**Directions:** Work each problem in a separate bluebook. Give reasons for your answers, and make clear which facts you are assuming. If you have any questions about notation, terminology the meaning of a problem or the level of detail appropriate, please do not hesitate to ask the proctor.

**Notation:**
- \( \mathbb{Z} \): Integers
- \( \mathbb{Q} \): Rational Field
- \( \mathbb{R} \): Real Field
- \( \mathbb{C} \): Complex Field
- \( GL(\cdot) \): Full linear group
- \( \mathbb{F}_q \): Finite field with \( q \) elements

1. Classify groups of order 171 = 9 \cdot 19.

2. Find all groups which can occur as the Galois group of the splitting field over \( \mathbb{F}_5 \) of a polynomial of degree 9. (The polynomial is not assumed irreducible.)

3. (a) Let \( p \) be an odd prime. Explain why \(-1 \in \mathbb{Z}/(p)\) is a square if and only if \( p \equiv 1 \mod 4 \).

(b) You may assume the fact that the ring \( \mathbb{Z}[i] \) of Gaussian integers is a principal ideal domain. Show that an odd prime \( p \in \mathbb{Z} \) is irreducible in \( \mathbb{Z}[i] \) if and only if \( p \equiv 3 \mod 4 \). **[Hint: Use (a).]**

4. Suppose that \( V \) is a finite dimensional complex vector space and suppose that \( S_1, \ldots, S_n \) are endomorphisms of \( V \) such that each \( S_i \) is diagonalizable and \( S_i S_j = S_j S_i \) for all \( i, j \). Show that there is a basis of \( V \) consisting of vectors each of which is an eigenvector for all \( S_i \).

5. Let \( F \subset K \) be subfields of the complex numbers such that \( K \) is a finite algebraic extension of \( F \). Let \( \zeta \in \mathbb{C} \).

(a) If \( \zeta \) is *transcendental* over \( K \), prove that \([K(\zeta) : F(\zeta)] = [K : F]\).

(b) Give an example of \( F \subset K \) and \( \zeta \) *algebraic* over \( K \) such that \([K(\zeta) : F(\zeta)] \) does not divide \([K : F]\).
Directions: Work each problem in a separate bluebook. Give reasons for your answers, and make clear which facts you are assuming. If you have any questions about notation, terminology the meaning of a problem or the level of detail appropriate, please do not hesitate to ask the proctor.

Notation:
Z: Integers
Q: Rational Field
R: Real Field
C: Complex Field
GL( ): Full linear group
F_q: Finite field with q elements

1. Let A be an abelian group with generators x, y and z subject to the relations

\[2x + 2y - 16z = 0,\]
\[8x + 4y + 2z = 0,\]
\[2x + y - 22z = 0.\]

What is the structure of A as a direct sum of cyclic groups?

2. Use linear algebra to prove that if \(F \subset E\) is a cyclic Galois field extension then there is an \(F\)-vector space basis of \(E\) of the form \(\{\sigma(x) | \sigma \in \text{Gal}(E/F)\}\), for some \(x \in E\).

3. (a) Assume that A is a commutative Noetherian integral domain. Show that every nonzero noninvertible element of A can be written as a finite product of irreducible elements. [Definition: a noninvertible element \(p \neq 0\) of A is irreducible if whenever \(p = bc\) with \(b, c \in A\) either \(b\) or \(c\) is invertible in A.]

(b) Give an example of a Noetherian integral domain which is not a unique factorization domain.

4. Let \(G\) be the group of order 20 with generators \(\sigma\) and \(\tau\) and relations \(\sigma^4 = \tau^5 = 1, \sigma \tau \sigma^{-1} = \tau^2\). Determine the conjugacy classes of \(G\) and compute the character table of the irreducible complex representations of \(G\).

5. (a) Find the Galois group of \(x^5 + 3x^2 + 1\) over the prime fields \(\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5\).

**Hint:** The only irreducible quadratic over \(\mathbb{F}_2\) is \(x^2 + x + 1\).

(b) Find the Galois group of \(x^5 + 3x^2 + 1\) over \(\mathbb{Q}\).

**Hint:** Use part (a).
Directions: Work each problem in a separate bluebook. Give reasons for your answers, and make clear which facts you are assuming. If you have any questions about notation, terminology the meaning of a problem or the level of detail appropriate, please do not hesitate to ask the proctor.

Notation:
\( \mathbb{Z} \): Integers
\( \mathbb{Q} \): Rational Field
\( \mathbb{R} \): Real Field
\( \mathbb{C} \): Complex Field
\( GL(,): \) Full linear group
\( \mathbb{F}_q \): Finite field with \( q \) elements

1. Let \( G \) be a group of order \( p^n \) where \( p \) is prime and \( n > 1 \). Show that \( G \) has an automorphism of order \( p \).

2. Let \( M \) be a \( 9 \times 9 \) matrix over \( \mathbb{C} \) with characteristic polynomial \( (x^2 + 1)^3(x + 1)^3 \) and with minimal polynomial \( (x^2 + 1)^2(x + 1) \).
   
   (a) Find \( \text{trace}(M) \) and \( \text{det}(M) \).
   
   (b) How many distinct conjugacy classes of such matrices are there in \( GL(9, \mathbb{C}) \)? Write down the Jordan form over \( \mathbb{C} \) for one such matrix \( M \).
   
   (c) Write down a \( 9 \times 9 \) matrix with rational coefficients with the above characteristic and minimal polynomials.

3. Let \( F = \mathbb{C}(z) \) be the field of rational functions in one variable over \( \mathbb{C} \), i.e. the field of fractions of the polynomial ring \( A = \mathbb{C}[z] \).
   
   (a) Show that \( A = \mathbb{C}[z] \) is integrally closed in \( F = \mathbb{C}(z) \).
   
   (b) Show that \( f(y) = y^5 - (z + 1)(z + 2) \in F[y] \) is irreducible.
   
   (c) Let \( E = F[y]/(f(y)) \) and let \( B = \mathbb{C}[z, y] \subset E \) be the integral closure of \( A = \mathbb{C}[z] \) in \( E \). Consider the prime ideals \( p_0 = (z) \) and \( p_1 = (z + 1) \) in \( A \). How many prime ideals in \( B \) lie above \( p_0 \) and \( p_1 \), respectively.

4. Suppose \( G \) is a finite group, \( N \subset G \) is a subgroup, and \( \rho : G \to \text{End}(V) \) is an irreducible complex representation of \( G \). Suppose there is a nonzero vector \( v_0 \in V \) such that \( \rho(x)v_0 = v_0 \) for all \( x \in N \).
   
   (a) If \( N \) is normal in \( G \), prove that \( N \) is contained in the kernel of \( \rho \).
   
   (b) Give an example to show that the conclusion to (a) need not be true if \( N \) is not normal in \( G \).

5(a). Suppose that \( F \) is a field of characteristic \( p > 0 \). If \( \alpha \) is algebraic over \( F \), show that \( \alpha \) is separable over \( F \) if and only if \( F(\alpha) = F(\alpha^{p^n}) \) for all \( n \geq 1 \).

(b). Suppose that \( k \) is a field of characteristic \( p > 0 \) and let \( F = k(x, y) \) by the field of rational functions in two independent variables over \( k \). Let \( E = F(x^{1/p}, y^{1/p}) \). Prove that \( E \) is not primitively generated over \( F \). In other words, prove for all \( \theta \in E \) that \( F(\theta) \neq E \).
Directions: Work each problem in a separate bluebook. Give reasons for your answers, and make clear which facts you are assuming. If you have any questions about notation, terminology the meaning of a problem or the level of detail appropriate, please do not hesitate to ask the proctor.

Notation:
\( \mathbb{Z} \): Integers
\( \mathbb{Q} \): Rational Field
\( \mathbb{R} \): Real Field
\( \mathbb{C} \): Complex Field
\( GL(\cdot) \): Full linear group
\( \mathbb{F}_q \): Finite field with \( q \) elements

1. Classify groups of order 306 that have a cyclic 3-Sylow subgroup.

2(a). Find the order of \( GL(5, \mathbb{F}_2) \), the group of invertible \( 5 \times 5 \) matrices over the field \( \mathbb{F}_2 \).

(b). Show that the polynomial \( f(x) = x^5 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x] \) is irreducible. (Hint: how many irreducible quadratics are there over \( \mathbb{F}_2 \)?)

(c). Exhibit a matrix \( A \) of order 31 in \( GL(5, \mathbb{F}_2) \). (Hint: use (b) and some finite field theory.)

3. Let \( R \) be a commutative ring and let \( E \) be an \( R \)-module spanned over \( R \) by elements \( e_1, \ldots, e_n \). Suppose that \( b : E \times E \to R \) is an \( R \)-bilinear map such that \( \text{det}(B) \in R \) is not a zero divisor, where \( B \) is the \( n \times n \) matrix \( (b(e_i, e_j)) \). Prove that \( E \) is a free \( R \)-module.

4. Let \( G \) be the group of order 136 = 8 \cdot 17 with presentation
\[
(x, y : y^8 = x^{17} = 1, \ yxy^{-1} = x^4).
\]

(a) Find the center of \( G \).
(b) Describe the number and dimensions of the irreducible complex representations of \( G \).
(c) Find the simple summands of the group ring \( \mathbb{Q}[G] \).

5(a). Let \( \zeta \) be a primitive 7th root of unity in \( \mathbb{C} \) and let \( \beta = \zeta + \zeta^2 + \zeta^4 \). Show that \( [\mathbb{Q}(\beta) : \mathbb{Q}] = 2 \) and that \( \sqrt{-7} \in \mathbb{Q}(\beta) \). (Hint: find a linear relation between 1, \( \beta \), and \( \beta^2 \).)

(b). Let \( E \) be the splitting field of the polynomial \( x^{14} + 7 = f(x) \) over \( \mathbb{Q} \) and let \( \alpha \) be a root of \( f(x) \) in \( \mathbb{C} \). Show that \( E = \mathbb{Q}[\zeta, \alpha] \) and find the degrees \([E : \mathbb{Q}],[E : \mathbb{Q}(\zeta)],\) and \([E : \mathbb{Q}(\alpha)]\).

(c). Write down elements \( \sigma \) and \( \tau \) of orders 6 and 7, respectively, in \( \text{Gal}(E/\mathbb{Q}) \) by explicitly giving the values \( \sigma(\zeta) \), \( \sigma(\alpha) \), and \( \tau(\zeta) \), \( \tau(\alpha) \).
**General Directions:** Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

**Notation:**
- \( \mathbb{Z} \): the ring of ordinary integers
- \( \mathbb{Q} \): the field of rational numbers
- \( \mathbb{R} \): the field of real numbers
- \( \mathbb{C} \): the field of complex numbers
- \( \mathbb{F}_q \): the finite field with \( q \) elements
- \( M_{n}(R) \): the ring of \( n \times n \) matrices with entries in the ring \( R \)
- \( \text{GL}_n(R) \): the group of invertible \( n \times n \) matrices in \( M_{n}(R) \)
- \( R[t] \): the ring of polynomials with coefficients in the ring \( R \)
- \( \mathbb{Z}/n \): the ring of integers mod \( n \). (Can also be thought of as the cyclic group of order \( n \).)

1. If \( G \) is a simple group of order 60, determine, with proof, the number of elements of order 3 in \( G \). (You may not assume there is only one such group.)

2. Let \( G \) be the group given by generators and relations \( G = \langle x, y \mid x^5 = xyx^{-1}y^{-2} = 1 \rangle \).
   
   (a) Prove \( G \) is finite.
   
   (b) What is \( |G| \)?
   
   (c) How many 5-Sylow subgroups are there in \( G \)?

3. Let \( G \) be the finite group of order 21 defined by generators and relations:
   
   \( \langle x, y \mid x^3 = y^7 = 1, xyx^{-1} = y^2 \rangle \).

Determine the conjugacy classes of \( G \) and construct its character table.

4. Let \( \mathbb{K} \) be an arbitrary field and suppose that \( T \in M_n(\mathbb{K}) \). Prove that there exists a vector \( v \in \mathbb{K}^n \) so that the vectors
   
   \( \{ v, Tv, T^2v, \ldots, T^{n-1}v \} \)

form a basis for \( \mathbb{K}^n \) if and only if the only matrices in \( M_n(\mathbb{K}) \) which commute with \( T \) are expressible as polynomials in \( T \) (i.e., \( A \) commutes with \( T \) if and only if \( A = a_0I + a_1T + \cdots + a_{n-1}T^{n-1} \) where \( I \in M_n(\mathbb{K}) \) is the identity matrix).

5. 
   
   (a) Determine the Galois group of \( x^3 - x + 3 \) over \( \mathbb{Q} \).
   
   (b) Determine the Galois group of \( x^3 - x + 3 \) over \( \mathbb{F}_5 \).
   
   (c) Determine the Galois group of \( x^4 + t \) over \( \mathbb{R}[t] \).
**General Directions:** Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

**Notation:**
- \( \mathbb{Z} \): the ring of ordinary integers
- \( \mathbb{Q} \): the field of rational numbers
- \( \mathbb{R} \): the field of real numbers
- \( \mathbb{C} \): the field of complex numbers
- \( \mathbb{F}_q \): the finite field with \( q \) elements
- \( M_n(R) \): the ring of \( n \times n \) matrices with entries in the ring \( R \)
- \( \text{GL}_n(R) \): the group of invertible \( n \times n \) matrices in \( M_n(R) \)
- \( R[t] \): the ring of polynomials with coefficients in the ring \( R \)
- \( \mathbb{Z}/n \): the ring of integers mod \( n \). (Can also be thought of as the cyclic group of order \( n \).)

1. Suppose that \( K \) is a non-Galois extension of \( \mathbb{Q} \) of degree 5. Let \( L \) be the Galois closure of \( K \) (the smallest Galois extension of \( \mathbb{Q} \) containing \( K \)), and suppose \( L \) does not contain any quadratic extensions of \( \mathbb{Q} \). Prove \( \text{Gal}(L/\mathbb{Q}) = A_5 \), the alternating group on 5 letters.

2. Determine all prime ideals of the ring \( \mathbb{Z}[t]/(t^2) \).

3. Suppose that \( A, B \) are elements of \( M_2(\mathbb{C}) \) such that \( A^2 = B^3 = I \), \( ABA = B^{-1} \) with \( A \neq I, B \neq I \). If \( D \in M_2(\mathbb{C}) \) commutes with \( A \) and \( B \), show that \( D \) is a scalar matrix, i.e., a scalar multiple of \( I \).

4. Let \( V \) be a valuation ring, i.e. a commutative ring (with unit) such that for all \( a, b \in V \) either \( a|b \) or \( b|a \). (Here, \( a|b \) means that \( b = ac \) for some \( c \in V \).)
   (i) Prove that if \( I \) and \( J \) are two ideals in \( V \) then \( I \subset J \) or \( J \subset I \).
   (ii) Prove that any finitely generated ideal of \( V \) is principal, that is, generated by a single element.
   (iii) Prove that if \( V \) is a Noetherian valuation ring, then there exists an element \( t \in V \) such that any proper nonzero ideal of \( V \) is \( (t^n) \) for some whole number \( n \geq 1 \).

5. Let \( G \) be a finite simple group, and let \( \rho: G \to \text{GL}_n(\mathbb{C}) \) be an irreducible representation, where \( n > 1 \). Let \( \chi \) be its character. If \( |\chi(g)| = n \), prove that \( g \) is the identity element of \( G \).
Do all problems. Use a separate blue book for each.

Notation: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $F_q$ denote the ring of integers, and the fields of rational numbers, real numbers, complex numbers, and $q$ elements, respectively.

1. Classify all groups of order 24 containing a normal subgroup which is cyclic of order 4.

2. Describe all similarity classes (conjugacy classes) of $6 \times 6$ matrices with minimal polynomial $x^4 + x^2$:
   (i) over $\mathbb{Q}$,
   (ii) over $F_5$.

3. Find the Galois group of the splitting field of the polynomial $x^3 - x + 1$:
   (i) over $\mathbb{R}$,
   (ii) over $\mathbb{Q}$,
   (iii) over $F_2$.

4. Suppose $K$ is a finite extension of $\mathbb{Q}$. Prove that the integral closure of $\mathbb{Z}$ in $K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

5. Suppose $G$ is a nonabelian group of order $pq$, where $p < q$ are primes.
   (a) Describe the conjugacy classes in $G$.
   (b) Describe all representations of $G$ (over $\mathbb{C}$).
Do all problems. Use a separate blue book for each.

Notation: \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) and \( \mathbb{F}_q \) denote the ring of integers, and the fields of rational numbers, real numbers, complex numbers, and \( q \) elements, respectively.

1. Describe all simple left modules over the matrix ring \( M_n(\mathbb{Z}) \) (\( n \times n \) matrices over \( \mathbb{Z} \)).
   Recall that a module is simple if it has no proper submodules.

2. Let \( G \) be a finite group. Prove that the following are equivalent:
   (i) every element of \( G \) is conjugate to its inverse,
   (ii) every character of \( G \) is real-valued.

3. Let \( R \) be the ring \( \mathbb{C}[x,y]/(y^4 - (x-1)(x-2)(x-3)(x-4)) \). (You may assume that \( y^4 - (x-1)(x-2)(x-3)(x-4) \) is irreducible.) Let \( K \) be the quotient field of \( R \).
   (a) Show that \( K \) is a Galois extension of \( \mathbb{C}(x) \).
   (b) Consider \( R \) as an extension of \( \mathbb{C}[x] \). For every prime \( p \) of \( \mathbb{C}[x] \), find the primes of \( R \) above \( p \) and describe the action of \( \text{Gal}(K/\mathbb{C}(x)) \) on them.

4. Suppose \( G \) is a finite group, \( F \) is a field whose characteristic does not divide the order of \( G \), and \( V \) is a representation of \( G \) over \( F \) (i.e., an \( F \)-vector space on which \( G \) acts \( F \)-linearly). Prove that if \( U \) is a subspace of \( V \) stable under \( G \), then there is a complementary subspace \( W \) of \( V \), also stable under \( G \), such that \( V = U \oplus W \).

5. Suppose \( K \) is an extension of \( \mathbb{Q} \) of degree \( n \), and let \( \sigma_1, \ldots, \sigma_n : K \to \mathbb{C} \) be the distinct embeddings of \( K \) into \( \mathbb{C} \). Let \( \alpha \in K \). Regarding \( K \) as a vector space over \( \mathbb{Q} \), let \( \phi : K \to K \) be the linear transformation \( \phi(x) = \alpha x \). Show that the eigenvalues of \( \phi \) are \( \sigma_1(\alpha), \ldots, \sigma_n(\alpha) \).
Directions: Work each problem in a separate bluebook. Give reasons for your answers, and make clear which facts you are assuming.

Notation:
\( \mathbb{Z} \): Integers
\( \mathbb{Q} \): Rational Field
\( \mathbb{R} \): Real Field
\( \mathbb{C} \): Complex Field
\( \text{GL}_n(R) \): Group of invertible \( n \times n \) matrices with entries in the ring \( R \)
\( \mathbb{F}_q \): Finite field with \( q \) elements
\( \mathbb{Z}/n \): Ring of integers mod \( n \) (can also be regarded as the cyclic group of order \( n \))

1. How many distinct isomorphism types are there for groups of order 2525?

2. (a) Suppose \( K \) is a field of characteristic zero which contains the \( p \)-th roots of 1, where \( p \) is a fixed prime. If \( L/K \) is a Galois extension of degree \( p \), explain why \( L = K[\alpha] \) where \( \alpha^p = a \in K \).

   (b) If \( p \) is odd, show that there is no \( \beta \in L \) with \( \beta^p = \alpha \). (Hint: Use norms.)

   (c) Give a counterexample to the assertion in part (b) if \( p = 2 \).

3. Suppose that \( W \) is an even-dimensional real vector space, \( T : W \to W \) a linear transformation with \( T^m = I \) (the identity transformation) with \( m \) odd. Show that there exists a linear transformation \( S : W \to W \) with \( S^2 = -I \) and \( ST = TS \).

4. Let \( A \) be a principal ideal domain, \( M \) a finitely generated free \( A \)-module.
   (a) Show that the number of elements in a free basis for \( M \) over \( A \) is independent of the choice of basis.
   (b) Let \( N \subseteq A^m \) be a submodule. Prove that \( N \) is free on \( n \) generators for some \( n \leq m \).
   (c) Prove that \( n = m \) in part (b) if and only if there is an nonzero \( a \in A \) with \( aA^m \subseteq N \).

5. Suppose \( G \) is a finite group, \( K \) a normal subgroup of \( G \), and that \( (\rho, V) \) is an irreducible complex representation of \( G \). Consider the restriction \( (\rho_K, V) \) of this representation to \( K \). Show that all \( K \)-invariant subspaces of \( V \) which are irreducible over \( K \) have the same dimension and occur with the same multiplicity in \( V \).
Directions: Work each problem in a separate bluebook. Give reasons for your answers, and make clear which facts you are assuming.

Notation:
\( \mathbb{Z} \): Integers
\( \mathbb{Q} \): Rational Field
\( \mathbb{R} \): Real Field
\( \mathbb{C} \): Complex Field
\( \text{GL}_n(R) \): Group of \( n \times n \) invertible matrices with entries in the ring \( R \)
\( \mathbb{F}_q \): Finite field with \( q \) elements
\( \mathbb{Z}/n \): Ring of integers mod \( n \) (can also be regarded as the cyclic group of order \( n \))

1. If \( G \) is a group, define subgroups \( G^{(n)} \) recursively by \( G^{(1)} = [G, G] \) (the commutator subgroup) and \( G^{(n+1)} = [G^{(n)}, G^{(n)}] \). The group \( G \) is solvable if \( G^{(n)} = \{ e \} \) for some \( n \).
   (a) If \( K \) is a normal subgroup of \( G \) such that both \( K \) and \( G/K \) are solvable, show that \( G \) is solvable.
   (b) Show that all groups of order \( p^n \) with \( p \) prime are solvable.

2. Determine the number of conjugacy classes in the group \( \text{GL}_2(\mathbb{F}_q) \) for all finite fields \( \mathbb{F}_q \).
   (Hint: Use linear algebra.)

3.(a) If \( A \) is a commutative ring with 1 show that the polynomial ring \( A[X] \) contains infinitely many distinct maximal ideals.
   (b) Describe all maximal ideals in the ring of formal power series \( \mathbb{Z}[[X]] \).

4.(a) If \( G \) is a non-abelian group of order \( p^3 \), show that \( G \) has a quotient group isomorphic to \( (\mathbb{Z}/p) \times (\mathbb{Z}/p) \). What are the number and dimensions of the irreducible complex representations of \( G \)?
   (b) If the nonabelian group of order \( p^3 \) contains an element \( x \) of order \( p^2 \) show that \( G \) has irreducible \( p \)-dimensional representations induced from suitable 1-dimensional representations of \( \langle x \rangle \cong \mathbb{Z}/p^2 \).

5. Let \( \mathbb{Q}[\zeta] \) be the field extension of \( \mathbb{Q} \) generated by a primitive 11-th root of unity \( \zeta \). The integral closure of \( \mathbb{Z} \) in \( \mathbb{Q}[\zeta] \) is the ring \( \mathbb{Z}[\zeta] \). For each of the following primes \( p \in \mathbb{Z} \), describe how the ideal \( p \mathbb{Z}[\zeta] \) factors in \( \mathbb{Z}[\zeta] \).
   (a) \( p = 11 \);
   (b) \( p = 43 \);
   (c) \( p = 37 \).
Directions: Work each problem in a separate bluebook. Give reasons for your assertions and state precisely any theorems that you quote.

Notation:
\( \mathbb{Z} \): Integers
\( \mathbb{Q} \): Rational Field
\( \mathbb{R} \): Real Field
\( \mathbb{C} \): Complex Field
\( \text{GL}_n(R) \): Group of invertible \( n \times n \) matrices with entries in the ring \( R \)
\( \mathbb{F}_q \): Finite field with \( q \) elements
\( \mathbb{Z}/n \): Ring of integers mod \( n \) (can also be regarded as the cyclic group of order \( n \))
\( S_n \): Symmetric group of degree \( n \)

1. How many distinct isomorphism types are there for groups of order 5555?

2. Find the Galois group of \( x^4 - 2 \) over the fields \( \mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{F}_3 \) and \( \mathbb{F}_{27} \).

3. Prove the following generalization of Nakayama’s Lemma to noncommutative rings. Let \( R \) be a ring with 1 (not necessarily commutative) and suppose that \( J \subset R \) is an ideal contained in every maximal left ideal of \( R \). If \( M \) is a finitely generated left \( R \)-module such that \( JM = M \), prove that \( M = 0 \).

4. Let \( S \) be a set of \( n \times n \) nilpotent matrices over a field \( K \) that pairwise commute. Show that there is an invertible matrix \( M \) such that every matrix \( MAM^{-1} \) with \( A \in S \) is strictly upper triangular, that is, all entries on or below the main diagonal are zero.

5. (a) Compute \( |\text{GL}_3(\mathbb{F}_2)| \), the number of invertible \( 3 \times 3 \) matrices over the field \( \mathbb{F}_2 \). If \( \mu \in \text{GL}_3(\mathbb{F}_2) \) has order 7 explain why \( \mu \) must act transitively on the non-zero elements of \( \mathbb{F}_2^3 = (\mathbb{Z}/2)^3 \).

(b) Using (a), show that there is a non-abelian group \( G \) of order 56 = 8 \cdot 7 with a normal 2-Sylow subgroup isomorphic to \( (\mathbb{Z}/2)^3 \). Find the number of irreducible complex representations of \( G \) and their dimensions.

(c) Find the conjugacy classes of \( G \) and compute the character values for at least one irreducible complex representation of \( G \) of dimension greater than one.
Directions: Work each problem in a separate bluebook. Give reasons for your assertions and state precisely any theorems that you quote.

Notation:
\( \mathbb{Z} \): Integers
\( \mathbb{Q} \): Rational Field
\( \mathbb{R} \): Real Field
\( \mathbb{C} \): Complex Field
\( \text{GL}_n(R) \): Group of invertible \( n \times n \) matrices with entries in the ring \( R \)
\( \mathbb{F}_q \): Finite field with \( q \) elements
\( \mathbb{Z}/n \): Ring of integers mod \( n \) (can also be regarded as the cyclic group of order \( n \))
\( S_n \): Symmetric group of degree \( n \)

1. Suppose that \( A \) is a Noetherian local ring with maximal ideal \( m \). If \( a \subset A \) is an ideal such that the only prime ideal of \( A \) containing \( a \) is \( m \), show that \( m^k \subset a \) for some \( k \geq 1 \).

2. A subgroup \( H \subseteq S_n \) is transitive if for all \( i, j \) with \( 1 \leq i, j \leq n \), there exists some \( \sigma \in H \) with \( \sigma(i) = j \). An automorphism of a group \( G \) is called inner if it is of the form \( x \rightarrow axa^{-1} \) for some \( a \in G \).

   (a) Show that \( S_5 \) has six 5-Sylow subgroups.
   (b) Show that \( S_6 \) contains a transitive subgroup isomorphic to \( S_5 \).
   (c) The subgroup \( H \subset S_6 \) from part b has six cosets. Show that there is an isomorphism \( \alpha : S_6 \rightarrow S_6 \) such that \( \alpha(H) \subset S_6 \) is not a transitive subgroup of \( S_6 \).
   (d) Explain why the automorphism in part (c) is not inner.

3. How many similarity classes are there of \( 10 \times 10 \) matrices with minimal polynomial \( (x^2 + 1)(x^3 - 2) \) over the field \( \mathbb{Q} \)? Over the field \( \mathbb{F}_5 \)?

4. Let \( k \) be a field of characteristic zero.

   (a) Suppose \( K \) and \( L \) are two finite extensions of \( k \), in some fixed algebraic closure of \( k \), such that \( K \) is normal over \( k \). Prove that \( |KL:L| \) divides \( |K:k| \).
   (b) Suppose that \( E \) is a Galois extension of \( k \) with \( \text{Gal}(E/k) = S_n \), the symmetric group. Show that for any integer \( j \) with \( 1 < j < n \) there are subfields \( K, L \subset E \) with \( K \cap L = k \), \( |K:k| = n \), \( |KL:L| = j \) and \( |L:k| = n! / j! \). [Hint: Galois correspondence.]

5. Let \( G \) be a group of odd order.

   (a) Show that the only irreducible complex character of \( G \) which is real valued is the trivial character \( \chi_1 \). [Hints: Assume \( \chi_V \) is a counterexample and get a contradiction from \( 0 = \langle \chi_1, \chi_V \rangle \). Make use of algebraic integers and the fact that \( g 
eq g^{-1} \) for \( g \neq 1 \).]
(b) Using (a), explain why the real group ring $\mathbb{R}[G]$ has structure

$$\mathbb{R} \times \prod_{i=1}^{s} \text{Mat}_{r_i}(\mathbb{C}),$$

where $s$ is the number of conjugacy classes of $G$ and $\text{Mat}_{r_i}(\mathbb{C})$ is the ring of $r_i \times r_i$ matrices with entries in $\mathbb{C}$. 
General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. Determine the number of isomorphism classes of groups of order $1705 = 5 \cdot 11 \cdot 31$.

2. If $A$ is a commutative Noetherian ring with 1 prove that $(0) = p_1 p_2 \cdots p_k$ for some finite collection of (not necessarily distinct) prime ideals $p_i \subset A$.

   [Hint: Consider the set of all ideals of $A$ which do not contain a finite product of prime ideals.]

3. Determine the number of similarity classes of matrices over $\mathbb{C}$ and which have characteristic polynomial $(X^4 - 1)(X^8 - 1)$. Do the same thing over $\mathbb{Q}$.

4. Let $F$ be a field. Consider the polynomial $f(X) = X^4 - a$ where $a \in F$. Determine (with explanation) all possible Galois groups of $f(X)$ as the field $F$ and the element $a \in F$ vary. Give an example for every possible Galois group.

5. Let $G$ be a finite group and let $z \in G$. Suppose for every irreducible complex character $\chi$ of $G$ we have $|\chi(z)| = |\chi(1)|$. Prove that $z$ is in the center of $G$. 
**General Directions:** Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. If $A$ is a finite abelian group and $m$ is a positive integer show that every automorphism of the subgroup $mA$ of $A$ can be extended to an automorphism of $A$.

   [Hint: Reduce to the case where $m$ is prime. Then use the structure theorem for finite abelian groups.]

2. Let $k$ be a field and let $A$ and $B$ be $k$-algebras with unit having centers $Z(A)$ and $Z(B)$. Prove that the center of the $k$-algebra $A \otimes_k B$ is $Z(A) \otimes_k Z(B)$.

   [Hint: First express $z \in A \otimes B$ as $\sum_{i=1}^{n} a_i \otimes b_i$ where $a_i$ are linearly independent over $k$. Show all $b_i \in Z(B)$.

3. Suppose $V$ is a finite dimensional vector space over a field $k$ and $T : V \to V$ is a linear transformation. Let $\wedge^2 T : \wedge^2 V \to \wedge^2 V$ be the induced endomorphism of the second exterior power of $V$. Explain why the characteristic polynomial of $\wedge^2 T$ depends only on the characteristic polynomial of $T$, and express the characteristic polynomial of $\wedge^2 T$ in terms of the eigenvalues of $T$.

4. Let $G$ be the group of matrices of the form

   \[
   \begin{pmatrix}
   1 & x & y \\
   0 & 1 & z \\
   0 & 0 & 1
   \end{pmatrix}
   \]

   in $GL(3, \mathbb{F}_3)$. Find the conjugacy classes in $G$ and compute it character table.

5. Suppose $F$ is a field and $K$ and $E$ are finite extensions of $F$ in some algebraic closure of $F$. Suppose that $E$ is Galois over $F$ (normal and separable). Show that $L = KE$ is Galois over $K$ with $[L : K] = [E : E \cap K]$. 
General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. If $p < q < r$ are primes and $G$ is a group of order $pqr$, show that $G$ contains a normal subgroup of order $r$. [Hint: First show that $G$ contains some normal Sylow subgroup.]

2. (a) If $I \subset A$ is an ideal in a commutative Noetherian ring and if $ab \in I$ for some $a, b$ with $a \notin I$ and $b^n \notin I$ for all $n$, show that $I = (I, b^m) \cap (I, a)$ for some $m$. [Hint: first show $xb^m + 1 \in I$ implies that $xb^m \in I$ for some $m$.]

(b) Let $A$ be a commutative ring and $E$ be a finitely generated $A$-module. If $\{e_1, \cdots, e_r\} \subset E$ is a finite subset whose images span $E/mE$ as an $A/m$ vector space for all maximal ideals $m \subset A$, show that $\{e_1, \cdots, e_r\}$ generate $E$ as an $A$-module.

3. (a) How many similarity classes of $10 \times 10$ matrices over $\mathbb{Q}$ are there with minimal polynomial $(x + 1)^2(x^4 + 1)$?

(b) Give an example of a $10 \times 10$ matrix over $\mathbb{R}$ with minimal polynomial $(x + 1)^2(x^4 + 1)$ which is not similar to a matrix with rational coefficients.

4. Let $G$ be a finite group and $H$ be a subgroup of index $k$. Let $(\pi, V)$ be an irreducible complex representation of $G$, and let $U$ be a nonzero $H$-invariant subspace. Prove that the dimension of $U$ is at least $\frac{1}{k} \dim(V)$. If its dimension is exactly $\frac{1}{k} \dim(V)$, prove $U$ is irreducible over $H$ and that there is no other $H$-invariant subspace of $V$ isomorphic to $U$ as an $H$-module.

5. (a) Find $[E : \mathbb{Q}]$ where $E$ is the splitting field of $x^6 - 4x^3 + 1$ over $\mathbb{Q}$.

(b) Show that $\text{Gal}(E/\mathbb{Q})$ is nonabelian and contains an element of order 6.
General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. Determine the number of isomorphism classes of groups of order $273 = 3 \cdot 7 \cdot 13$.

2. Suppose that $E/F$ is an algebraic extension of fields of characteristic zero. Suppose that every polynomial in $F[x]$ has at least one root in $E$.

(a) Show that $E/F$ is normal.

(b) Show that $E$ is algebraically closed.

3. Suppose that $E$ is the degree three field extension of the rational function field $\mathbb{Q}(x)$ defined by $E = \mathbb{Q}(x)[Y]/(Y^3 + x^2 - 1)$. Let $y$ be the image of $Y$ in $E$ and let $B \subset E$ denote the integral closure of $A = \mathbb{Q}[x]$ in $E$. It is known—and you may assume—that $B$ is the ring $\mathbb{Q}[x, y]$ generated by $x$ and $y$ over $\mathbb{Q}$. For each of the prime ideals $P$ of $A$ below, describe the factorization of the ideal $PB$ of $B$.

(i) $P = (x)$.

(ii) $P = (x - 1)$.

(iii) $P = (x^2 + 3)$.

4. Suppose $k$ is a field and $V$ is a module over the polynomial ring $k[T]$ which is finite dimensional as a vector space over $k$. Define a $k[T]$ module structure on the dual vector space $V^*$ by $(T\alpha)v = \alpha(Tv)$, $\alpha \in V^*$, $v \in V$. Show that $V \cong V^*$ as $k[T]$ modules.

5. Let $G$ be the nonabelian group of order 39 with generators and relations

$$\langle x, y | x^3 = y^{13} = 1, xyx^{-1} = y^3 \rangle.$$ 

Find its conjugacy classes and compute its character table.
Notation:

\( \mathbb{Q} \) denotes the field of rational numbers,

\( \mathbb{Z} \) denotes the ring of ordinary integers,

\( \mathbb{R} \) denotes the field of real numbers,

\( \mathbb{C} \) denotes the field of complex numbers,

\( \mathbb{F}_q \) denotes the finite field with \( q \) elements.

If \( R \) is any ring then \( \text{Mat}_n(R) \) denotes the ring of \( n \times n \) matrices with coefficients in \( R \).

If \( R \) is any ring then \( GL_n(R) \) denotes the group of invertible \( n \times n \) matrices in \( \text{Mat}_n(R) \).

If \( A \) is any ring then \( A[t] \) denotes the ring of polynomials with coefficients in \( A \).
Fall 2002
Ph.D. Qualifying Examination
Algebra
Part I

General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. (a) Let $F$ be a field, $V$ a finite-dimensional vector space over $F$ and $T : V \rightarrow V$ a linear transformation. Suppose that all roots of the characteristic polynomial of $T$ are in $F$. Show that with respect to some basis of $V$ the matrix of $T$ is upper triangular.

(b) Suppose that $V$ is a four dimensional vector space over the field $\mathbb{R}$ of real numbers and $T : V \rightarrow V$ a linear transformation. Show that with respect to some basis of $V$ the matrix of $T$ has the form

$$
\begin{pmatrix}
a_{11} & a_{12} & a_{13} & a_{14} \\
a_{21} & a_{22} & a_{23} & a_{24} \\
0 & 0 & a_{33} & a_{34} \\
0 & 0 & a_{43} & a_{44}
\end{pmatrix}.
$$

2. Classify those finite groups of order $351 = 3^3 \cdot 13$ that have an abelian 3-Sylow subgroup containing no elements of order 9.

3. Let $K$ be the splitting field of the polynomial $x^6 - 3 = 0$ over $\mathbb{Q}$. Compute $\text{Gal}(K/\mathbb{Q})$.

4. (Chinese remainder theorem.) Let $A$ be a commutative ring with unit and let $I$, $J$ be ideals of $A$ such that $A = I + J$. Prove that $IJ = I \cap J$ and that there is a ring isomorphism

$$
A/IJ \cong (A/I) \times (A/J).
$$

5. A nonabelian group $G$ of order 36 has generators $x$, $y$ and $z$ subject to the relations:

$$
x^3 = y^3 = 1, \quad xy = yx, \quad z^4 = 1, \quad zxz^{-1} = y, \quad yz^{-1} = x^2.
$$

Find the conjugacy classes of $G$ and compute its character table.
General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. Let $p$ be a prime.

(a) Consider the action of $GL(4, \mathbb{F}_p)$ on the set of two-dimensional vector subspaces of $\mathbb{F}_p^4$. Let $U = \{(0, 0, x, y) \mid x, y \in \mathbb{F}_p\}$. Describe the subgroup of $g \in GL(4, \mathbb{F}_p)$ such that $gU = U$ and compute its order.

(b) Compute the number of two dimensional vector subspaces of $\mathbb{F}_p^4$.

2. Let $p$ and $q$ be primes with $q \geq p$. Prove that there exists a nonabelian group of order $pq^2$ if and only if $p$ divides one of $q - 1$, $q$ or $q + 1$.

3. If $A$ is a commutative ring with unit and $I \subset A$ is a proper ideal, prove that there exists a prime ideal $P \subset A$ which is “minimal over $I$.” This means that $I \subset P$ and if $Q$ is prime with $I \subset Q \subset P$ then $Q = P$. [Hint: Zorn’s Lemma.]

4. Let $p$ be a prime and let $E/F$ be a cyclic Galois extension of degree $p$. Let $\sigma$ be a generator of $Gal(E/F)$.

(a) Suppose the characteristic of $E$ and $F$ is $p$. Show that there exists $\alpha \in E$ such that $\alpha \notin F$ but $\sigma(\alpha) - \alpha \in F$.

(b) Show that if the characteristic of $E$ and $F$ is not $p$ then $\sigma(\alpha) - \alpha \in F$ if and only if $\alpha \in F$.

Hint for both parts: It may help to think of $E$ as a vector space over $F$, and $\sigma$ as a linear transformation.

5. Let $R$ be a commutative ring containing $\mathbb{C}$, and let $M$ be a simple $R$-module. (Recall that this means that $M$ has no submodules except $\{0\}$ and $M$ itself.) Suppose that $\dim_\mathbb{C}(M) < \infty$.

(a) Prove that if $r \in R$ there exists $\alpha \in \mathbb{C}$ such that $rm = \alpha m$ for all $m \in M$. (Remark: If you use some version of Schur’s Lemma, you must prove it.)

(b) Prove that $\dim_\mathbb{C}(M) = 1$. 

Spring 2002
Ph.D. Qualifying Examination
Algebra
Part I

General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. Let \( p \) and \( q \) be primes, \( q > 2 \). Let \( G = SL(2, \mathbb{F}_p) \). (Here \( \mathbb{F}_p \) is the finite field with \( p \) elements.) Suppose that \( q \) divides \( |G| = p(p^2 - 1) \). Show that a \( q \)-Sylow subgroup of \( G \) is cyclic. (Hint: first show that \( G \) has cyclic subgroups of orders \( p, p - 1 \) and \( p + 1 \).)

2. Let \( R \) be a commutative ring with unit.
   
   (i) Let \( S \) be a saturated multiplicative set of \( R \). This means that \( 1 \in S \), \( 0 \notin S \), and \( xy \in S \) if and only if \( x \in S \) and \( y \in S \). Show that \( R - S \) is a union of prime ideals. [Hint: If \( a \in R - S \) consider ideals \( J \) with \( a \in J \subseteq R - S \).]

   (ii) An element \( a \in R \) is a zero divisor if \( ab = 0 \) for some \( b \neq 0 \). Apply (i) to show that the set of zero divisors is a union of prime ideals of \( R \).

3. Let \( p \) be prime. Show that there exists \( \alpha \in \mathbb{C} \) such that \( K = \mathbb{Q}(\alpha) \) is a Galois extension of \( \mathbb{Q} \) and that \( \text{Gal}(K/\mathbb{Q}) \) is cyclic of order \( p \). Exhibit such an \( \alpha \) when \( p = 5 \).

4. Let \( G \) be a finite group and let \( H \subseteq G \) be an abelian subgroup of prime index \( p \). Let \( \chi \) be an irreducible character of \( G \) such that \( \chi(1) = p \). Prove that there exists a character \( \psi \) of \( H \) such that \( \chi \) is the character of \( G \) induced from \( \psi \).

5. (i) Let \( R \) be a principal ideal domain, and let \( f, g \in R \) be coprime elements. Show that
   \[
   R/(fg) \cong R/(f) \oplus R/(g)
   \]
   as \( R \)-modules.

   (ii) Let \( F \) be a field, and let \( f(X) = X^2 + aX + b, g(X) = X^2 + cX + d \) be distinct irreducible polynomials over \( F \). Let \( fg = X^4 + tX^3 + uX^2 + vX + w \). Show that the matrices
   \[
   \begin{pmatrix}
   0 & 1 & 0 & 0 \\
   -b & -a & 0 & 0 \\
   0 & 0 & 0 & 1 \\
   0 & 0 & -d & -c
   \end{pmatrix}, \quad
   \begin{pmatrix}
   0 & 1 & 0 & 0 \\
   0 & 0 & 1 & 0 \\
   0 & 0 & 0 & 1 \\
   -w & -v & -u & -t
   \end{pmatrix}
   \]
   are conjugate in \( GL(4, F) \), the group of \( 4 \times 4 \) invertible matrices with coefficients in \( F \).
General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

Notation: Here \( \mathbb{F}_p \) denotes the finite field with \( p \) elements, and \( S_n \) denotes the symmetric group of degree \( n \).

1. Let \( H \) be the subgroup of \( S_6 \) generated by \((16425)\) and \((16)(25)(34)\). Let \( H \) act on \( S_6 \) by conjugation. Show that the set

\[
\]

is invariant under \( H \). Hence obtain a homomorphism \( \phi : H \to S_5 \). Show that \( \phi \) is an isomorphism.

2. Let \( Q \) be the group of order 8 having generators \( x \) and \( y \) such that \( x^4 = y^4 = 1 \), \( x^2 = y^2 \) and \( xyx^{-1} = y^3 \). Find the conjugacy classes of \( Q \) and compute its character table.

3. Let \( p \) and \( q \) be distinct primes. Show that the polynomial

\[
\Phi(X) = X^{p-1} + X^{p-2} + \ldots + 1
\]

has a root in \( \mathbb{F}_{q^2} \) if and only if \( q \equiv \pm 1 \) modulo \( p \).

4. Let \( V \) be a finite dimensional complex vector space endowed with an inner product, that is, a positive definite Hermitian form \( \langle , \rangle \). Let \( T : V \to V \) be a linear transformation which commutes with its adjoint \( T^* \), defined by

\[
\langle Tx, y \rangle = \langle x, T^*y \rangle.
\]

Prove that \( V \) has a basis consisting of eigenvectors of \( T \).

5. Let \( A \) be a commutative Noetherian ring with unit. An ideal \( J \subset A \) is called a radical ideal if \( x^n \in J \) implies that \( x \in J \). Show that every proper radical ideal is a finite intersection of prime ideals. [Hint: Among counterexamples, a maximal one couldn’t be prime.]
1. Classify finite groups of order $2p^2$ up to isomorphism, where $p$ is an odd prime.

2. Let $A \in M(n, K)$ be an $n \times n$ matrix over a field $K$ such that the minimal polynomial of $A$ has degree $n$. Show that every matrix in $M(n, K)$ that commutes with $A$ is a $K$-linear combination of the identity matrix and powers of $A$.

3(a). Suppose $\rho : G \to \text{GL}(V)$ is an irreducible complex representation of a finite group $G$. Show that if $Z(G) \subset G$ is the center of $G$, then there is a homomorphism $\chi : Z(G) \to \mathbb{C}^*$ such that $\rho(g)v = \chi(g)v$ for all $g \in Z(G)$ and $v \in V$.

(b). Conversely, show that for any homomorphism $\chi : Z(G) \to \mathbb{C}^*$, there exists an irreducible $\rho : G \to \text{GL}(V)$ such that $\rho(g)v = \chi(g)v$ for all $g \in Z(G)$ and $v \in V$.

4. Suppose $g(T) \in \mathbb{Z}[T]$ is a monic polynomial with roots $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$. If $|\alpha_j| = 1$ for all $j$, show that each $\alpha_j$ is a root of unity. Show by example that this conclusion may fail to hold if $g(T)$ is not assumed monic.

5. Let $R$ be a ring with identity, and let $M$ be a left $R$-module. Prove there exist submodules $M = M_0 \supset M_2 \supset \cdots \supset M_n = (0)$ so that $M_j/M_{j+1}$ is a simple $R$-module (for all $j$) if and only if $M$ satisfies both the ascending chain condition and the descending chain condition for submodules. [Hints: For the “if” direction, begin by using one chain condition to get a maximal or a minimal proper submodule. For the “only if” direction, use an induction on $n$.]

1. If $p < q < r$ are primes and $G$ is a finite group with $|G| = pqr$, prove that the Sylow-$r$ subgroup of $G$ is normal. [Hint: First get some normal Sylow subgroup.]

2. Suppose $V$ is a vector space of dimension 20 over the field $\mathbb{Q}$, and $A : V \to V$ is a linear transformation with minimal polynomial $(T^2 + 1)^2(T^3 + 2)^2$.

(a). How many distinct similarity classes of such $A$ exist?

(b). If $V$ is generated by two elements as a $\mathbb{Q}[T]$ module, where $T$ acts on $V$ as the linear transformation $A$, and if $p(T) \in \mathbb{Q}[T]$, what integers can occur as the dimension of the kernel of $p(T) : V \to V$ as a rational vector space?

3. Find the Galois groups of the polynomials $X^6 + 3$ and $X^6 + X^3 + 1$ over the fields $\mathbb{Q}$ and $\mathbb{F}_7$.

4. Suppose $k$ is a field of characteristic $\neq 2$, and let $R$ denote the polynomial ring $k[x_1, x_2, \ldots, x_n]$. Suppose $f(x_1, x_2, \ldots, x_n) \in R$ is a non-constant polynomial that is not divisible by the square of any non-constant polynomial in $R$. Show that the ring $S = R[T]/(T^2f)$ is the integral closure of $R$ in the field of fractions of $S$.

5. Suppose $G$ is the group of order 12 with presentation

$$G = \langle x, y \mid x^4 = y^3 = 1, xyx^{-1} = y^2 \rangle.$$ 

Find the complex character table of $G$. 

Directions: Work each problem in a separate bluebook. Give reasons for your answers, and make clear which facts you are assuming.

Notation:
\( \mathbb{Z} \): Integers
\( \mathbb{Q} \): Rational Field
\( \mathbb{R} \): Real Field
\( \mathbb{C} \): Complex Field
\( \text{GL}_n(R) \): Group of invertible \( n \times n \) matrices with entries in the ring \( R \)
\( \mathbb{F}_q \): Finite field with \( q \) elements
\( \mathbb{Z}/n \): Ring of integers mod \( n \) (can also be regarded as the cyclic group of order \( n \))

1. Classify all finite groups of order 140 up to isomorphism.

2. Find the degree \( |E: \mathbb{Q}| \) if \( E \) is the splitting field of the polynomial \( X^{10} - 5 \in \mathbb{Q}[X] \). How many distinct intermediate fields \( K \) exist with \( \mathbb{Q} \subset K \subset E \)?

3(a). Find all positive integers that can occur as the order of some element of \( \text{GL}(2, \mathbb{R}) \). Exhibit an element of order 5.

(b). Find all positive integers that can occur as the order of some element of \( \text{GL}(3, \mathbb{F}_7) \).

(c). Find all positive integers that can occur as the order of some element of \( \text{GL}(4, \mathbb{Q}) \). Exhibit an element of order \( \neq 1 \) or 2.

4(a). Find the integral closure \( B \) of the integers \( \mathbb{Z} \) in the field \( \mathbb{Q}[\sqrt{-39}] \).

(b). Show that there are two distinct prime ideals of \( B \) that contain the ideal \( 5B \subset B \). Give generators for these two prime ideals and show that neither is principal.

(c). How does the ideal \( 3B \subset B \) factor as a product of prime ideals?

5. Let \( \rho : G \to \text{GL}(3, \mathbb{C}) \) be a 3-dimensional complex representation of a finite group \( G \). Let \( V \) be the vector space of all \( 3 \times 3 \) matrices over \( \mathbb{C} \). Define the adjoint representation \( \rho^\sim : G \to \text{GL}(V) \) by

\[
\rho^\sim(g)A = \rho(g)A\rho(g^{-1})
\]

for \( g \in G \) and \( A \in V \). Which integers can occur as the multiplicity of the trivial one dimensional representation in \( \rho^\sim \)?
**Directions:** Work each problem in a separate bluebook. Give reasons for your answers, and make clear which facts you are assuming.

**Notation:**
- $\mathbb{Z}$: Integers
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: Fields of rational, real, and complex numbers, respectively
- $\text{GL}_n(R)$: Group of $n \times n$ invertible matrices with entries in the ring $R$
- $\mathbb{F}_q$: Finite field with $q$ elements
- $\mathbb{Z}/n$: Ring of integers mod $n$ (can also be regarded as the cyclic group of order $n$)

1(a). Find all abelian groups $G$ that contain a subgroup $H$ isomorphic to $\mathbb{Z}/72\mathbb{Z}$ for which the quotient group $G/H$ is also isomorphic to $\mathbb{Z}/72\mathbb{Z}$.

(b). Find the invariant factors of the abelian group $(\mathbb{Z}/44\mathbb{Z}, 0)$, i.e., the multiplicative group of invertible elements in the ring $\mathbb{Z}/44\mathbb{Z}$.

2. Suppose $I \subset \mathbb{Q}[x_1, x_2, \ldots, x_n]$ is an ideal such that the set of zeroes
   \[ V(I) = \{ x \in \mathbb{C}^n : f(x) = 0 \text{ for all } f \in I \} \]
   is a finite set. Show that the ring $\mathbb{Q}[x_1, x_2, \ldots, x_n]/I$ is a finite dimensional vector space over $\mathbb{Q}$.

   [Hint: first show that $\mathbb{Q}[x_1, x_2, \ldots, x_n]/J$ is finite dimensional, where $J = \sqrt{I}$ is the radical of $I$. Then consider powers $J^2 \supset J^2 \supset \ldots$.]

3(a). Factor $X^5 + 7X^3 + 6X^2 + X + 5$ over the fields $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_5$.

   [You may assume the (true) result that this polynomial has no irreducible quadratic factors over $\mathbb{F}_3$.]

   (b). What are the Galois groups of $X^5 + 7X^3 + 6X^2 + X + 5$ over $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_5$?

   (c). What are the Galois groups of $X^5 + 7X^3 + 6X^2 + X + 5$ over $\mathbb{Q}$?

4. Suppose $V$ is a finite dimensional vector space over a field $k$ and suppose $A : V \rightarrow V$ is a $k$-linear endomorphism whose minimal polynomial is not equal to its characteristic polynomial. Show that there exist $k$-linear endomorphisms $B, C : V \rightarrow V$ such that $AB = BA, AC = CA$, but $BC \neq CB$.

5(a). Produce a complex character table for the symmetric group $S_4$.

(b). The rotation group of the cube is isomorphic to $S_4$ as a permutation group of the four diagonals of the cube. Let $\rho : S_4 \rightarrow \text{GL}(8, \mathbb{C})$ be the permutation representation of $S_4$ defined by the action of the rotation group on the eight vertices of the cube. Find the character of $\rho$.

(c). Decompose $\rho$ as a direct sum of irreducible representations of $S_4$. 
1. Classify all finite groups of order $147 = 3 \cdot 7^2$.

2. Let $A, B \in \text{Mat}_n(\mathbb{R})$ be a pair of commuting matrices.
   (a) Suppose that $A$ and $B$ are both nilpotent. Show that they have a nonzero common nullvector.
   (b) Suppose that $n$ is odd. Show that $A$ and $B$ have a common eigenvector. (It is no longer assumed that they are nilpotent.)

3. (a) Find the minimal polynomial of $\sqrt{4 + \sqrt{7}}$ over $\mathbb{Q}$.
   (b) Find the Galois group of that polynomial’s splitting field over $\mathbb{Q}$.
   \textbf{Hint:} Check that $\sqrt{4 + \sqrt{7}} = \frac{1}{2}(\sqrt{2} + \sqrt{14})$.

4. Recall the following definitions: If $R$ is a commutative ring and $a$ is an ideal, then the \textit{radical} $r(a) = \{x \in R \mid x^n \in a\}$. An ideal $q$ is \textit{primary} if $xy \in q$ implies that either $x \in q$ or $y \in r(q)$. Prove that if $r(q)$ is a maximal ideal, then $q$ is primary.

5. Let $G$ be a nonabelian group of order $pq$ where $p$ and $q$ are distinct primes such that $p < q$.
   (a) Show that $p$ divides $q - 1$, and show that the number of conjugacy classes of $G$ is exactly $p + \frac{q-1}{p}$.
   (b) Determine the number and degrees of the irreducible complex characters of $G$. 
1. Let $G = \langle x \rangle$ be a cyclic group of order $2^n$, and let $R = F_2[G]$ be the group algebra.
   (a) Show that
   $$ J = \left\{ \sum_{i=0}^{2^n-1} a_i x^i \mid \sum a_i = 0 \right\} $$
   is a nilpotent ideal in the commutative ring $R$, and deduce that
   $$ \Gamma = 1 + J = \left\{ \sum_{i=0}^{2^n-1} a_i x^i \mid \sum a_i = 1 \right\} $$
   is an abelian group of order $2^{2^n-1}$.
   (b) Consider $\Gamma^{2k} = \{ u^{2k} \mid u \in \Gamma \}$. Show that
   $$ |\Gamma^{2k}| = \begin{cases} 2^{2n-k-1} & \text{if } k \leq n; \\ 1 & \text{if } k \geq n. \end{cases} $$
   (c) There is enough information in this fact to determine the structure of $\Gamma$. Illustrate this by determining the structure of $\Gamma$ when $n = 4$.

2. Let $r > 0$, and let $q$ be a prime power. If $a \in F_q^r$ let $T(a) : F_q^r \to F_q^r$ be the map $T(a)x = ax$. Regarding $F_q^r$ as a $r$-dimensional vector space over $F_q$, we may think of $T(a)$ as an element of $GL(r,F_q)$.
   (a) Show that the composite $\det \circ T$ coincides with the norm map $F_q^r \to F_q$.
   (b) Show that if $b \in F_q^\times$, then there exists $a \in F_q^\times$ such that $\det T(a) = b$.

3. Let $G$ be a finite group and $H$ a subgroup. Let $\rho : H \to GL_n(\mathbb{C})$ be an irreducible representation. Show that if $\rho_1$ and $\rho_2$ are extensions of $\rho$ to $G$, and if the characters $\chi_1$ and $\chi_2$ of $\rho_1$ and $\rho_2$ are the same, then $\rho_1(g) = \rho_2(g)$ for all $g \in G$. 

2
4. Let $A$ be a Noetherian local commutative ring with maximal ideal $\mathfrak{m}$. Assume that $\mathfrak{m}$ is principal. Show that every nonzero ideal of $A$ is of the form $\mathfrak{m}^k$ for some $k$.

5. Let $\zeta = e^{2\pi i/40}$ and let $K = \mathbb{Q}(\zeta)$. (a) Determine the Galois group $\text{Gal}(K/\mathbb{Q})$.

(b) Find all quadratic extensions of $\mathbb{Q}$ contained in $K$. Express them in the form $\mathbb{Q}(\sqrt{D})$ for $D \in \mathbb{Z}$. 

General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. Classify the finite groups of order $333 = 3^2 \cdot 37$.

2. (a) If $\mathbb{F}_q$ is the finite field with $q$ elements, show that $X^{q^r} - X \in \mathbb{F}_q[X]$ is exactly the product of all irreducible polynomials $f(X) \in \mathbb{F}_q[X]$ whose degree divides $r$.

(b) Prove that the number of irreducible polynomials of degree $r$ in $\mathbb{F}_q[X]$ is

$$\frac{1}{r} \sum_{d | r} \mu \left( \frac{r}{d} \right) q^d,$$

where $\mu$ is the Moebius function:

$$\mu(d) = \begin{cases} (-1)^k & \text{if } d \text{ is a product of } k \text{ distinct primes;} \\ 0 & \text{otherwise.} \end{cases}$$

3. Let $A$ be an integral domain with field of fractions $F$. Assume that for every prime ideal $p \subset A$ the localization $A_p$ is integrally closed (in $F$). Prove that $A$ is integrally closed (in $F$).

4. Let $A$ and $B$ be nilpotent complex $n \times n$ matrices. Suppose that $\text{rank}(A^k) = \text{rank}(B^k)$ for all $k$. Prove that $A = MBM^{-1}$ for some $M \in \text{GL}(n, \mathbb{C})$.

5. Here is a partial character table of $A_5$.

<table>
<thead>
<tr>
<th></th>
<th>$\chi_1$</th>
<th>$\chi_2$</th>
<th>$\chi_3$</th>
<th>$\chi_4$</th>
<th>$\chi_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>$(123)$</td>
<td>1</td>
<td>1</td>
<td>$-1$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$(12)(34)$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$(12345)$</td>
<td>1</td>
<td>$-1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$(13524)$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Complete this character table by constructing $\chi_4$ and $\chi_5$. 

1
General Directions: Work all problems in separate bluebooks. Give reasons for your assertions and state precisely any theorems that you quote.

1. An abelian group $G$ (written additively) is called divisible if the homomorphism $x \mapsto nx = x + \ldots + x$ ($n$ terms) is surjective for all $n \geq 1$. The abelian group $G$ is called injective if whenever $A$ and $B$ are abelian groups with $A \subset B$, a homomorphism $\varphi : A \to G$ can be extended to a homomorphism $\Phi : B \to G$. Assume that $G$ is divisible. Prove that $G$ is injective. [Hint: Use Zorn’s Lemma.]

2. Show that if $G$ is a finite abelian group, then there exists a finite extension $F$ of $\mathbb{Q}$ such that $\text{Gal}(F/\mathbb{Q}) \cong G$. [Hint: Think about roots of unity.]

3. Suppose that $A$ is a commutative Noetherian ring.
   (a) Prove that every ideal $I \subset A$ contains a finite product of prime ideals.
   (b) Prove that $A$ has only finitely many minimal prime ideals. [Hint: Think about the zero ideal.]
   (c) Prove that if $A$ has no nilpotent elements then the set of zero divisors in $A$ is exactly the union of the minimal prime ideals of $A$.

4. Let $(\pi, V)$ be a nontrivial irreducible complex representation of the finite group $G$ with character $\chi$. Suppose that $1 \neq g \in G$ is such that $|\chi(g)| = \chi(1)$. Show that $\pi(g)$ is a scalar endomorphism of $V$ and deduce that $G$ is not a nonabelian simple group.

5. Determine the number of conjugacy classes of elements of orders 3, 5 and 11 in $\text{GL}(2, \mathbb{F}_{11})$. 

Stanford Math PhD Qualifying Exam, Part II
Spring, 2004
1. Let $p$ and $q$ be primes with $p, q \neq 2$ and suppose that $p$ divides $q + 1$.
   
   (a) Show that there exists a nonabelian group $G$ of order $pq^2$ whose Sylow $q$-subgroup is not cyclic.
   
   (b) Show that if $G$ is a nonabelian group of order $pq^2$ then it has a normal $q$-Sylow subgroup $Q$, and if $Q$ is not cyclic then a $p$-Sylow subgroup of $\text{Aut}(Q)$ is cyclic.
   
   (c) Show that any two nonabelian groups of order $pq^2$ with noncyclic Sylow $q$-subgroups are isomorphic.

2. Suppose that $f(t) \in \mathbb{Q}[t]$ is an irreducible polynomial of degree 5 with exactly 3 real roots. Let $K$ be the splitting field of $f$ over $\mathbb{Q}$. Show that $\text{Gal}(K/\mathbb{Q}) \cong S_5$. Prove any nonobvious facts you use about $S_5$.

3. Let $A$ be a commutative ring. The ring $A$ is called Artinian if it satisfies the decreasing chain condition: if $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ is a sequence of ideals then for some $N$ we have $I_N = I_{N+1} = I_{N+2} = \cdots$.
   
   (a) If $A$ is an Artinian integral domain show that $A$ is a field.
   
   (b) If $A$ is an Artinian commutative ring, show that every prime ideal in $A$ is maximal.

4. Let $G$ be a group of odd order. Prove that if $\chi$ is a complex irreducible character of $G$ and $\chi(g)$ is real for all $g \in G$ then $\chi = 1$. (Hint: Consider the value of $\sum_{g \neq 1} \chi(g)$ and the fact that $g \neq g^{-1}$ when $g \neq 1$. Think about algebraic integers.)

5. Let $T, U \in \text{Mat}_n(F)$ where $F$ is any field. Prove that if $T$ and $U$ are nilpotent matrices and $\text{rank}(T^k) = \text{rank}(U^k)$ for all $k$, then $T = AU A^{-1}$ for some $A \in \text{Mat}_n(F)$. 
1. Let $G$ be the group of order 18 with generators $x, y, z$ subject to relations

$$x^3 = y^3 = z^2 = 1, \quad xy = yx, \quad zxz^{-1} = y, \quad zyz^{-1} = x.$$ 

Determine the conjugacy classes of $G$ and compute its character table.

2. Let $p$ be an odd prime and $\zeta = e^{2\pi i/p}$. Show that there exists a unique subfield $K$ of $\mathbb{Q}(\zeta)$ such that $[K: \mathbb{Q}] = 2$. Let $\chi: (\mathbb{Z}/p\mathbb{Z})^\times \to \{ \pm 1 \}$ be the unique nontrivial homomorphism and let

$$\alpha = \sum_{a=1}^{p-1} \chi(a) \zeta^a.$$ 

Show that $\alpha^2 = (-1)^{(p-1)/2} p$ and conclude that $K = \mathbb{Q}(\alpha)$.

3. Let $A$ be an Noetherian integral domain with field of fractions $F$. If $f \in A$ is not a unit, prove that the ring $A[f^{-1}]$ generated by $f^{-1}$ and $A$ is not a finitely-generated $A$-module.

4. Let $G$ be a finite group of odd order. Prove that if $g \in G$ is conjugate to $g^{-1}$ then $g = 1$.

5. Let $n > 1$ be odd. Let $A$ and $B$ be matrices in $\mathrm{GL}_2(\mathbb{C})$ such that $A^n = 1$, $BAB^{-1} = A^{-1}$ and $A \neq I$. Suppose that $X$ commutes with both $A$ and $B$. Prove that $X$ is a scalar matrix.
1. Suppose $p$ and $q$ are odd primes and $p < q$. Let $G$ be a finite group of order $p^3q$.
   (a) Prove that $G$ has a normal Sylow subgroup.
   
   (b) Let $n_p$ and $n_q$ denote the number of $p$-Sylow and $q$-Sylow subgroups of $G$. Determine, with proof, all ordered pairs $(n_p, n_q)$ that are possible for groups of order $p^3q$.

2. Let $f(X) \in \mathbb{Q}[X]$ be a monic irreducible polynomial of degree 4 with roots $\alpha, \beta, \gamma, \delta$. The discriminant of a polynomial with roots $r_1, \ldots, r_n$ is $\prod_{i < j} (r_i - r_j)^2$.
   (a) Prove that $\lambda = \alpha \beta + \gamma \delta$ is the root of a monic cubic polynomial $g(X) \in \mathbb{Q}[X]$ whose discriminant is the same as the discriminant of $f$.
   (b) If $f \in \mathbb{Z}[X]$ prove that $g \in \mathbb{Z}[X]$.

3. Let $M$ be a finitely-generated module over the Noetherian commutative ring $R$. Prove that if $f: M \rightarrow M$ is an $R$-module homomorphism, and if $f$ is surjective, then $f$ is also injective. Hint: consider the submodules $\ker(f^n)$.

4. Let $G$ be the nonabelian group of order 16 with generators $x$ and $y$ subject to the relations

   $x^8 = y^2 = 1, \quad yxy^{-1} = x^3$.

   Determine the conjugacy classes of $G$ and compute its character table.

5. If $B$ is a positive-definite symmetric real matrix, show that there exists a unique positive-definite symmetric real matrix $C$ such that $C^2 = B$.
1. Suppose that $A \subset B$ is an integral extension of commutative rings with unit.
(a) If $q$ is a maximal ideal of $B$, prove that $p = q \cap A$ is a maximal ideal of $A$.
(b) Outline the proof that for any prime ideal $p \subset A$ there exists a prime ideal $q$ of $B$ with $p = q \cap A$.

2. Let $F = \mathbb{Z}/2\mathbb{Z}$, and let $F[X, Y]$ be the polynomial ring in two variables. Let $I$ be the ideal generated by $X^5 + X^3 + X$ and $Y^3 + (X^3 + 1)Y + 1$, and let $R$ be the quotient ring $F[X, Y]/I$. Determine the number of maximal ideals in the ring $R$.

**Hint:** if $a \in \mathbb{F}_4$, what is $a^3$?

3. If $G$ is a permutation group acting on a set $S$ we say $G$ is $n$-transitive if $|S| \geq n$ and whenever $x_1, \ldots, x_n$ are distinct elements of $S$ and $y_1, \ldots, y_n$ are distinct elements of $S$ there exists $g \in G$ such that $g(x_i) = y_i$. We will denote by $\chi(g)$ the number of fixed points of $g$. Prove that a necessary and sufficient condition for $G$ to be 3-transitive is that

$$\frac{1}{|G|} \sum \chi(g)^3 = 5.$$  

4. Suppose that $A$ is an $n \times n$ matrix over $\mathbb{C}$ with minimal polynomial $(X - \lambda)^n$ where $\lambda \neq 0$. Find the Jordan form of $A^2$. What if $\lambda = 0$?

5. Find the Galois group of the polynomial $X^5 + 99X - 1$ over the fields $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z}$ and $\mathbb{Q}$. 

2
1. In parts (a) and (c), let $G$ be a nonabelian group of order 56.

(a) Prove that $G$ has a normal 2-Sylow subgroup or a normal 7-Sylow subgroup.

(b) Let $Z_n$ denote a cyclic group of order $n$. Compute the order of $\text{Aut}(Q)$ when $Q = Z_8$, $Z_4 \times Z_2$ and $Z_2 \times Z_2 \times Z_2$.

(c) How many isomorphism classes are there of nonabelian groups of order 56 with normal abelian 2-Sylow subgroup? Explain. (Hint: use part (b).)

2. Let $G$ be the following group of order 42.

$$G = \langle x, y | x^7 = y^6 = 1, yxy^{-1} = x^2 \rangle.$$ Determine the conjugacy classes of $G$ and the degrees of its irreducible characters. Compute the values of at least one irreducible character of degree $> 1$.

3. Find an extension $E$ of $\mathbb{Q}$ with $\text{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.

4. Suppose $J$ is an $n \times n$ matrix over an algebraically closed field of characteristic $\neq 3$ and minimal polynomial $(T - \lambda)^n$ where $\lambda \neq 0$. Find the Jordan canonical form of $J^3$.

5. In this exercise, “commutative ring” means “commutative ring with unit,” and it is assumed that a ring homomorphism $f: A \to B$ satisfies $f(1_A) = 1_B$. If $A$, $B$ and $C$ are commutative rings, we say that $C$ is a coproduct of $A$ and $B$ if there exist ring homomorphisms $\alpha: A \to C$ and $\beta: B \to C$ such that if $D$ is any commutative ring, and $f: A \to D$ and $g: B \to D$ are ring homomorphisms, there exists a unique ring homomorphism $\phi: C \to D$ such that $f = \phi \circ \alpha$ and $g = \phi \circ \beta$.

(a) If $A$ and $B$ are commutative rings, regard them as $\mathbb{Z}$-modules, and let $A \otimes \mathbb{Z} B = A \otimes \mathbb{Z} B$. Explain briefly why $A \otimes \mathbb{Z} B$ naturally has the structure of a commutative ring.

(b) Prove that $C$ is a coproduct of $A$ and $B$ if and only if $C \cong A \otimes B$. 
1. Let $G$ be a $p$-group and $H$ a nontrivial normal subgroup. Show that $H \cap Z(G)$ has at least $p$ elements.

2. Let $A \subset B$ be finite abelian groups, and let $\chi: A \rightarrow \mathbb{C}^\times$ be a homomorphism (linear character). Show that $\chi$ can be extended to $B$, and that the number of such extensions equals $[B:A]$.

3. Let $q = p^n$ where $p$ is a prime, and let $\mathbb{F}_q$ denote the finite field with $q$ elements. Show that the Frobenius automorphism $\sigma: \mathbb{F}_q \rightarrow \mathbb{F}_q$ defined by $\sigma(x) = x^p$ is diagonalizable as a linear transformation over $\mathbb{F}_p$ if and only if $n$ divides $p - 1$.

4. Determine the splitting field $K$ and Galois group $\text{Gal}(K/\mathbb{Q})$ of the polynomial $x^4 - 2$ over the field $\mathbb{Q}$. Find all quadratic extensions of $\mathbb{Q}$ contained in $K$.

5. Let $F \subset K$ be fields. Let $R$ be the polynomial ring $F[X]$, where $X$ is an indeterminate, and similarly let $S = K[X]$.

(a) Show that if $f$ and $g$ are monic polynomials in $S$, and $S/fS \cong S/gS$ as $S$-modules, then $f = g$.

(b) Show that if $x \in R$ then $S \otimes_R (R/xR) \cong S/xS$.

(c) Suppose that $M, N$ be finitely generated $R$-modules. Show that if $S \otimes_R M \cong S \otimes_R N$ as $S$-modules then $M \cong N$ as $R$-modules.
Stanford Mathematics PhD Qualifying Exam
Algebra – Spring 2006
Morning Session

1. Suppose that $H$ is a subgroup of a group $G$ of index $n$. Show that $G$ has a normal subgroup of index $\leq n!$. Use this to prove that there is no finite simple group of order $2430 = 2 \cdot 3^5 \cdot 5$.

2. Let $G$ be the following group of order 28.

   $$G = \langle x, y | x^7 = y^4 = 1, yxy^{-1} = x^{-1} \rangle.$$ 

Determine the conjugacy classes of $G$ and compute its character table.

3. (i) Suppose that $d > 1$ is a square-free integer and $d \equiv 1 \pmod{4}$. Determine (with proof) the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$.

   (ii) Explain how the principal ideals (2), (3) and (13) factor into prime ideals in the ring of algebraic integers in $\mathbb{Q}(\sqrt{13})$.

4. Find the Galois group of $x^4 + 1$ over $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$.

5. How many similarity classes are there of rational matrices with characteristic polynomial $(x^3 + 1)^3(x^2 + 1)^3$ and a minimal polynomial of degree 10?
1. Let $V$ be a finite-dimensional vector space over a field $F$ of characteristic $p$ and let $T: V \rightarrow V$ be a linear transformation such that $T^p = I$ is the identity map.

(i) Show that $T$ has an eigenvector in $V$.

(ii) Show that $T$ is upper triangular with respect to a suitable basis of $V$.

2. Let $G$ be a finite group, and let $H$ be a subgroup of index two. Let $x \in H$ and let $C_G(x)$ be the centralizer of $x$ in $G$.

(i) Prove that if $C_G(x) \not\subset H$ then the conjugacy class of $x$ in $G$ agrees equals the $H$-conjugacy class of $x$; on the other hand, if $C_G(x) \subset H$ then the conjugacy class of $x$ in $G$ is contained in $H$ but splits into two $H$-conjugacy classes.

(ii) Let $G$ be the symmetric group $S_9$ and $H$ be $A_9$. Determine the $G$-conjugacy classes of even permutations that split into two conjugacy classes in $H$. **Hint:** there are two.

3. Let $A$ be a Noetherian commutative ring containing a field $k$ and an ideal $I$ such that if $J = \sqrt{I}$ is the radical of $I$ then $A/J$ is a finite-dimensional $k$-vector space. Prove that $A/I$ is also a finite-dimensional $k$-vector space.

4. Let $G$ be a finite $p$-group, and $\lambda: G \rightarrow \mathbb{C}^\times$ a homomorphism. Assume that the order of $\lambda$ is a prime $p$, so that $H = \ker(\lambda)$ is a subgroup of index $p$. Let $\theta$ be an irreducible character of $G$ such that $\lambda\theta = \theta$. Show that $\langle \theta, H \rangle = p$ and deduce that $\theta$ is induced from a character of $H$.

5. Let $\zeta = e^{2\pi i / 7}$. Find an element $\alpha$ of $\mathbb{Q}(\zeta)$ such that $[\mathbb{Q}(\alpha): \mathbb{Q}] = 3$. Show that there does not exist $\beta \in \mathbb{Q}(\alpha)$, $\beta \notin \mathbb{Q}$ such that $\beta^3 \in \mathbb{Q}$.
1. Let $G$ be a group and $X$ and $Y$ two sets with (left) actions of $G$. We say the actions are \textit{equivalent} if there is a bijection $\phi: X \rightarrow Y$ such that $\phi(g \cdot x) = g \cdot \phi(x)$. Fix elements $x_0 \in X$ and $y_0 \in Y$. Let $H = \{g \in G \mid g \cdot x_0 = x_0\}$ and $K = \{g \in G \mid g \cdot y_0 = y_0\}$ denote the isotropy subgroups of $x_0$ and $y_0$, respectively.

(a) If the actions on $X$ and $Y$ are transitive, show the actions are equivalent if and only if $H$ and $K$ are conjugate.

(b) Let $F = \mathbb{F}_p$ where $p$ is prime, and let $G = \text{GL}(2, \mathbb{F}_p)$. Here are two sets $X$ and $Y$ with actions of $G$. The set $X$ is the projective line, consisting of all one-dimensional subspaces of the two-dimensional vector space $\mathbb{F}_p^2$, and $Y$ is the set of $p$-Sylow subgroups of $G$. Here the action of $G$ on $X$ is by matrix multiplication, and the action of $G$ on $Y$ is by conjugation. Show that these two actions are equivalent. \textbf{[Hint: Let $V = F(\begin{pmatrix} 1 \\ 0 \end{pmatrix}) \in X$. What is the isotropy subgroup of $V$?]} 

2. Show that there is a nonabelian group $G$ of order $3 \cdot 13 = 39$. Describe $G$ by generators and relations, find the conjugacy classes and construct the character table.

3. Suppose that $A$ is a commutative Noetherian ring.

(a) Prove that every ideal $\mathfrak{a}$ of $A$ contains a finite product $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ of prime ideals.

(b) Prove that $A$ has only finitely many minimal prime ideals, and that every prime ideal of $A$ contains at least one of these.

4. Let $F = \mathbb{F}_p$ where $p$ is prime. How many irreducible polynomials over $F$ are there of degrees 2, 3 and 6?

5. Consider the field of rational functions $E = \mathbb{Q}(s, t, u, v)$ in four variables. Let $F \subset E$ denote the fixed field of the obvious action of $S_4$ on $E$ permuting $\{s, t, u, v\}$. Show that $w = st + uv \in E$ has degree 3 over $F$. What is the Galois group $\text{Gal}(E/F(w))$?
1. Classify all groups of order 225 up to isomorphism.

2. Let $G$ be a finite group with center $Z(G)$. Show that the number of irreducible complex representations of $G$ is at least $|Z(G)|$. (**Hint:** first prove that if $\theta: Z(G) \rightarrow \mathbb{C}^\times$ there is an irreducible complex representation $\pi: G \rightarrow \text{GL}(V)$ such that $\pi(zg) = \theta(z)\pi(g)$ for $z \in Z(G).$)

3. (a) Suppose that $g$ is a complex matrix such that $\mathbb{C}^n$ has a basis of eigenvectors $v_1, \ldots, v_n$ such that $v_i \in \mathbb{R}^n$ and the $v_i$ are orthogonal with respect to the usual dot product, which is the symmetric bilinear form

$$
\begin{pmatrix}
    x_1 \\
    \vdots \\
    x_n
\end{pmatrix}
\begin{pmatrix}
    y_1 \\
    \vdots \\
    y_n
\end{pmatrix} = \sum_{i=1}^{n} x_i y_i.
$$

Prove that there exists a real orthogonal matrix $k = (k^t)^{-1}$ such that $kgk^{-1} = kgk^t$ is diagonal.

(b) Let $g \in \text{GL}(n, \mathbb{C})$ be a unitary symmetric matrix; that is, $g = g^t$ and $g \cdot g^t = I$. Prove that there exists a real orthogonal matrix $k = (k^t)^{-1}$ such that $kgk^{-1} = kgk^t$ is diagonal. (**Hint:** Let $\lambda$ be an eigenvalue of $g$. Observe that $|\lambda| = 1$ and show that $V_{\lambda} = \{v \in \mathbb{C}^n | gv = \lambda g\}$ is stable under complex conjugation.)

4. (a) Suppose $k$ is an infinite field, $k(\alpha, \beta)$ an algebraic extension of $k$ such that $\beta$ is separable over $k$ ($\alpha$ is not assumed separable). Let $f(x)$ and $g(x)$ denote the minimal polynomials of $\alpha$ and $\beta$ respectively over $k$. Show that there exists a $c \in k$ such that if $\theta = \alpha + c\beta$ then the polynomials $g(x)$ and $h(x) = f(\theta - cx)$ have exactly one root in common in an algebraic closure of $k$, namely $x = \beta$.

(b) Deduce that $k(\alpha, \beta) = k(\theta)$. (**Hint:** What is the greatest common divisor of the polynomials $g(x)$ and $h(x)$ in the polynomial ring $k(\theta)[x]$?)

5. Let $A$ be an integral domain with field of fractions $K$.

(a) If $m$ is a maximal ideal of $A$ then the localization $A_m$ can be regarded as a subring of $K$. Prove that

$$
A = \bigcap_{\text{maximal } m} A_m.
$$

(b) Show that if $A_m$ is a unique factorization domain for all maximal ideals $m$ then $A$ is integrally closed in $K$. 

2
1. Let $V$ be a finite-dimensional vector space over a field $F$, and let $S$ be a set of commuting linear transformations of $V$. Assume that for every $T \in S$ the characteristic polynomial of $T$ factors into linear factors over $F$, not necessarily distinct. Prove that $V$ has a basis with respect to which every $T \in S$ is represented by an upper-triangular matrix.

2. Let $K$ be a field, $p$ a prime. Let $\mu \subset K$ be the group of $p$-th roots of unity in $K$. Assume that $|\mu| = p$.

(i) Prove that the characteristic of $K$ is not equal to $p$.

(ii) Let $\sigma: K \rightarrow K$ be an automorphism of order $p$, and let $F$ be the fixed field of $\sigma$. Show that $\mu \subset F$ and deduce that $K = F(\alpha)$ for some $\alpha$ such that $\alpha^p \in F$. State any theorems you quote.

3. Let $A$ be a commutative ring and $I$ an ideal. Recall that the radical $\sqrt{I}$ is the ideal $\{x \in A|\forall n \exists\, x^n \in I\}$, and that $I$ is called primary if whenever $ab \in I$ we have either $a \in I$ or $b \in \sqrt{I}$.

(a) Let $A$ be a commutative ring, and let $I \in A$ be an ideal such that the radical $\sqrt{I}$ is maximal. Prove that $I$ is primary.

(b) Show that if $A = \mathbb{Q}[x, y]$ is a polynomial ring in two variables and $I = (x^3, x^2 + xy)$, then $\sqrt{I}$ is prime, but $I$ is not primary.

4. Classify the finite groups of order $2007 = 3^2 \cdot 223$. (Hint: 223 is prime; 222 = $2 \cdot 3 \cdot 37$.)

5. Let $G$ be the finite group of order 16 with generators and relations

$$G = \langle x, y | x^8 = y^2 = 1, yxy^{-1} = x^3 \rangle.$$ 

Find the conjugacy classes and construct the character table of $G$. 

1
1. Let $G$ be a nonabelian group of order $117 = 3^2 \cdot 13$. Show that $G$ has a normal cyclic subgroup of index 3. Find the degrees of the irreducible representations, and deduce number of conjugacy classes. (Hint: there are two possible $G$ but the answer is the same for both. You can do both cases simultaneously.)

2. Let $G$ be a finite group of odd order, and let $p$ be the smallest prime dividing $|G|$. Suppose that $G$ has a normal $p$-Sylow subgroup $P$ of order $\leq p^2$. Prove that $P$ is contained in the center of $G$.

3. Suppose that $A \subset B$ are integral domains so that the field of fractions of $B$ is algebraic over the field of fractions of $A$.

   (i) If $Q \subset B$ is a nonzero prime ideal, prove that $A \cap Q \neq 0$.

   (ii) Assume that $A$ is a principal ideal domain. Prove that every non-zero prime ideal of $B$ is maximal.

4. Let $F$ be a finite field with $q$ elements, and let $W = F^6$. Count the number of pairs $(U, V)$ where $W \supset V \supset U$, with $U$ a 2-dimensional subspace and $V$ a 4-dimensional subspace.

5. Let $p$ be a prime, $a \in \mathbb{Q}$.

   (a) Prove that either $x^p - a$ is irreducible, or it has a root in $\mathbb{Q}$. [Hint: what is the factorization of $x^p - a$ over $\mathbb{C}$?]

   (b) Show that the splitting field of $x^p - a$ over $\mathbb{Q}$ contains no primitive $p^2$ root of 1.
1. Let $G = \text{SL}_2(\mathbb{F}_q)$ where $q$ is an odd prime power. If $\ell$ is a prime dividing either $q - 1$ or $q + 1$ prove that the $\ell$-Sylow subgroup of $G$ is cyclic.

2. Let $F$ be a field and let $K$ be an algebraic closure of $F$. Let $G = \text{Gal}(K/F)$ denote the group, possibly infinite, of automorphisms of $K$ that are trivial on $F$. Use the Nullstellensatz, stating the version that you use, to exhibit a bijection between the orbits of $G$ on $K^n$ and maximal ideals in the polynomial ring $F[x_1, \cdots, x_n]$. (Prove your answer.)

3. Let $A$ be a commutative ring with unit such that (i) for every maximal ideal $m$ of $A$, the local ring $A_m$ is Noetherian and (ii) for every $0 \neq x \in A$ the set of maximal ideals of $A$ which contain $x$ is finite. Show that $A$ is Noetherian.

4. Let $V$ be a $n$-dimensional vector space over $\mathbb{F}_q$. For $1 \leq j \leq n$ determine the number of $j$-dimensional vector subspaces of $V$.

5. Let $G$ be a cyclic group of order $p^n$ where $p$ is prime. Let $V$ be a finite-dimensional vector space of dimension $n$ over $\mathbb{F}_p$. We say that a representation $\sigma : G \rightarrow \text{GL}(W)$ is indecomposable if it is not a direct sum of nontrivial invariant subspaces. Show that if $\pi : G \rightarrow \text{GL}(V)$ is any representation on a finite dimensional vector space over $\mathbb{F}_p$ then $V$ is a direct sum of invariant subspaces $W_i$ such that the restriction of $\pi$ to $W_i$ is an indecomposable representation. Show that the number and dimensions of the $W_i$ are determined by $\pi$. Make explicit what an indecomposable $W_i$ looks like. [Hint: this is essentially a question of linear algebra. If $x$ is a generator of $G$, consider $\pi(x)$ as a linear transformation.]
1. Let $G$ be a group of order $p^r$ where $p$ is prime and $r \geq 3$. Show that $p$ divides $|\text{Aut}(G)|$ and that $|\text{Aut}(G)| \geq p^2$.

2. (a) Find (with proof) the Galois group of $x^9 - 2$ over $\mathbb{Q}$.
(b) Find (with proof) the Galois group of $x^9 - 2$ over $\mathbb{F}_3$, $\mathbb{F}_5$, and $\mathbb{F}_7$.

3. Find all algebraic integers in the field $\mathbb{Q}[\sqrt{10}]$. For which primes $p$ in $\mathbb{Z}$ does $p$ generate a prime ideal in this ring of integers? (Prove your answer.)

4. Let $F$ be a field and $E \supset F$ an extension field.
   (i) If $M, N \in \text{GL}_n(F)$ are conjugate in $\text{GL}_n(E)$ show that they are conjugate in $\text{GL}_n(F)$.
   (ii) Give an example of two matrices in $\text{SL}_2(\mathbb{R})$ that are conjugate in $\text{SL}_2(\mathbb{C})$ but not in $\text{SL}_2(\mathbb{R})$.

5. Let $G$ be the group of order 24 with the following generators and relations:
   \[ \langle x^2 = y^2 = (xy)^2 = 1, z^6 = 1, zxz^{-1} = y, zyz^{-1} = xy \rangle. \]
Find the eight conjugacy classes of $G$ and compute its character table.
1. Let $G = \text{SL}_2(\mathbb{F}_q)$ where $q$ is an odd prime power. If $\ell$ is a prime dividing either $q - 1$ or $q + 1$ prove that the $\ell$-Sylow subgroup of $G$ is cyclic.

2. Let $F$ be a field and let $K$ be an algebraic closure of $F$. Let $G = \text{Gal}(K/F)$ denote the group, possibly infinite, of automorphisms of $K$ that are trivial on $F$. Use the Nullstellensatz, stating the version that you use, to exhibit a bijection between the orbits of $G$ on $K^n$ and maximal ideals in the polynomial ring $F[x_1, \cdots, x_n]$. (Prove your answer.)

3. Let $A$ be a commutative ring with unit such that (i) for every maximal ideal $m$ of $A$, the local ring $A_m$ is Noetherian and (ii) for every $0 \neq x \in A$ the set of maximal ideals of $A$ which contain $x$ is finite. Show that $A$ is Noetherian.

4. Let $V$ be and $n$-dimensional vector space over $\mathbb{F}_q$. For $1 \leq j \leq n$ determine the number of $j$-dimensional vector subspaces of $V$.

5. Let $G$ be a cyclic group of order $p^n$ where $p$ is prime. Let $V$ be a finite-dimensional vector space of dimension $n$ over $\mathbb{F}_p$. We say that a representation $\sigma : G \rightarrow \text{GL}(W)$ is indecomposable if it is not a direct sum of nontrivial invariant subspaces. Show that if $\pi : G \rightarrow \text{GL}(V)$ is any representation on a finite dimensional vector space over $\mathbb{F}_p$ then $V$ is a direct sum of invariant subspaces $W_i$ such that the restriction of $\pi$ to $W_i$ is an indecomposable representation. Show that the number and dimensions of the $W_i$ are determined by $\pi$. Make explicit what an indecomposable $W_i$ looks like. [Hint: this is essentially a question of linear algebra. If $x$ is a generator of $G$, consider $\pi(x)$ as a linear transformation.]
Stanford Mathematics PhD Qualifying Exam
Algebra – Fall 2008
Afternoon Session

1. Let $G$ be a group of order $p^r$ where $p$ is prime and $r \geq 3$. Show that $p$ divides $|\text{Aut}(G)|$ and that $|\text{Aut}(G)| \geq p^2$.

2. (a) Find (with proof) the Galois group of $x^9 - 2$ over $\mathbb{Q}$.
(b) Find (with proof) the Galois group of $x^9 - 2$ over $\mathbb{F}_3$, $\mathbb{F}_5$, and $\mathbb{F}_7$.

3. Find all algebraic integers in the field $\mathbb{Q}[\sqrt{10}]$. For which primes $p$ in $\mathbb{Z}$ does $p$ generate a prime ideal in this ring of integers? (Prove your answer.)

4. Let $F$ be a field and $E \supset F$ an extension field.
   (i) If $M, N \in \text{GL}_n(F)$ are conjugate in $\text{GL}_n(E)$ show that they are conjugate in $\text{GL}_n(F)$.
   (ii) Give an example of two matrices in $\text{SL}_2(\mathbb{R})$ that are conjugate in $\text{SL}_2(\mathbb{C})$ but not in $\text{SL}_2(\mathbb{R})$.

5. Let $G$ be the group of order 24 with the following generators and relations:
   \[
   \langle x^2 = y^2 = (xy)^2 = 1, z^6 = 1, zxz^{-1} = y, zyz^{-1} = xy \rangle.
   \]
   Find the eight conjugacy classes of $G$ and compute its character table.
1. Let $k$ be a finite field of size $q$.

(a) Prove that the number of $2 \times 2$ matrices over $k$ satisfying $T^2 = 0$ is $q^2$.

(b) Prove that the number of $3 \times 3$ matrices over $k$ satisfying $T^3 = 0$ is $q^6$.

2. (a) Prove that if $K$ is a field of finite degree over $\mathbb{Q}$ and $x_1, \ldots, x_n$ are finitely many elements of $K$ then the subring $\mathbb{Z}[x_1, \ldots, x_n]$ they generate over $\mathbb{Z}$ is not equal to $K$. (Hint: Show they all lie in $O_K[1/a]$ for a suitable nonzero $a$ in $O_K$, where $O_K$ denotes the integral closure of $\mathbb{Z}$ in $K$.)

(b) Let $m$ be a maximal ideal of $\mathbb{Z}[x_1, \ldots, x_n]$ and $F = \mathbb{Z}[x_1, \ldots, x_n]/m$. Use (a) and the Nullstellensatz to show that $F$ cannot have characteristic 0, and then deduce for $p = \text{char}(F)$ that $F$ is of finite degree over $\mathbb{F}_p$ (so $F$ is actually finite).

3. Let $E$ be the splitting field of

$$f(x) = (x^7 - 1)/(x - 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

over $\mathbb{Q}$. Let $\zeta$ be a zero of $f(x)$, i.e. a primitive seventh root of 1.

(a) Show that $f(x)$ is irreducible over $\mathbb{Q}$. (Hint: consider $f(y + 1)$ and use Eisenstein’s criterion.)

(b) Show that the Galois group of $E/\mathbb{Q}$ is cyclic, and find an explicit generator.

(c) Let $\beta = \zeta + \zeta^2 + \zeta^4$. Show that the intermediate field $\mathbb{Q} (\beta)$ is actually $\mathbb{Q} (\sqrt{-7})$. (Hint: first show that $[\mathbb{Q} (\beta) : \mathbb{Q}] = 2$ by finding a linear dependence over $\mathbb{Q}$ among $\{1, \beta, \beta^2\}$.)

(d) Let $\gamma_q = \zeta + \zeta^q$. Find (with proof) a $q$ such that $\mathbb{Q} (\gamma_q)$ is a degree 3 extension of $\mathbb{Q}$. (Hint: use (b).) Is this extension Galois?

4. Let $G$ be a nontrivial finite group and $p$ be the smallest prime dividing the order of $G$. Let $H$ be a subgroup of index $p$. Show that $H$ is normal. (Hint: If $H$ isn’t normal, consider the action of $G$ on the conjugates of $H$.)

5. Let $G$ be a finite group and $\pi : G \to \text{GL}(V)$ a finite-dimensional complex representation. Let $\chi$ be the character of $\pi$. Show that the characters of the representations on $V \otimes V$, $\text{Sym}^2(V)$ and $\wedge^2(V)$ are $\chi(g)^2$, $(\chi(g)^2 + \chi(g^2))/2$ and $(\chi(g)^2 - \chi(g^2))/2$. (Hint: Express $\chi(g)^2$, $(\chi(g)^2 + \chi(g^2))/2$ and $(\chi(g)^2 - \chi(g^2))/2$ in terms of the eigenvalues of $\pi(g)$.)
This part has five problems on two pages.

1. Let \( V \) be a vector space over a field \( F \), and let \( B : V \times V \to F \) be a symmetric bilinear form. This means that \( B \) is bilinear and \( B(x, y) = B(y, x) \). Let \( q(v) = B(v, v) \).

   (a) Show that if the characteristic of \( F \) is not 2 then \( B(v, w) = \frac{1}{2}(q(v+w) - q(v) - q(w)) \).
   (This obviously implies that if \( q = 0 \) then \( B = 0 \).)

   (b) Give an example where the characteristic of \( F \) is 2 and \( q = 0 \) but \( B \neq 0 \).

   (c) Show that if the characteristic of \( F \) is not 2 or 3 and if \( B(u, v, w) \) is a symmetric trilinear form, and if \( r(v) = B(v, v, v) \), then \( r = 0 \) implies \( B = 0 \).

2. Let \( G \) be a finite group.

   (a) Let \( \pi : G \to \text{GL}(V) \) be an irreducible complex representation, and let \( \chi \) be its character. If \( g \in G \), show that \( |\chi(g)| = \dim(V) \) if and only if there is a scalar \( c \in \mathbb{C} \) such that \( \pi(g)v = cv \) for all \( v \in V \).

   (b) Show that \( g \) is in the center \( Z(G) \) if and only if \( |\chi(g)| = \chi(1) \) for every irreducible character \( \chi \) of \( G \).

3. Let \( V \) be a vector space of finite dimension \( d \geq 1 \) over a field \( k \) of arbitrary characteristic. Let \( V^* \) denote the dual space.

   (a) For any \( n \geq 1 \), prove that there is a unique bilinear pairing \( V^\otimes n \times (V^*)^\otimes n \to k \) satisfying
   \[
   (v_1 \otimes \cdots \otimes v_n, \ell_1 \otimes \cdots \otimes \ell_n) \mapsto \prod \ell_i(v_i),
   \]
   and by using bases show that it is a perfect pairing (i.e., identifies \( (V^*)^\otimes n \) with \( (V^\otimes n)^* \)).

   (b) For any \( 1 \leq n \leq d \), do similarly with \( \wedge^n(V) \) and \( \wedge^n(V^*) \) using the requirement
   \[
   (v_1 \wedge \cdots \wedge v_n, \ell_1 \wedge \cdots \wedge \ell_n) \mapsto \det(\ell_i(v_j)).
   \]

4. Let \( K/k \) be a finite extension of fields with \( \alpha \in K \) as a primitive element over \( k \). Let \( f \in k[x] \) be the minimal polynomial of \( \alpha \) over \( k \).

\[ Date: \] Thursday, September 17, 2009. \]
(a) Explain why \( K \simeq k[x]/(f) \) as \( k \)-algebras, and use this to relate the local factor rings of \( K \otimes_k F \) to the irreducible factors of \( f \) in \( F[x] \), with \( F/k \) a field extension.

(b) Assume \( K/k \) is Galois with Galois group \( G \). Prove that the natural map \( K \otimes_k K \rightarrow \prod_{g \in G} K \) defined by \( a \otimes b \mapsto (g(a)b) \) is an isomorphism.

5. Let \( G \) be a finite abelian group, \( \omega : G \times G \rightarrow \mathbb{R}/\mathbb{Z} \) a bilinear mapping so that

(i) \( \omega(g, g) = 0 \) for all \( g \) in \( G \);
(ii) \( \omega(x, g) = 0 \) for all \( g \) if and only if \( x \) is the identity element.

Prove that the order of \( G \) is a square. Give an example of \( G \) of square order for which no such \( \omega \) exists.

\textit{Hint:} Consider a subgroup \( A \) of \( G \) which is maximal for the property that \( \omega(x, y) = 0 \) for \( x, y \) in \( A \). You may use the following fact without proof: any finite abelian group \( X \) admits \( |X| \) distinct homomorphisms to \( \mathbb{R}/\mathbb{Z} \).
ALGEBRA QUAL, SPRING 2009, PART I

1. (a) [5 points] Prove that if \( A \) is a commutative noetherian ring then the polynomial ring \( A[T] \) is noetherian. (That is, prove the 'Hilbert Basis Theorem'.)

(b) [3 points] Suppose \( k \) is a field and \( B \) is a commutative ring finitely generated over \( k \). Let \( S \subset B \) be a multiplicative set. Explain why the localization \( S^{-1}B \) is a noetherian ring.

(c) [2 points] Give an example (with proof) of the situation in part (b) where \( S^{-1}B \) is not finitely generated over \( k \) as a ring.

2. Let \( k \) be a field, \( f(x) \in k[x] \) a monic, non-constant polynomial.

(a) [2 points] Define what it means for a field \( K \supset k \) to be a splitting field of \( f(x) \) over \( k \).

(b) [8 points] Prove the existence of such a splitting field \( K \), and the uniqueness of \( K \) up to isomorphism over \( k \).

3. Let \( K \) be a splitting field for \( x^4 - 7 \) over \( Q \).

(a) [5 points] Determine \( [K : Q] \) and give field generators for \( K \) over \( Q \). Describe \( G = Gal(K/Q) \) in terms of generators and relations, and describe how the group generators of \( G \) act on the field generators of \( K \).

(d) [5 points] List all intermediate fields \( L \) with \( Q \subset L \subsetneq K \), their degrees over \( Q \), and the inclusion relations that hold between the fields \( L \). The fields \( L \) should be named in terms of generators over \( Q \).

4. Consider the finite groups \( SL(2, F_3) \) and \( PSL(2, F_5) = SL(2, F_5)/\{\pm I \} \). In the following problem, you are not allowed to use the fact that \( PSL(2, F_5) \) is isomorphic to a more familiar group, unless you give a complete proof of that fact.

(a) [2 points] Calculate \( |SL(2, F_3)| \). Explain why \( SL(2, F_3) \nsubsetneq S_5 \), the symmetric group.

(b) [3 points] Show that there are no elements of order 15 in \( PSL(2, F_5) \).

[Hint: Work in \( SL(2, F_3) \).]

(c) [5 points] Exhibit a 3-Sylow subgroup and a 5-Sylow subgroup of \( PSL(2, F_5) \) and determine (with proof) the number of distinct 3-Sylow subgroups and 5-Sylow subgroups.

[Hint: Part (b) is useful for (c), but there are various approaches.]
5. Let $Q[x_1, \ldots, x_k]$ be the polynomial ring in $k$ variables over $Q$, and let $\overline{Q}$ be the algebraic closure of $Q$, say inside $C$. A special case of the weak Nullstellensatz states that if $I \subset Q[x_1, \ldots, x_k]$ is any proper ideal, then

$$V(I) = \{ \overline{\gamma} = (\gamma_1, \ldots, \gamma_k) \in (\overline{Q})^k \mid f(\overline{\gamma}) = 0 \text{ for all } f \in I \} \neq \emptyset.$$  

(a) [3 points] Use the weak Nullstellensatz in the form stated above to prove the strong Nullstellensatz, in the form that for any proper ideal $J \subset Q[x_1, \ldots, x_n]$ the radical $\sqrt{J}$ is given by

$$\sqrt{J} = \{ g \in Q[x_1, \ldots, x_n] \mid g(\overline{\gamma}) = 0 \text{ for all } \overline{\gamma} \in V(J) \subset (\overline{Q})^n \}.$$  

[Hint: Make use of $k = n+1$ in the weak Nullstellensatz.]

(b) [2 points] Explain why $\sqrt{J}$ is the intersection of all maximal ideals $Q \subset Q[x_1, \ldots, x_n]$ with $J \subset Q$.

(c) [5 points] If $P \subset Q[x_1, \ldots, x_n]$ is a minimal nonzero prime ideal, prove that $P = (f)$, where $f \in Q[x_1, \ldots, x_n]$ is irreducible. Then prove that there is a $j$, $1 \leq j \leq n$, so that the $n - 1$ elements $\{ \overline{x_i} = x_i \mod P \mid i \neq j \}$ are algebraically independent over $Q$ in the integral domain $Q[x_1, \ldots, x_n]/P$. 
ALGEBRA QUAL, SPRING 2009, PART II

1. (a) [2 points] Prove that every finite field $\mathbb{F}$ has order $q = p^n$ for some prime integer $p$ and some integer $n \geq 1$.

(b) [5 points] Prove that for each such $q = p^n$ there is up to isomorphism exactly one field $\mathbb{F}_q$ of order $q$.

[You may use the existence and uniqueness of splitting fields of polynomials.]

(c) [3 points] Prove that $K = \mathbb{F}_3[x]/(x^2 + x - 1)$ and $K' = \mathbb{F}_3[y]/(y^2 + 1)$ are fields and exhibit an explicit isomorphism between them.

2. Suppose $G_1$ and $G_2$ are groups and $H \leq G_1 \times G_2$ is a subgroup so that the two compositions

$p_1 : H \rightarrow G_1 \\
p_2 : H \rightarrow G_2$

are surjections. Let $N_1 = \text{ker}(p_2)$ and $N_2 = \text{ker}(p_1)$. Thus, if $e_1 \in G_1$ and $e_2 \in G_2$ are the identity elements then

$N_1 = H \cap (G_1 \times \{e_2\}) \subset G_1 \times \{e_2\}$

$N_2 = H \cap (\{e_1\} \times G_2) \subset \{e_1\} \times G_2.$

(a) [5 points] Show that $N_1 \triangleleft G_1 \times \{e_2\}$ and $N_2 \triangleleft \{e_1\} \times G_2$ are normal subgroups.

(b) [5 points] Show that

$\frac{G_1 \times \{e_2\}}{N_1} \simeq \frac{\{e_1\} \times G_2}{N_2}.$

3. Let $T : V \rightarrow V$ be a linear endomorphism of a non-zero finite dimensional vector space over $\mathbb{C}$.

(a) [4 points] State precisely the theorem on the existence and uniqueness of a Jordan canonical form for $T$, and prove it using the structure theorem for modules over a PID.

(b) [2 points] Using the Jordan form, prove that $T = T_s + T_n$, where $T_s : V \rightarrow V$ is diagonalizable and $T_n : V \rightarrow V$ is nilpotent, and where $T_sT_n = T_nT_s$.

(c) [4 points] It is a fact that the $T_s$ and $T_n$ from part (b) can be expressed as polynomials in $T$ with coefficients in $\mathbb{C}$. You don't need to prove this fact, but assuming it, prove that there is a unique decomposition $T = T'_s + T'_n$, where $T'_s$ is diagonalizable, $T'_n$ is nilpotent, and $T'_sT'_n = T'_nT'_s$. 

3
4. Let \( Q \subset E \) be a finite Galois extension and let \( B \subset E \) be the ring of algebraic integers in \( E \). Suppose \( P \subset B \) is a non-zero prime ideal with \( P \cap \mathbb{Z} = (p) \), a prime ideal in \( \mathbb{Z} \). Set \( \overline{E} = B/P \) and suppose \( \xi \in \overline{E} \) is a primitive generator for \( \overline{E} \) over \( \mathbb{F}_p = \mathbb{Z}/p \).

(a) [3 points] Explain why there exists \( x \in B \) such that \( \xi \equiv x \mod P \in B/P = \overline{E} \) and such that \( x \in \tau P \subset B \) for all \( \tau \in Gal(E/Q) \) with \( \tau P \neq P \).

(b) [7 points] If \( G_P = \{ \sigma \in Gal(E/Q) \mid \sigma P = P \} \subset Gal(E/Q) \), prove that the obvious homomorphism \( G_P \to Gal(\overline{E}/\mathbb{F}_p) \) is surjective.

5. Suppose that \( A \) is a noetherian integral domain. Suppose further that for every maximal ideal \( Q \subset A \), the quotient \( Q/Q^2 \) is a one dimensional vector space over the field \( A/Q \).

(a) [5 points] Prove that every non-zero prime ideal of \( A \) is maximal.

[Hint: Prove something about the localizations \( A_q \) for maximal ideals \( Q \).

(b) [5 points] Prove that \( A \) is integrally closed.

[In both (a) and (b), give precise statements of any lemmas you use.]
1. Part I

(1) (a) Explicitly exhibit an element \( \sigma \) of \( G = \text{GL}(2, \mathbb{Z}/7\mathbb{Z}) \) of order 8.
(b) Describe, with proof, the structure of the 2-Sylow subgroup of \( G \).

*Hint:* think about the multiplicative group of the field of size 49, and the action of the nontrivial automorphism of this field.

(2) Let \( V, W \) be vector spaces over an algebraically closed field \( k \), with \( \dim(V) = 6 \) and \( \dim(W) = 9 \). Suppose \( T : V \to V, S : W \to W \) are linear transformations whose minimal polynomials are, respectively, \( T^6 = 0 \) and \( S^9 = 0 \).

Consider the linear transformation \( S \otimes T : W \otimes V \to W \otimes V \).
(i) What is the minimal polynomial of \( S \otimes T \)?
(ii) What is the dimension of \( \ker(S \otimes T) \)?
(iii) Describe the Jordan normal form of \( S \otimes T \) (i.e., number of blocks, and their sizes).

*Hint:* You should not need to write down any matrices.

(3) Suppose \( A \) and \( B \) are commutative rings containing a field \( k \), with \( B \) finitely generated over \( k \) as a ring. If \( \phi : A \to B \) is a ring homomorphism with \( \phi|_k = 1_d \) and if \( Q \subset B \) is a maximal ideal, prove that \( \phi^{-1}(Q) \subset A \) is a maximal ideal.

(4) Let \( \alpha \) be a root of \( x^7 - 12 \) and \( \zeta \) a primitive 7th root of unity, both in \( \mathbb{C} \).
(a) Explain why the powers \( \{ \alpha^j \} \) are linearly independent over the field \( \mathbb{Q}[\zeta] \).
(b) If \( \beta \in \mathbb{Q}[\alpha] \) has a conjugate of the form \( \zeta^i \beta (0 < i < 7) \) in the algebraic closure of \( \mathbb{Q} \), explain why \( \beta = c \alpha^j \) for some rational number \( c \) and some \( j \) with \( 0 < j < 7 \).
(c) Show, using the results of the prior parts, that \( x^7 - 11 \) has no root in \( \mathbb{Q}(\alpha) \).

(5) Let \( R \) be a ring and

\[
\cdots \xrightarrow{d} F_j \xrightarrow{d} F_{j-1} \xrightarrow{d} \cdots \xrightarrow{d} F_1 \xrightarrow{d} F_0 \xrightarrow{d} 0 \xrightarrow{d} 0 \xrightarrow{d} 0 \cdots
\]

a complex of free \( R \)-modules.
(a) Show that this complex is exact (i.e., has vanishing homology) if and only if there exists degree 1 homomorphism \( h : F_s \to F_s \) (i.e., a collection of \( R \)-module homomorphisms \( h_j : F_j \to F_{j+1} \)) so that \( dh + hd \) is the identity on the complex \( F_s \).
(b) In this case, show that \( \text{Hom}(F_s, M) \) has vanishing cohomology for any module \( M \).
(c) Give counterexamples to both statements if \( F_s \) is exact but not free.
2. PART II

(1) Find a root of unity $\zeta$ so that $\mathbb{Q}(\zeta)$ contains a subfield $K$ which is Galois over $\mathbb{Q}$ with Galois group $\mathbb{Z}/3\mathbb{Z}$. Compute the minimal polynomial over $\mathbb{Q}$ of an element that generates $K$ over $\mathbb{Q}$.

(2) (i) Prove that if a nonzero ideal $I$ in a domain $R$ is free as an $R$-module then $I$ is principal. As an application, for $R = \mathbb{Z}[\sqrt{-5}]$ prove that neither of the ideals $P = (3, 1 + \sqrt{-5})$ nor $Q = (3, 1 - \sqrt{-5})$ is free. *Hint*: Use norms!
(ii) Prove that $P \cap Q = 3R$, and that the addition map $P \oplus Q \to R$ defined by $(a, b) \mapsto a + b$ is surjective.
(iii) Deduce that $P \oplus Q \cong R^2$ as $R$-modules, so a direct summand of a free module need not be free as an $R$-module!

(3) Let $G$ be a finite group and $H$ a subgroup whose index is prime to $p$. Suppose $V$ is a finite-dimensional representation of $G$ over $\mathbb{F}_p$ whose restriction to $H$ is semisimple. Prove that $V$ is semisimple. *Hint*: Imitate the proof of Maschke’s theorem.

(4) (i) If $A$ is a commutative Noetherian ring, prove the power series ring $A[[x]]$ is Noetherian.
(ii) If $A$ is a commutative Artin ring, that is, if the ideals satisfy the descending chain condition, prove that every prime ideal $P \subset A$ is maximal and that there are only finitely many prime ideals. *Hints*: If $x \notin P$, consider the ideals $(x^n)$; consider also finite products of prime ideals.

(5) Let $K$ be an algebraically closed field and let $V \subset K^n, W \subset K^m$ be irreducible algebraic sets. Prove that $V \times W \subset K^{n+m}$ is an irreducible algebraic set.