Final Exam

Final Exam (100 points)

Instructions: Write your solutions clearly. You may use your notes, the book(s), and other reference materials. Be sure to cite any sources that you consult. Do not consult with other people besides the instructor.

Problem 1 (15 points)

Let G be a finite group, X a set on which G acts transitively, and H a subgroup of G.

a. (5) Suppose that H is *normal*. Prove that, under the action of H on X, X is a disjoint union of H-orbits all of which are of the same size.

b. (5) Illustrate this result when G is the dihedral group of a polygon with an even number n of sides generated by a rotation r and a reflection s, X is the vertices of the polygon, and $H = \langle r^2 \rangle$. (Note that this H is normal).

c. (5) Prove that the H-orbits need not be of the same size if H is not normal by giving a counterexample.

Problem 2 (15 points)

Let $G = \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$, the group of two-by-two matrices with entries in $\mathbb{Z}/7\mathbb{Z}$ and determinant one.

a. (5) Prove that G has order $(2^5)(3)(7) = 672$.

b. (5) Prove that the subgroup of upper triangular matrices with 1's on the diagonal is a Sylow 7-subgroup.

c. (5) How many Sylow 7-subgroups are there in G?

Problem 3 (20 points)

Let N be a positive integer greater than one and let $\mathbb{Z}[\frac{1}{N}]$ be the subring of $\mathbb{Q}$ generated by $\frac{1}{N}$.

a. (5) Prove that $\mathbb{Z}[\frac{1}{N}]$ is isomorphic to $\mathbb{Z}[x]/(Nx - 1)$.

b. (5) Prove that any prime $p \in \mathbb{Z}$ that divides N is a unit in $\mathbb{Z}[\frac{1}{N}]$.

c. (5) Prove that, if I is an ideal of $\mathbb{Z}[\frac{1}{N}]$, then $I \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$ (hence principal). Suppose $I \cap \mathbb{Z} = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Prove that $I = n\mathbb{Z}[\frac{1}{N}]$. Conclude that $\mathbb{Z}[\frac{1}{N}]$ is a PID.

d. (5) Prove that, if p is a prime in $\mathbb{Z}$ that does not divide N then $p\mathbb{Z}[\frac{1}{N}]$ is a proper prime ideal of $\mathbb{Z}[\frac{1}{N}]$, and that every proper prime ideal of $\mathbb{Z}[\frac{1}{N}]$ is of this type.

Problem 4 (20 points)

In the Gaussian integers $\mathbb{Z}[i]$:

a. (10) Find the gcd d of $a = 3 + 2i$ and $b = 11 - i$ and find $x, y \in \mathbb{Z}[i]$ such that $ax + by = d$.

b. (5) Factor 1105 into Gaussian primes.

c. (5) Prove that the polynomial $f(x) = x^4 + (5+3i)x + (1+i)$ is irreducible over $\mathbb{Q}(i)$.

Problem 5 (30 points)

Let G be a finite group and let V_G be the space of all functions $f : G \to \mathbb{R}$. (Note that this is all functions, not homomorphisms).

a. (5) Let $\delta_g \in V_G$ be the function δ_g where $\delta_g(h) = 0$ if $g \neq h$ and $\delta_g(g) = 1$. Prove that the δ_g are a basis for V_G.

b. (5) For $g \in G$, define a linear map $T_g : V_G \to V_G$ by $(T_g f)(x) = f(g^{-1}x)$ for all $x \in G$. Prove that $T_g \delta_h = \delta_{gh}$.

c. (5) As an illustration, for $G = S_3$, let $g = (12)$ and write the matrix of T_g in the basis given by the δ_g. For concreteness, use the following ordering of the elements of S_3:

$$e, (123), (132), (12), (13), (23)$$

d. (5) Prove that (G here is a general finite group again)

$$\langle f_1, f_2 \rangle = \sum_{g \in G} f_1(g) f_2(g)$$

is an inner product on V_G.

e. (5) Prove that the adjoint of T_g is $T_{g^{-1}}$. Therefore, if g has order 2, T_g is self-adjoint.

f. (5) The spectral theorem says that V_G has an orthogonal basis consisting of eigenvectors for T_g when g has order 2. Let g be an element of G of order 2 and let H be the order 2 subgroup generated by g. Choose

a set $k_1, \ldots, k_{n/2}$ of $n/2$ representatives for the *right* cosets of H in G. For each k_i, define

$$e_i^+ = \delta_{k_i} + \delta_{gk_i}$$

and

$$e_i^- = \delta_{k_i} - \delta_{gk_i}.$$

Prove that e_i^+ are eigenvectors with eigenvalue $+1$ and e_i^- are eigenvectors with eigenvalue -1. In fact these n vectors are an orthogonal basis; you don't have to check all of this, but do verify that e_i^+ and e_j^+ are orthogonal if $i \neq j$.