{Z} \), define the ring homomorphism
   \[ \phi_n : \mathbb{Z}[x] \to \mathbb{Z} \text{ by } \phi_n(f) = f(n). \]

   This gives a \( \mathbb{Z}[x] \)-module structure on \( \mathbb{Z} \), i.e,

   \[ f \circ a = f(n) \cdot a \text{ for all } f \in \mathbb{Z}[x] \text{ and } a \in \mathbb{Z}. \]

   Now given two integers \( m, n \in \mathbb{Z} \), compute the tensor product \( \mathbb{Z} \otimes_{\mathbb{Z}[x]} \mathbb{Z} \) where the left-hand copy of \( \mathbb{Z} \) uses the module structure from \( \phi_n \) and the right-hand copy of \( \mathbb{Z} \) uses the module structure from \( \phi_m \). (Note: The answer depends on the numbers \( n \) and \( m \).)

6. Let \( R \) be a semi-simple finite dimensional algebra over complex numbers \( \mathbb{C} \). Let \( M \) be an \( R \)-module such that \( M = E \oplus E \). Here \( E \) is a simple \( R \)-module. Show that \( \text{Aut}_R(M) \cong GL_2(\mathbb{C}) \).
Do all problems. All problems are equally weighted. Show all work.

1. Let $k$ be a field. Consider the subgroup $B \subset \text{GL}_2(k)$ where

$$B = \{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in k, \ ad \neq 0 \}.$$

(a). Let $Z$ be the center of $\text{GL}_2(k)$. Show that

$$\bigcap_{x \in \text{GL}_2(k)} x^{-1}Bx = Z.$$ 

(b). Assume $k$ is algebraically closed. Show that

$$\bigcup_{x \in \text{GL}_2(k)} x^{-1}Bx = \text{GL}_2(k).$$

(c). Assume $k$ is a finite field. Can the statement in (b) still be true?

2. Let $\xi$ be a primitive 9-th root of unity. Find the minimal polynomial of $\xi + \xi^{-1}$ over $\mathbb{Q}$.

3. Let $K$ be the splitting field of the polynomial $X^4 - 6X^2 - 1$ over $\mathbb{Q}$.

(a). Compute $\text{Gal}(K/\mathbb{Q})$.

(b). Determine all intermediate fields that are Galois over $\mathbb{Q}$.

4. Let $V \cong \mathbb{C}^n$ be an $n$-dimensional complex vector space with the standard basis $e_1, \ldots, e_n$. Consider the permutation group action $S_n \times V \to V$ where $\sigma(e_i) = e_{\sigma(i)}$. Decompose $V$ into simple $\mathbb{C}[S_n]$-modules.

5. Let $k$ be a field of characteristic zero. Assume that $E$ and $F$ are algebraic extensions of $k$ and both contained in a larger field $L$. Show that the $k$-algebra $E \otimes_k F$ has no nonzero nilpotent elements.

6. Give an example of non-isomorphic finite groups with same character table. Construct the character table in detail.
Algebra Qualifying Exam, Fall, 2007

Sept 11, 2007, 2:00-4:30

1. Let $G$ be a cyclic group of order 12. Construct a Galois extension $K$ over $\mathbb{Q}$ so that the Galois group is isomorphic to $G$.

2. Prove that no group of order 148 is simple.

3. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a real matrix such that $a, b, c, d > 0$. (1) Prove that $A$ has two distinct real eigenvalues, $\lambda > \mu$. (2) Prove that $\lambda$ has an eigenvector in the first quadrant and $\mu$ has an eigenvector in the second quadrant.

4. A differentiation of a ring $R$ is a mapping $D : R \to R$ such that, for all $x, y \in R$,
   
   (1) $D(x + y) = D(x) + D(y)$; and
   
   (2) $D(xy) = D(x)y + xD(y)$.

   If $K$ is a field and $R$ is a $K$-algebra, then its differentiation are supposed to be over $K$, that is,

   (3) $D(x) = 0$ for any $x \in K$.

   Let $D$ be a differentiation of the $K$-algebra $M_n(K)$ of $n \times n$-matrices. Prove that there exists a matrix $A \in M_n(K)$ such that $D(X) = AX -XA$ for all $X \in M_n(K)$.

5. Prove the existence of a 1-dimensional invariant subspace for any 5-dimensional representation of the group $A_4$ (the alternating group of degree 4).
1. Prove that the integer orthogonal group $O_n(\mathbb{Z})$ is a finite group. (By definition, an $n \times n$ square matrix $X$ over $\mathbb{Z}$ is orthogonal if $XX^t = I_n$.)

2. Prove that no group of order 224 is simple.

3. Write down the irreducible polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ and prove that it is reducible modulo $p$ for every prime $p$.

4. Find the invertible elements, the zero divisors and the nilpotent elements in the following rings:
   (a) $\mathbb{Z}/p^n\mathbb{Z}$, where $n$ is a natural number, $p$ is a prime one.

   (b) the upper triangular matrices over a field.

5. Prove that the group $GL(2, \mathbb{C})$ does not contain a subgroup isomorphic to $S_4$. 
Do all problems. All problems are equally weighted. Show all work.

1. Let $SL_n(k)$ be the special linear group over a field $k$, i.e, $n \times n$ matrices with determinant 1. Let $I$ be the identity matrix, and $E_{ij}$ be the elementary matrix that has 1 at $(i, j)$-entry and 0 elsewhere. Here $1 \leq i \neq j \leq n$.
   (1). Let $C_{ij}$ be the centralizer of the matrix $I + E_{ij}$. Find explicit generators of $C_{ij}$.
   (2). Find the intersection $\bigcap_{1 \leq i \neq j \leq n} C_{ij}$.
   (3). Determine all the elements in the conjugacy class of $I + E_{ij}$.

2. Let $f$ be a polynomial in $\mathbb{Q}[x]$. Let $E$ be a splitting field of $f$ over $\mathbb{Q}$. For the following cases, determine whether $E$ is solvable by radicals.
   (1). $f(x) = x^4 - 4x + 2$.
   (2). $f(x) = x^5 - 4x + 2$.

3. Let $A$ be a principal integral domain and $K$ be its field of fractions. Assume that $R$ is a ring such that $A \subset R \subset K$. Show that $R$ is also a principal integral domain.

4. Let $R$ be a commutative ring. Let $M$ be an $R$-module.
   (1). Write down the definition of $T(M)$, the tensor algebra of $M$.
   (2). Assume $R = \mathbb{Z}$ and $M = \mathbb{Q}/\mathbb{Z}$. Compute $T(M)$.
   (3). If $M$ is a vector space over a field $R$, show that $T(M)$ contains no zero divisors.

5. Let $A$ be an invertible $n \times n$ matrix over complex numbers $\mathbb{C}$. Show that $A$ has a square root, i.e, there exists a $n \times n$ matrix $B$ such that $A = B^2$.

6. Let $R$ be a semi-simple finite dimensional algebra over complex numbers $\mathbb{C}$. Let $M$ be an $R$-module such that $M = E \oplus E$. Here $E$ is a simple $R$-module. Show that $\text{Aut}_R(M) \cong GL_2(\mathbb{C})$. 

Algebra Qualifying Exam    Spring 2006
May 24, 2006    (150 minutes)

Do all problems. All problems are equally weighted. Show all work.

1. Let $\mathbb{F}_p$ be the field with $p$ elements, here $p$ is prime. Let $SL_2(\mathbb{F}_p)$ be the group of 2x2 matrices over $\mathbb{F}_p$ with determinant 1.
   (1). Find the order of $SL_2(\mathbb{F}_p)$. Deduce that $H = \{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} | a \in \mathbb{F}_p \}$ is a Sylow-subgroup of $SL_2(\mathbb{F}_p)$.
   (2). Determine the normalizer of $H$ in $SL_2(\mathbb{F}_p)$ and find its order.

2. Let $R$ be a ring with identity 1. Let $x, y \in R$ such that $xy = 1$.
   (1). Assume $R$ has no zero-divisor. Show that $yx = 1$.
   (2). Assume $R$ is finite. Show that $yx = 1$.

3. Let $V$ be a $n$-dimensional vector space over a field $k$, with a basis $\{e_1, \ldots, e_n\}$. Let $A$ be the ring of all $n \times n$ diagonal matrices over $k$. $V$ is a $A$-module under the action:
   \[
   \text{diag}(\lambda_1, \ldots, \lambda_n) \cdot (a_1 e_1 + \cdots + a_n e_n) = (\lambda_1 a_1 e_1 + \cdots + \lambda_n a_n e_n).
   \]
   Find all $A$-submodules of $V$.

4. Let $k$ be a field. Let $p$ be a prime number. Let $a \in k$. Show that the polynomial $x^p - a$ either has a root in $k$ or is irreducible in $k[x]$.

5. Let $V$ be a finite-dimensional vector space over a field $k$. Let $T \in \text{End}_k(V)$. Show that $tr(T \otimes T) = (tr(T))^2$. Here $tr(T)$ is the trace of $T$.

6. Let $S_4$ be the symmetric group of 4 elements.
   (1). Give an example of non-trivial 8-dimensional representation of the group $S_4$.
   (2). Show that for any 8-dimensional complex representation of $S_4$, there exists a 2-dimensional invariant subspace.
1. Let $K$ be a finite field with $q$ elements. Let $n > 0$ be a positive integer. Compute the sum
$$\sum_{x \in K} x^n.$$ 

2. Let $K$ be the splitting field (in $\mathbb{C}$) of the polynomial $x^4 - 3x^2 + 5$ over $\mathbb{Q}$.
   (1). Determine $\text{Gal}(K/\mathbb{Q})$.
   (2). Find all intermediate fields $\mathbb{Q} \subset E \subset K$ such that $E$ is Galois over $\mathbb{Q}$.

3. Let $k \subset E$ be an algebraic extension of fields of characteristic zero. Assume that every non-constant polynomial $f(x) \in k[x]$ has a root in $E$. Show that $E$ is algebraically closed.

4. Let $R$ be a commutative ring. Let $I$ be a finitely generated ideal. Assume that $I^2 = I$. Show that $I$ is a direct summand of $R$.

5. Let $\mathbb{C}$ and $\mathbb{R}$ be complex and real number fields. Let $\mathbb{C}(x)$ and $\mathbb{C}(y)$ be function fields of one variable. Consider $\mathbb{C}(x) \otimes_{\mathbb{R}} \mathbb{C}(y)$ and $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$.
   (1). Determine if they are integral domains.
   (2). Determine if they are fields.

6. Let $E$ be a finite-dimensional vector space over a field $k$. Assume $S, T \in \text{End}_k(E)$. Assume $ST = TS$ and both of them are diagonalizable. Show that there exists a basis of $E$ consisting of eigenvectors for both $S$ and $T$. 
Do all 6 problems. All problems are equally weighted. Show all details in your proofs.

1. Let $k$ be a field. Let $G = GL_n(k)$ be the general linear group. Here $n > 0$. Let $D$ be the subgroup of diagonal matrices. Let $N = N_G(D)$ be the normalizer of $D$. Determine the quotient group $N/D$.

2. Let $F_p$ be the field with $p$ elements, where $p$ is a prime number. Let $f_{n,p}(x) = x^{p^n} - x + 1$, and suppose that $f_{n,p}(x)$ is irreducible in $F_p[x]$. Let $\alpha$ be a root of $f_{n,p}(x)$.
   (a) Show that $F_p^n \subset F_p(\alpha)$ and $[F_p(\alpha) : F_p^n] = p$.
   (b) Determine all pairs $(n, p)$ for which $f_{n,p}(x)$ is irreducible.

3. Let $\xi$ be a primitive $p^n$-th root of unity. Here $p$ is prime and $n > 0$. Let $f(x)$ be the minimal polynomial of $\xi$ over $\mathbb{Q}$, and let $m$ be its degree.
   (a) Determine $f(x)$.
   (b) Let $\alpha_1, \ldots, \alpha_m$ be all the roots of $f(x)$. Define the discriminant of $\xi$ as:
      $$D(\xi) = [\det(\alpha_i^{-1})_{ij}]^2, \quad i, j = 1, \ldots, m.$$  
      Show that $D(\xi) = (-1)^{\frac{m(m-1)}{2}} N_{\mathbb{Q}}(\xi)(f'(\xi))$.
   (c) Take $n = 2$. Compute $D(\xi)$ in this case.

4. Let $R$ be a ring. Let $L$ be a minimal left ideal of $R$ (i.e., $L$ contains no nonzero proper left ideal of $R$). Assume $L^2 \neq 0$. Show that $L = Re$ for some non-zero idempotent $e \in R$.

5. Let $A$ be an integral domain and let $K$ be its field of fractions. Let $A'$ be the integral closure of $A$ in $K$. Let $P \subset A$ be a prime ideal and let $S = A - P$. (Note that $A_P = S^{-1}A$ is contained in $K$.) Show that $A_P$ is integrally closed in $K$ if and only if $(A'/A) \otimes_A A_P = 0$.

6. Let $V$ be a finite dimensional vector space over a field $k$. Let $G$ be a finite group. Let $\varphi : G \rightarrow GL(V)$ be an irreducible representation of $G$. Suppose that $H$ is a finite abelian subgroup of $GL(V)$ such that $H$ is contained in the centralizer of $\varphi(G)$. Show that $H$ is cyclic.
Do all problems. All problems are equally weighted. Show all details.

1. Let \( H \) be a proper subgroup of a finite group \( G \). Show that \( G \) is not the union of all the conjugates of \( H \).

2. Let \( \mathfrak{N} \) be the set of all nilpotent elements in a ring \( R \). Assume first that \( R \) is commutative.
   (a) Show that \( \mathfrak{N} \) is an ideal in \( R \), and \( R/\mathfrak{N} \) contains no non-zero nilpotent elements.
   (b) Show that \( \mathfrak{N} \) is the intersection of all the prime ideals of \( R \).
   (c) Give an example with \( R \) non-commutative where \( \mathfrak{N} \) is not an ideal in \( R \).

3. Let \( f(x) = x^5 - 9x + 3 \). Determine the Galois group of \( f \) over \( \mathbb{Q} \).

4. Let \( \lambda_1, \ldots, \lambda_n \) be roots of unity, with \( n \geq 2 \). Assume that \( \frac{1}{n} \sum_{i=1}^{n} \lambda_i \) is integral over \( \mathbb{Z} \). Show that either \( \sum_{i=1}^{n} \lambda_i = 0 \) or \( \lambda_1 = \lambda_2 = \cdots = \lambda_n \).

5. Consider the ideal \( I = (2, x) \) in \( R = \mathbb{Z}[x] \).
   (a) Construct a non-trivial \( R \)-module homomorphism \( I \otimes_R I \to R/I \), and use that to show that \( 2 \otimes x - x \otimes 2 \) is a non-zero element in \( I \otimes_R I \).
   (b) Determine the annihilator of \( 2 \otimes x - x \otimes 2 \).

6. Let \( D_8 \) be the dihedral group of order 8, given by generators and relations
   \[
   < r, s \mid r^4 = 1 = s^2, \; rs = sr^{-1} >
   \]
   (a) Determine the conjugacy classes of \( D_8 \).
   (b) Determine the commutator subgroup \( D'_8 \) of \( D_8 \). Determine the number of distinct degree one characters of \( D_8 \).
   (c) Write down the complete character table of \( D_8 \).
Do all 6 problems. All problems are equally weighted. Show all details in your solutions.

Notation: $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields of rational, real and complex numbers.

1. Let $\mathbb{F}_2$ be the finite field with 2 elements.
   (a) What is the order of $GL_3(\mathbb{F}_2)$, the group of $3 \times 3$ invertible matrices over $\mathbb{F}_2$?
   (b) Assuming the fact that $GL_3(\mathbb{F}_2)$ is a simple group, find the number of elements of order 7 in $GL_3(\mathbb{F}_2)$.

2. Let $K \subseteq \mathbb{C}$ be the splitting field of $f(x) = x^6 + 3$ over $\mathbb{Q}$. Let $\alpha$ be a root of $f(x)$ in $K$.
   (a) Show that $K = \mathbb{Q}(\alpha)$.
   (b) Determine the Galois group $\text{Gal}(K/\mathbb{Q})$.

3. Let $k$ be a field with characteristic 0. Let $m \geq 2$ be an integer. Show that $f(x, y) = x^m + y^m + 1$ is irreducible in $k[x, y]$.

4. Let $k$ be a field. Consider the integral domain $R = k[x, y]/(x^2 - y^2 + y^3)$.
   (a) Show that $R$ is not a unique factorization domain.
   (b) Let $F$ be the field of fractions of $R$. Find $t \in F$ such that $F = k(t)$.
   (c) Determine the integral closure of $R$ in $F$.

5. Show that there is a $\mathbb{C}$-algebra isomorphism between $\mathbb{C} \otimes_\mathbb{R} \mathbb{C}$ and $\mathbb{C} \times \mathbb{C}$.

6. Consider complex representations of a finite group $G$. Let $\sigma_1 \ldots \sigma_s$ be representatives from the conjugacy classes of $G$, and let $\chi_1 \ldots \chi_s$ be all the different simple characters of $G$.
   (a) Define an inner product on the $\mathbb{C}$-space of class functions on $G$, so that $\{\chi_1 \ldots \chi_s\}$ forms an orthogonal basis for this space.
   (b) Let $A = (a_{ij})$ be the matrix of the character table of $G$, i.e., $a_{ij} = \chi_i(\sigma_j)$ $(1 \leq i, j \leq s)$. Show that $A$ is invertible.
Qualifying Exam in Algebra, Fall 2003

**Directions:** This is a closed book exam. You have two hours to do all five of the (equally weighted) problems.

1. In a group $G$, let $1$ denote the identity element and let $[x, y] = xyx^{-1}y^{-1}$ denote the commutator of the elements $x, y \in G$.
   a) Express $[z, xy]x$ in terms of $x$, $[z, x]$ and $[z, y]$.
   b) Prove that if the identity $[[x, y], z] = 1$ holds in a group $G$, then the identities

   $$[x, yz] = [x, y][x, z] \quad \text{and} \quad [xy, z] = [x, z][y, z]$$

   hold in $G$.

2. Let $k$ be a field of characteristic $p$ and let $t, u$ be algebraically independent over $k$. Prove the following:
   a) $k(t, u)$ has degree $p^2$ over $k(t^p, u^p)$.
   b) There exist infinitely many fields between $k(t, u)$ and $k(t^p, u^p)$.

3. Obtain a factorization into irreducible factors in $\mathbb{Z}[x]$ of the polynomial $x^{10} - 1$.

4. Verify the isomorphism of algebras over a field $K$:

   $$\mathbb{M}_n(K) \otimes_K \mathbb{M}_m(K) \simeq \mathbb{M}_{mn}(K).$$

   [Note: $\mathbb{M}_n(K)$ denotes the algebra of $n \times n$ matrices over $K$.]

5. Let $S_4$ be the symmetric group on 4 elements.
   a) Give an example of a non-trivial 8-dimensional representation of the group $S_4$.
   b) Prove for any 8-dimensional complex representation of $S_4$ the existence of a 2-dimensional invariant subspace.
1. Show that every group of order $p^2$, $p$ a prime, is Abelian. Show that up to isomorphism there are only two such groups.

2. Let $K$ be a field. A polynomial $f(x) \in K[x]$ is called separable if, in any field extension, it has distinct roots. Prove that:
   (a) if $K$ has characteristic 0, then each irreducible polynomial in $K[x]$ is separable;
   and
   (b) if $K$ has characteristic $p \neq 0$, then an irreducible polynomial $f(x) \in K[x]$ is separable if and only if has no form $g(x^p)$ where $g(x) \in K[x]$.
   Give an example of an inseparable irreducible polynomial.

3. Prove that if a linear operator on a complex vector space is diagonal in some basis, then its restriction on any invariant subspace $L$ is also diagonal in some basis of $L$.

4. A differentiation of a ring $R$ is a mapping $D : R \rightarrow R$ such that, for all $x, y \in R$,
   (1) $D(x + y) = D(x) + D(y)$; and
   (2) $D(xy) = D(x)y + xD(y)$.
   If $K$ is a field and $R$ is a $K$-algebra, then its differentiation are supposed to be over $K$, that is,
   (3) $D(x) = 0$ for any $x \in K$.

   Let $D$ be a differentiation of the $K$-algebra $M_n(K)$ of $n \times n$-matrices. Find a matrix $A \in M_n(K)$ such that $D(X) = AX - XA$ for all $X \in M_n(K)$.

5. Prove the existence of a 1-dimensional invariant subspace for any 5-dimensional representation of the group $A_4$ (the alternating group of degree 4).
Algebra Core Qualifying Exam, September, 2002

Notation: Integers: \( \mathbb{Z} \), the integers modulo \( p \): \( \mathbb{Z}/(p) \), rationals: \( \mathbb{Q} \).

(1) (3 points) Let \( H \) be a subgroup of \( G \) with \( a, b \in G \). Prove (without assuming very much) that the right cosets \( Ha \) and \( Hb \) are either equal or disjoint.

(2) (3 points) Prove that if \( H \) is a subgroup of index 2 in \( G \) then \( H \) is normal in \( G \).

(3) (3 points) Working over the integers, calculate (and show your work in a readable fashion) \( \text{Tor}(\mathbb{Z}/(p), \mathbb{Z}/(p)) \).

(4) (3 points) Working over the integers, calculate (and show your work in a readable fashion) \( \text{Ext}(\mathbb{Z}/(p), \mathbb{Z}/(p)) \).

(5) (6 points) Recall \( D_4 = \{1, a, a^2, a^3, ba, ba^2, ba^3\} \), \( |a|=4 \), \( |b|=2 \), \( aba=b \). Find the center of \( D_4 \), \( Z(D_4) \), and describe \( D_4/Z(D_4) \).

(6) (3 points) Calculate all the group homomorphisms from \( S_3 \), the symmetric group on 3 elements, to \( \mathbb{Z}/(2) \times \mathbb{Z}/(2) \). Explain your answer.

(7) (1 point) How many monic polynomials of degree 3 are there over \( \mathbb{Z}/(3) \)?

(8) (3 points) How many irreducible monic polynomials of degree 3 are there over \( \mathbb{Z}/(3) \).

(9) (5 points) For every monic polynomial, \( f(x) \), in problem \# 7, we can define the quotient ring \( \mathbb{Z}/(3)[x]/(f(x)) \). How many different rings do we get if we use only the monic polynomials of problem \# 8? Explain your answer and identify your answers as familiar rings.

(10) (3 points) Find all the idempotents not equal to 0 or 1 in the ring \( \mathbb{Z}/(2)[x]/(x^3+1) \).

(11) (4 points) Find the minimal polynomial for \( \sqrt{2}+i \) over \( \mathbb{Q} \).

(12) (10 points) Demonstrate your knowledge of Galois theory for the field extension \( \mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+i) \) (in the complex numbers).

(13) (3 points) Prove Cauchy's theorem that if a prime \( p \) divides the order of a group, \( |G| \), then \( G \) has an element of order \( p \). (You can assume the result for Abelian groups.)

(14) (3 points) Give all groups of order 175. Two are pretty easy, it is the rest I care about. Explain your answer.
1. How many elements of order 7 are there in a simple group of order 168?

2. Let $m$ be an integer $\geq 2$ and $\mathbb{Z}[X]$ be the polynomial ring over $\mathbb{Z}$. Find a condition on $m$ so that the ideal $(m, X)$ in the ring is maximal.

3. Prove that the group of automorphisms of the field $\mathbb{R}$ of real numbers is trivial.

4. For a field $K$, let $SL_2(K)$ be the special linear group over $K$, i.e. the group of $2 \times 2$–matrices over $K$ with determinant 1, and let $PSL_2(K)$ be the quotient of $SL_2(K)$ by its center, i.e. the projective special linear group. Find the order of $PSL_2(F_7)$ where $F_7$ denotes the finite field of 7 elements.

5. Let $\zeta = e^{\frac{2\pi i}{5}}$ and $K = \mathbb{Q}(\zeta)$ the field generated by $\zeta$ over the field of rational numbers. Prove that $K$ contains $\sqrt{5}$. 
Directions: Solve four problems from the following list of five and clearly indicate which problems you chose as only those will be graded. Show all your work. In general, it is permissible to use earlier parts of a problem in order to solve a later part even if you have not solved the earlier parts.

1. Let $G$ be a finite group and let $N$ be a normal subgroup of $G$ such that $N$ and $G/N$ have relatively prime orders. 
(a) Assume that there exists a subgroup $H$ of $G$ having the same order as $G/N$. Show that $G = HN$. (Here $HN$ denotes the set $\{xy \mid x \in H, y \in N\}$.)
(b) Show that $\phi(N) = N$, for all automorphisms $\phi$ of $G$.

2. Let $S$ denote the ring $\mathbb{Z}[X]/X^2\mathbb{Z}[X]$, where $X$ is a variable.
(a) Show that $S$ is a free $\mathbb{Z}$–module and find a $\mathbb{Z}$–basis for $S$.
(b) Which elements of $S$ are units (i.e. invertible with respect to multiplication)?
(c) List all the ideals of $S$.
(d) Find all the nontrivial ring morphisms defined on $S$ and taking values in the ring of Gaussian integers $\mathbb{Z}[i]$.

3. Assume that $A$ is an $n \times n$ matrix with entries in the field of complex numbers $\mathbb{C}$ and $A^m = 0$ for some integer $m > 0$.
(a) Show that if $\lambda$ is an eigenvalue of $A$, then $\lambda = 0$.
(b) Determine the characteristic polynomial of $A$.
(c) Prove that $A^n = 0$.
(d) Write down a $5 \times 5$ matrix $B$ for which $B^3 = 0$ but $B^2 \neq 0$.
(e) If $M$ is any $5 \times 5$ matrix over $\mathbb{C}$ with $M^3 = 0$ and $M^2 \neq 0$, must $M$ be similar to the matrix $B$ you found in part (d)? Justify your answer.

4. Let $K := \mathbb{Q}(\sqrt{3} + \sqrt{5})$.
(a) Show that $K$ is the splitting field of $X^4 - 6X^2 + 4$.
(b) Find the structure of the Galois group of $K/\mathbb{Q}$.
(c) List all the fields $k$, satisfying $\mathbb{Q} \subseteq k \subseteq K$.

5. Let $\rho : G \to \text{GL}_n(\mathbb{C})$ be a complex irreducible representation of degree $n$ of a finite group $G$. Let $\chi$ be its associated character and let $C$ be the center of $G$.
(a) Show that, for all $s \in C$, $\rho(s)$ is a scalar multiple of the identity matrix $I_n$.
(b) Use (a) to show that $|\chi(s)| = n$, for all $s \in C$.
(c) Prove the inequality $n^2 \leq [G : C]$, where $[G : C]$ denotes the index of $C$ in $G$.
(d) Show that, if $\rho$ is faithful (i.e. an injective group morphism), then the group $C$ has to be cyclic.
1. Let $G$ be a finite group and $p$ the smallest prime number dividing the cardinality $|G|$ of $G$. Let $H$ be a subgroup of $G$ of index $p$ in $G$. Show that $H$ is necessarily a normal subgroup of $G$.

2. Let $K$ be the splitting field of $f(X) = X^3 - 2$ over $\mathbb{Q}$.
   (a) Determine an explicit set of generators for $K$ over $\mathbb{Q}$.
   (b) Show that the Galois group $G(K/\mathbb{Q})$ of $K$ over $\mathbb{Q}$ is isomorphic to the symmetric group $S_3$.
   (c) Provide the complete list of intermediate fields $k$, $\mathbb{Q} \subseteq k \subseteq K$, satisfying $[k : \mathbb{Q}] = 3$.
   (d) Which of the fields determined in (c) are normal extensions of $\mathbb{Q}$?

3. Calculate the complete character table for $\mathbb{Z}/3\mathbb{Z} \times S_3$, where $S_3$ is the symmetric group in 3 letters.

4. Let $p$ be a prime number, $\mathbb{F}_p$ the prime field of $p$ elements, $X$ and $Y$ algebraically independent variables over $\mathbb{F}_p$, $K = \mathbb{F}_p(X, Y)$, and $F = \mathbb{F}_p(X^p - X, Y^p - X)$.
   (a) Show that $[K : F] = p^2$ and the separability and inseparability degrees of $K/F$ are both equal to $p$.
   (b) Show that there exists a field $E$, such that $F \subseteq E \subseteq K$, which is a purely inseparable extension of $F$ of degree $p$.

5. (a) Prove that an $n \times n$ matrix $A$ with entries in the field $\mathbb{C}$ of complex numbers, satisfying $A^3 = A$, can be diagonalized over $\mathbb{C}$.
   (b) Does the statement in (a) remain true if one replaces $\mathbb{C}$ by an arbitrary algebraically closed field $F$? Why or why not?

6. Let $R$ be the ring $\mathbb{Z}[X, Y]/(YX^2 - Y)$, where $X$ and $Y$ are two algebraically independent variables, and $(YX^2 - Y)$ is the ideal generated by $YX^2 - Y$.
in \( \mathbb{Z}[X,Y] \).

(a) Show that the ideal \( I \) generated by \( Y - 4 \) in \( R \) is not prime.

(b) Provide the complete list of prime ideals in \( R \) containing the ideal \( I \) described in question (a).

(c) Which of the ideals found in (b) are maximal?
Directions: Solve five problems from the following list of seven and clearly indicate which problems you chose as only those will be graded. Show all your work.

In general, it is permissible to use earlier parts of a problem in order to solve a later part even if you have not solved the earlier parts.

1. Let $G$ be a non-abelian group of order $p^3$, where $p$ is a prime number. Let $Z(G)$ be its center and $G^0$ its commutator subgroup.
   (a) Show that $Z(G) = G^0$ and this is the unique normal subgroup of $G$ of order $p$.
   (b) What is the exact number of distinct conjugacy classes of $G$?

2. (a) Let $p$ be a prime number. Show that $f(X) = X^p - pX - 1$ is irreducible in $\mathbb{Q}[X]$. (Hint: use Eisenstein’s criterion of irreducibility for the image of $f(X)$ via a ring automorphism of $\mathbb{Q}[X]$.)
   (b) Let $R$ be the ring $\mathbb{Z}[X]/(X^4 - 3X^2 - X)$, where $(X^4 - 3X^2 - X)$ is the ideal generated by $X^4 - 3X^2 - X$ in $\mathbb{Z}[X]$. Find all the prime ideals of $R$ containing 3 (the image of 3 in $\mathbb{Z}[X]$ via the canonical surjection $\mathbb{Z}[X] \rightarrow R$).

3. Let $K/k$ be a finite, separable field extension of degree $n$. Let
   $\rho, \rho' : K \rightarrow M_n(k)$
   be two morphisms of $k$-algebras, where $M_n(k)$ is the ring of $n \times n$ matrices with entries in $k$. Show that there exists an invertible matrix $A$ in $M_n(k)$ such that
   $\rho'(x) = A \cdot \rho(x) \cdot A^{-1}$, for all $x \in K$.

4. Let $G$ be a finite group. Show that there exists a Galois field extension $K/k$ whose Galois group is isomorphic to $G$.

5. Let $k$ be a field of characteristic $p$, where $p$ is a prime number. Let $X$ and $T$ be two (algebraically) independent variables over $k$.
   (a) Show that the degree of the field extension $k(X,T)/k(X^p,T^p)$ is $p^2$.
   (b) Show that there exist infinitely many distinct fields $F$ such that
   $k(X^p,T^p) \subseteq F \subseteq k(X,T)$.
   (see over, please)
6. Let $R$ be the ring $\mathbb{Q}[X]/(X^7 - 1)$, where $(X^7 - 1)$ is the ideal generated by $X^7 - 1$ in $\mathbb{Q}[X]$. Give an example of a finitely generated projective $R$–module which is not $R$–free. (We remind you that an $R$-module is called projective if it is a direct summand of a free $R$–module.)

7. Let $D_{10}$ be the dihedral group of order 10, given by the usual generators and relations

$$D_{10} = \langle r, s \mid r^5 = 1 = s^2, rs = sr^{-1} \rangle$$

(1) Compute the conjugacy classes of $D_{10}$.
(2) Compute the commutator subgroup $D'_{10}$ of $D_{10}$.
(3) Show that $D_{10}/D'_{10}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and conclude that $D_{10}$ has precisely two distinct characters of degree 1.
(4) Write down the complete character table of $D_{10}$.