Final Exam: Math 100C, Spring 2024

You have 180 minutes.

You are not permitted to use calculators, books, or notes.

YOU MUST SHOW ALL YOUR WORK TO RECEIVE CREDIT,
(unless a problem specifies otherwise)

Name _____

"I have adhered to UCSD policies on academic integrity while completing this examination."

Signature _____

There are 10 regular problems, worth 20 points each, and two bonus problems, worth 10 points each.

Good luck!

Problem 1. *(20 points) Let F be a field and V a finite-dimensional F vector space. Suppose that A and B are linear maps from V to V that commute. Recall that a linear map $T : V \to V$ is said to be* ***diagonalizable*** *if there is a basis $e_1, \ldots, e_n$ of V and elements $\lambda_1, \ldots, \lambda_n \in F$ so that $Te_j = \lambda_j e_j$ for all j. Suppose that A is diagonalizable on V with* ***distinct eignenvalues****. That is, there is a basis $b_1, \ldots, b_n$ of V and $\alpha_1, \ldots, \alpha_n \in F$ so that $Ab_j = \alpha_j b_j$ for all j, and $\alpha_i \neq \alpha_j$ if $i \neq j$. Prove that B is diagonalizable on V.*

Proof. Observe that, if $v \in V$ and $Av = \alpha_j v$, then necessarily v is in the line Fb_j. This is because the α_j are distinct. Now $A(Bb_j) = BAb_j = \alpha_j Bb_j$, so $Bb_j \in Fb_j$. Thus B is diagonalizable on V, with eigenvectors the b_j. □

Problem 2. *(20 points) Let F be a field, $n > 1$ a positive integer, and V an n-dimensional F vector space. Suppose $T : V \to V$ is a linear map that has the following property: There is a basis $e_1, \ldots, e_n$ of V for which $T(e_1) = e_n$ and $T(e_j) = e_{j-1}$ if $j = 2, 3, \ldots, n$. What is the trace of T?*

Proof. The matrix of the transformation T with respect to the basis $e_1, \ldots, e_n$ contains all ones and zeroes. However, the 1's are never on the diagonal, because $T(e_j)$ is expressed in terms of the other basis vectors. Thus, the trace of T is 0. □

Problem 3. *(20 points) In class, we proved that if F is a finite field of size q, then $\alpha^q = \alpha$ for all $\alpha \in F$. Please reprove this fact.* ***Hint****: Apply Lagrange's theorem for the group $F^\times$.*

Proof. If $\alpha = 0$, the claim is immediate. If $\alpha \neq 0$, then $\alpha \in F^\times$, which has size $q-1$. Thus $\alpha^{q-1} = 1$ by Lagrange's theorem for the finite group $F^\times$. Thus $\alpha^q = \alpha$. □

Problem 4. *(20 points) Recall that, for a prime number p, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ denotes the field of size p. For this question, you do not need to justify your response.*

1. *(10 points) Find a polynomial $f(x) \in \mathbf{F}_2[x]$ so that $\mathbf{F}_2[x]/\langle f(x)\rangle$ is a field of size 8.*

   Proof. The polynomial $f(x) = x^3 - x + 1$ works. □

2. *(10 points) Find a polynomial $g(x) \in \mathbf{F}_3[x]$ so that $\mathbf{F}_3[x]/\langle g(x)\rangle$ is a field of size 27.*

Proof. The polynomial $g(x) = x^3 - x + 1$ still works. □

Problem 5. *(20 points) For a positive integer n, let $\zeta_n = e^{2\pi i/n}$ and $K = \mathbf{Q}(\zeta_n)$. Suppose $\beta \in K^\times$, and let $L = K(\beta^{1/n})$.*

1. *(10 points) Explain why the extension L/K is Galois.*

   Proof. Let $f(x) = x^n - \beta \in K[x]$. The roots of $f(x)$ in $\mathbf{C}$ are the elements $\zeta_n^j \beta^{1/n}$. Thus L is a splitting field for f over K, so is Galois. □

2. *(10 points) Prove that the Galois group $Gal(L/K)$ is cyclic.* ***Hint****: Let μ_n denote the set of n^{th} roots of unity in $\mathbf{C}$. Consider the map $Gal(L/K) \to \mu_n$ defined by $\sigma \mapsto \frac{\sigma(\beta^{1/n})}{\beta^{1/n}}$.*

Proof. Let $\Phi : Gal(L/K) \to \mu_n$ be the map of the hint. The point is that Φ is an injective group homomorphism, and thus $Gal(L/K)$ is a subgroup of the cyclic group μ_n, and thus itself cyclic. To see that Φ is well-defined, observe that if $\sigma \in Gal(L/K)$, then $\Phi(\sigma)^n = \sigma(\beta)\beta^{-1} = 1$, because $\beta \in K$. To see that Φ is a group homomormorphism, we have $\tau\sigma\beta^{1/n} = \tau(\Phi(\sigma)\beta^{1/n}) = \Phi(\sigma)\Phi(\tau)\beta^{1/n}$, because $\Phi(\sigma) \in \mu_n \subseteq K$. Finally, Φ is injective, because if $\sigma(\beta^{1/n}) = \beta^{1/n}$, then $\sigma = 1$ because $L = K(\beta^{1/n})$. □

Problem 6. *(20 points) Suppose F is a field of characteristic 0, and L is a finite extension of F. Must the extension L over F have finitely many intermediate fields? Be sure to justify your response.* ***Hint****: There exists a finite extension K of L so that K is Galois over F.*

Proof. Yes, there are finitely many intermediate fields. Using the hint, let $G = Gal(K/F)$. Then G is a finite group, and so has finitely many subgroups, thus K/F has finitely many intermediate fields. Consequently, L/F does as well. □

Problem 7. *(20 points) For a positive integer n, define*

$$\alpha_n = (1+\sqrt{2}+\sqrt{3})^n + (1-\sqrt{2}+\sqrt{3})^n + (1+\sqrt{2}-\sqrt{3})^n + (1-\sqrt{2}-\sqrt{3})^n.$$

Is α_n a rational number for all positive integers n? If so, prove it. If not, explain why not.

Proof. As was proved in class, the Galois group of $K := \mathbf{Q}(\sqrt{2},\sqrt{3})$ over $\mathbf{Q}$ is the Klein four group. Let $\beta = 1+\sqrt{2}+\sqrt{3}$. Then $\alpha_n = \sum_{\sigma \in Gal(K/\mathbf{Q})} \sigma(\beta^n)$. This expression is fixed by $Gal(K/\mathbf{Q})$, so is in $\mathbf{Q}$. □

Problem 8. *(20 points) For a positive integer n, let*

$$D_n = \langle \sigma, \tau : \sigma^n = 1, \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$$

denote the dihedral group of order $2n$. Prove that every irreducible representation of D_n has dimension 1 or 2. ***Hint****: Suppose $\rho : D_n \to \mathrm{GL}(V)$ is an irreducible representation. Let $v \in V$ be an eigenvector for $\rho(\sigma)$. Show that $\mathbf{C}v + \mathbf{C}(\tau \cdot v)$ is a D_n-invariant subspace of V.*

Proof. We have $\tau v' = \tau^2 v = v$, so $\mathbf{C}v + \mathbf{C}v'$ is stable by τ. As v is an eigenvector for σ, $\mathbf{C}v$ is stable by the action of σ. We have $\sigma\tau v = \tau\sigma^{-1}v \in \mathbf{C}\tau v$: v is an eigenvector for σ means its also an eigenvector for σ^{-1}. Thus $\mathbf{C}v'$ is also stable by σ, so $\mathbf{C}v + \mathbf{C}v'$ is stable by both τ and σ. Consequently, $\mathbf{C}v + \mathbf{C}v'$ is D_n-stable, so is equal to V by irreducibility. Thus $\dim(V) \leq 2$. □

Problem 9. *(20 points) Suppose G is a finite group, and $\rho : G \to \mathrm{GL}(V)$ is a representation. Let $\chi_\rho(g) = \mathrm{tr}_V(\rho(g))$ denote the character of ρ. Suppose that $\sum_{g\in G} |\chi_\rho(g)|^2 = 2 \cdot |G|$. Prove that ρ is the direct sum of two distinct irreducible representations.* ***Note****: Here $|G|$ denotes the order of the group G, and, for a complex number $z \in \mathbf{C}$, $|z|^2 = z\overline{z}$ where $\overline{z}$ is the complex conjugate of z.*

Proof. The assumption of the question is that $\langle \chi_\rho, \chi_\rho \rangle = 2$. But if $\rho = \rho_1^{n_1} \oplus \cdots \oplus \rho_r^{n_r}$ is the decomposition into irreducibles, then $\langle \chi_\rho, \chi_\rho \rangle = n_1^2 + \cdots + n_r^2$. The only way a sum of squares of integers can equal to 2 if exactly two of the $n_j = 1$ and the rest are 0. □

Problem 10. *(20 points) A representation $\rho : G \to \mathrm{GL}(V)$ is said to be* ***faithful*** *if* $\ker(\rho) = \{1\}$. *Suppose that G is a finite group that has a faithful irreducible representation. Prove that the center of G is cyclic.* ***Hint****: Apply Schur's lemma to the elements $\rho(z)$ for z in the center of G.*

Proof. Let $z \in Z(G)$, the center of G. Then $\rho(z)$ commutes with every $\rho(g)$, $g \in G$, so must be a scalar operator on V by Schur's lemma. Thus, $\rho(z) = r(z)1$, some $r : Z(G) \to \mathbf{C}^\times$. It is clear that r is a group homomorphism. It is injective because ρ is faithful. Thus, $Z(G)$ is a subgroup of a cyclic group, $\mu_{|Z(G)|}$, so must be cyclic. □

Problem 11. ***Bonus*** *(10 points) Suppose G is a finite abelian group, and for every representation $\rho : G \to \mathrm{GL}(V)$, one has that the character $\chi_\rho(g)$ lands in the real numbers $\mathbf{R} \subseteq \mathbf{C}$. Prove that $g^2 = 1$ for every $g \in G$.*

Proof. Every finite abelian group is isomorphic to $C_{n_1} \times \cdots \times C_{n_r}$ for some positive integers $n_1, n_2, \ldots, n_r$, where C_N denotes the cyclic group of order N. Let ρ be the representation that takes a generator of the j^{th} factor to $e^{2\pi i/n_j}$ and the other factors to 1. By the assumption of the problem, $\chi_\rho(g) \in \mathbf{R}$. But χ_χ of the generator is $e^{2\pi i/n_j}$. If this number is real, then $n_j = 1$ or 2. □

Problem 12. ***Bonus*** *(10 points) Suppose $K \subseteq \mathbf{C}$ is a subfield. Say that K is* ***constructible*** *if there exists a sequence of fields $\mathbf{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K$ such that K_{j+1} is a quadratic extension of K_j for $j = 0, 1, 2, \ldots, n-1$. Prove that $K = \mathbf{Q}(e^{2\pi i/17})$ is constructible.* ***Hint****: What is the Galois group of $K/\mathbf{Q}$?*

Proof. The Galois group of $K/\mathbf{Q}$ is $(\mathbf{Z}/17\mathbf{Z})^\times$, which is cyclic of order 16, C_{16}. For $j = 0, 1, 2, 3, 4$, let H_j be the unique subgroup C_{16} which has index 2^j. We have $\{1\} = H_4 \subseteq H_3 \subseteq H_2 \subseteq H_1 \subseteq H_0 = C_{16}$. Set $K_j = K^{H_j}$. Then by the main theorem of Galois theory, $K_{j+1} \subseteq K_j$ and the degree of the extension is 2. □

THIS PAGE INTENTIONALLY LEFT BLANK