Answer five (5) questions only. You must answer at least one from each of groups, rings, and fields. Be sure to show enough work that your answers are adequately supported.

Groups
For all groups questions below, \( \mathbb{Z} \) denotes the group of integers under addition; \( \mathbb{Z}_n \) denotes the group of integers modulo \( n \) under addition; \( S_n \) denotes the symmetric group on \( n \) letters; and \( A_n \) denotes the alternating group on \( n \) letters.

(A) Let \( G \) be a cyclic group. Prove the following:
(a) If \( G \) is infinite, then \( G \) is isomorphic to \( \mathbb{Z} \).
(b) If \( G \) is finite, then \( G \) is isomorphic to \( \mathbb{Z}_n \) for some \( n \).

(B) Suppose \( G \) is a nonabelian group with order \( p^3 \), where \( p \) is a prime. Show that the commutator subgroup of \( G \) has order \( p \).
You may use the following two facts without proving them: (i) If \( G/Z \) is cyclic, where \( Z \) is the center of \( G \), then \( G \) is abelian. (ii) If a group \( Q \) has order \( p^2 \), then \( Q \) is abelian.
Answer: [See S04] Let \( Z = Z(G) \) be the commutator subgroup of \( G \). The order of \( Z \) must divide \( p^3 \) so \( |Z| \) is 1, \( p \), \( p^2 \) or \( p^3 \).
(a) If \( |Z| = p^3 \), then \( G = Z \) is abelian, contrary to hypothesis.
(b) If \( |Z| = p^2 \), then \( G/Z \) is cyclic of order \( p \). By the quoted theorem this implies that \( G \) is abelian and so \( Z = G \) — a contradiction.
(c) If \( |Z| = 1 \), then this contradicts the theorem that the center of a nontrivial \( p \)-group is nontrivial (Fraleigh, Theorem 37.4, p. 329).
We have eliminated all possibilities for the order of the commutator except \( |Z| = p \).

(C) Suppose that \( \phi \) is a surjective group homomorphism from \( S_n \) to \( \mathbb{Z}_2 \) with kernel \( G \). Show that \( G = A_n \). [Hint: the set of all transpositions forms a conjugacy class in \( S_n \).]
Answer: Let \( a \) and \( b \) be transpositions. Since the transpositions form a single conjugacy class, we have \( a = gbg^{-1} \) for some \( g \in S_n \). Mapping this equation to the abelian group \( \mathbb{Z}_2 \) we get
\[
\phi(a) = \phi(g)\phi(b)\phi(g)^{-1} = \phi(b).
\]
Thus all transpositions get sent to the same element of \( \mathbb{Z}_2 \).

If \( \phi(a) = 0 \) for all transpositions \( a \in S_n \), then, because every element of \( S_n \) is a product of transpositions, the kernel of \( \phi \) is \( S_n \), contrary to assumption.

Hence we have \( \phi(a) = 1 \) for all transpositions \( a \in S_n \). Now, if \( g \in S_n \) is a product of an even number of transpositions, then \( \phi(g) \) is the sum of an even number of 1s, and so \( \phi(g) = 0 \). And, if \( g \in S_n \) is a product of an odd number of transpositions, then \( \phi(g) \) is the sum of an odd number of 1s, and so \( \phi(g) = 1 \). In other words, the kernel of \( \phi \) is \( A_n \), and \( G = A_n \).

Rings
For all rings questions below, \( \mathbb{Z}_n \) denotes the ring of integers modulo \( n \).
(A) Consider the ring \( \mathbb{Z}_n \) where \( n \geq 2 \). Let \( I \) be a subset of \( \mathbb{Z}_n \). Prove that \( I \) is an ideal of \( \mathbb{Z}_n \) if and only if
\[
I = \langle k \rangle = \{ ak \mid a \in \mathbb{Z} \}
\]
for some \( k \in \mathbb{Z}_n \).

**Answer:** Since \( I = \{ ak \mid a \in \mathbb{Z} \} \) is closed under subtraction and multiplication by elements of \( \mathbb{Z}_n \), \( I \) is an ideal. (Alternatively, since we are given that \( I = \langle k \rangle \) which means that \( I \) is, by definition, the smallest ideal containing \( k \), there is nothing to prove in this direction.)

Conversely, let \( J \) be an ideal of \( \mathbb{Z}_n \). If \( J = \{0\} \), then setting \( k = 0 \), \( J \) has the claimed form. If \( J \neq \{0\} \), let \( k \) be the least nonzero number in \( J \). Then \( \langle k \rangle \subseteq J \) is clear. For the opposite inclusion, suppose that \( a \in J \). Then \( a = qk + r \) for some integers \( q, r \) such that \( 0 \leq r < k \). Because \( r = a - qk \) with \( a, k \in J \) we have \( r \in J \). By the minimality of \( k \), this is possible only if \( r = 0 \). In this circumstance, \( a = qk \in \langle k \rangle \). This shows that \( J = \langle k \rangle \) for some \( k \in \mathbb{Z}_n \).

(B) Prove that \( \mathbb{Z}_9 \) is not isomorphic to a direct product of fields. [Hint: Count zero-divisors.]

**Answer:** The only direct product of fields that has 9 elements is \( \mathbb{Z}_3 \times \mathbb{Z}_3 \). Since \( \mathbb{Z}_9 \) has two zero divisors, namely, \( \{3, 6\} \), whereas \( \mathbb{Z}_3 \times \mathbb{Z}_3 \) has four zero divisors, namely \( \{(1, 0), (2, 0), (0, 1), (0, 2)\} \), these rings cannot be isomorphic.

(C) Let \( R \) be a ring with identity 1 and \( a, b \in R \) such that \( ab = 1 \). Let
\[
X = \{ x \in R \mid ax = 1 \}.
\]
Show the following.

(a) If \( x \in X \), then \( b + 1 - xa \in X \).

(b) If \( \phi : X \to X \) is defined by \( \phi(x) = b + 1 - xa \) for \( x \in X \), then \( \phi \) is injective (one-to-one).

(c) \( X \) contains either exactly one element or infinitely many elements. [Hint: Consider two cases, depending on whether \( ba = 1 \) or \( ba \neq 1 \). In the case where \( ba \neq 1 \), show that \( b \) is not in the image of \( \phi \).]

**Answer:** [See S07] Note: We are not assuming that \( R \) is commutative. The published exam has a typo that has been corrected here.

(a) If \( x \in X \), then \( ax = 1 \). Consequently,
\[
ab + a - axa = 1 + a - 1a = 1,
\]
and so \( b + 1 - xa \in X \).

(b) Suppose that \( x_1, x_2 \in X \) satisfy \( \phi(x_1) = \phi(x_2) \). Then \( b + 1 - x_1a = b + 1 - x_2a \). Canceling \( b + 1 \) from this equation gives \( x_1a = x_2a \). Then multiplying by \( b \) on the right and using \( ab = 1 \) gives \( x_1 = x_2 \). Thus \( \phi \) is injective.

(c) Note first that, since \( ab = 1 \), we have \( b \in X \). If \( X \) is infinite, we are done. Otherwise, suppose that \( X \) is finite. Since \( \phi : X \to X \) is injective, this implies that \( \phi \) is surjective, and so there is some \( x_b \in X \) such that \( \phi(x_b) = b \), that is, \( b + 1 - x_ba = b \). Canceling from this we get \( x_ba = 1 \). Multiplying this on the right by \( b \) and using \( ab = 1 \) gives \( x_b = b \). So we have \( \phi(b) = b \), and \( ba = 1 \).

Now we show that \( b \) is the only element of \( X \). If \( x \in X \), then \( ax = 1 \). Multiplying on the right by \( b \) and using \( ba = 1 \) gives \( x = b \). Thus \( X = \{b\} \).
Notice that what we have proved is that if \( a \in R \) has an inverse \( b \) on one side, then either \( b \) is a two-sided inverse of \( a \) (i.e. \( ab = ba = 1 \)), or \( a \) has infinitely many one-sided inverses.

**Fields**

For all fields questions below, \( \mathbb{Z}_n \) denotes the ring of integers modulo \( n \); \( \mathbb{Q} \) denotes the ring of rational numbers; and \( \mathbb{C} \) denotes the ring of complex numbers.

(A) Let \( p \) be a prime and \( n \geq 1 \). Prove that there exists a field of size \( p^n \). [Hint: Consider the polynomial \( x^{p^n} - x \) over \( \mathbb{Z}_p \).]


(B) Let \( \sigma = e^{2\pi i/7} \in \mathbb{C} \), a primitive seventh root of unity, and \( F = \mathbb{Q}(\sigma) \). Describe the Galois group of \( F \) over \( \mathbb{Q} \). Explain what theorems you are using.

Answer: The minimum polynomial for \( \sigma \) over \( \mathbb{Q} \) is the seventh cyclotomic polynomial \( \Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \). The other zeros of this polynomial are \( \sigma^k \) with \( k = 2, 3, 4, 5, 6 \), and these zeros are all in \( F \). This means that \( F \) is the splitting field for \( \Phi_7 \), and that \( F \) is Galois over \( \mathbb{Q} \).

Each automorphism of \( F \) over \( \mathbb{Q} \) sends \( \sigma \) to one of its conjugates and is uniquely determined by this conjugate. Thus there six automorphisms. Let \( \phi \) be the automorphism of \( F \) over \( \mathbb{Q} \) that sends \( \sigma \) to \( \sigma^3 \). Then \( \phi^2(\sigma) = \phi(\sigma^3) = \sigma^2 \), \( \phi^3(\sigma) = \sigma^6 \), \( \phi^4(\sigma) = \sigma^4 \), \( \phi^5(\sigma) = \sigma^5 \) and \( \phi^6(\sigma) = \sigma \). Thus each of the six automorphisms is a power of \( \phi \). In other words, the Galois group is cyclic of order 6 with \( \phi \) as generator.

(C) Find the minimal polynomial of \( \sqrt[3]{2} + \sqrt{2} \) over \( \mathbb{Q} \), and prove it is the minimal polynomial.

Answer: Set \( \alpha = \sqrt[3]{2} + \sqrt{2} \). Then \( \alpha^3 = 2 + \sqrt{2} \) and \( (\alpha^3 - 2)^2 = 2 \). Thus \( \alpha \) is a root of the polynomial \( f(x) = (x^3 - 2)^2 - 2 = x^6 - 4x^3 + 2 \). This polynomial is irreducible over \( \mathbb{Q} \) by Eisenstein with \( p = 2 \) and so \( f \) is the minimal polynomial for \( \alpha \) over \( \mathbb{Q} \).