Comments on the Final Exam

Problem 1.

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.

Comments

For part (a), there were two approaches. The first is to use the orbit stabilizer theorem to see that the size of an H-orbit Hx is $[H : \mathrm{Stab}_H(x)]$ and that

$$\mathrm{Stab}_H(x) = H \cap \mathrm{Stab}_G(x).$$

If x and y are two points in X, there is a $g \in G$ such that $gx = y$ since G acts transitively on X. Then

$$g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(y)$$

since if k fixes x, then $gkg^{-1}(y) = y$; and if k' fixes y, then $g^{-1}k'g$ fixes x. Finally, since $gHg^{-1} = H$,

$$H \cap \mathrm{Stab}_G(y) = H \cap g\mathrm{Stab}_G(x)g^{-1} = gHg^{-1} \cap g\mathrm{Stab}_G(x)g^{-1} = g(H \cap \mathrm{Stab}_G(x))g^{-1}$$

which tells us that

$$\mathrm{Stab}_H(x)$$

and

$$\mathrm{Stab}_H(y)$$

are conjugate and thus have the same number of elements. Therefore the indices

$$[H : \mathrm{Stab}_H(x)]$$

and

$$[H : \mathrm{Stab}_H(y)]$$

are the same for any pair $x, y \in X$ and so their orbits are the same size.

The second approach is to consider two orbits Hx and Hy for $x, y \in X$. By transitivity, there is a g such that $gx = y$. Then

$$gHx = \{ghx : h \in H\} = Hgx = Hy$$

since $gH = Hg$ by normality of H. This gives an explicit bijection between the H-orbits of x and y. The bijectivity follows because $g^{-1}Hy = Hx$ for the same reasons.

For part (b), the given element separates the vertices of the polygon into two orbits; if you number the vertices consecutively around the polygon, the rotation r^2 carries even numbered vertices to even numbered ones, and odd numbered ones to odd numbered ones.

For part (c), there are lots of examples, but the simplest one is to consider the subgroup H generated by (12) in S_3. S_3 acts transitively on $\{1, 2, 3\}$ but the orbits of H are $\{1, 2\}$ and $\{3\}$.

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 $(2^4)(3)(7) = 336$.

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?

Comments

For part (a), the determinant map is a group homomorphism from $\mathrm{GL}_2(\mathbb{Z}/7/Z)$ to $(\mathbb{Z}/7\mathbb{Z})^*$. If $x \in (\mathbb{Z}/7\mathbb{Z})^*$ then

$$\det \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = x$$

so the map is surjective. Since $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ is the kernel of this map, we have

$$|\mathrm{SL}_2(\mathbb{Z}/7/Z)| = \frac{1}{6}|\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})| = \frac{1}{6}(48)(42) = (16)(3)(7) = 336.$$

For part (b), the upper triangular matrices form a 7-element subgroup because one can choose any x in $\mathbb{Z}/7\mathbb{Z}$ for the entry and this is a subgroup because

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x-y \\ 0 & 1 \end{pmatrix}$$

Since 7 is the highest power of 7 dividing the order of the group, a Sylow 7-subgroup is any subgroup of order 7.

For part (c), we know that $n_7 \equiv 1 \pmod 7$ and $n_7|48$. This means that n_7 is either 1 or 8. But the lower triangular matrices with 1 on the diagonal are another subgroup of order 7, so we know $n_7 > 1$ and so it must be 8. You can also prove directly by computation that the upper triangular subgroup isn't normal.

Problem 3.

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.

Comments

For part (a), the evaluation map $f \mapsto f(1/N)$ from $\mathbb{Z}[\frac{1}{N}]$ to $\mathbb{Q}$ is a ring homomorphism and $Nx-1$ is in its kernel. (Most people got this far). To finish you have to prove that if $f \in \mathbb{Z}[x]$ and $f(1/N) = 0$ then $f = (Nx-1)g(x)$ for some polynomial $g(x)$ in $\mathbb{Z}[x]$.

The division algorithm doesn't help you directly because $Nx-1$ is not monic. It does tell you that

$$f(x) = (x - \frac{1}{N})h(x)$$

for some polynomial in $\mathbb{Q}[x]$. However, this is exactly the situation where Gauss's Lemma applies. (See Proposition 5 in Section 9.3 on page 303 of DF). That Proposition tells you that if $f(x)$ is as above, then there are integers r and s so that $f(x) = (r(x - \frac{1}{N}))(sh(x))$ and the two polynomials on the right of this equation have integer coefficients. If $r(x - \frac{1}{N})$ has integer coefficients then r is a multiple of N so $f(x)$ is a multiple of $(Nx-1)$.

For part (b), if $N = pm$, then $p(m/N) = 1$ so p has m/N as an inverse in $\mathbb{Z}[\frac{1}{N}]$.

For part (c), everything is easier if you realize that any element of $\mathbb{Z}[\frac{1}{N}]$ can be written as a fraction x/N^k with $x \in \mathbb{Z}$. Many people tried to work with polynomials in $\frac{1}{N}$, which isn't wrong; but any such polynomial can be put over a common denominator and simplified into a single fraction. Having said that,

first note that $I \cap \mathbb{Z}$ is closed under addition and inverses because both terms are, and if $r \in \mathbb{Z}$ then $rI \subset I$ since I is an ideal in $\mathbb{Z}[\frac{1}{N}]$ which contains $\mathbb{Z}$. So $I \cap \mathbb{Z}$ is an ideal. (In general, if $R \subset S$ is a subring and I is an ideal of S then $S \cap R$ is an ideal of R). Therefore $I \cap \mathbb{Z} = n\mathbb{Z}$.

It follows that $n \in I$ so $n\mathbb{Z}[\frac{1}{N}] \subset I$. To conclude, choose $z \in I$. Write $z = \frac{x}{N^k}$ for some $k \geq 0$. Then $N^k z = x \in \mathbb{Z}$ and $N^k z = x \in I$. So $x \in \mathbb{Z} \cap I$ and hence $x = nw$ for some w. Finally this means that $z = \frac{nw}{N^k} \in n\mathbb{Z}[\frac{1}{N}]$ so $I = n\mathbb{Z}[\frac{1}{N}]$.

For part (d), if p is prime in $\mathbb{Z}$ and does not divide N then $p\mathbb{Z}[\frac{1}{N}]$ is a proper ideal. If not, it would contain 1, meaning $1 = p\frac{x}{N^k}$ or $N^k = px$. But this can't happen since p does not divide N. Now suppose $xy \in p\mathbb{Z}[\frac{1}{N}]$. Then as above we have $N^k xy = pu$ for some integer u. This means that p divides either x or y, so one of them belongs to $p\mathbb{Z}[\frac{1}{N}]$. This proves that this is a prime ideal.

Finally, if I is a prime ideal of $\mathbb{Z}[\frac{1}{N}]$, then $I \cap \mathbb{Z} = n\mathbb{Z}$ for some n. If $n = xy$, then $xy \in I \cap \mathbb{Z}$ so $xy \in I$ so either x or y is in $I \cap \mathbb{Z}$. Thus $I \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, so n is (up to sign) a prime and $I = p\mathbb{Z}[\frac{1}{N}]$. (It's a general fact that if R is a subgring of S and P is a prime ideal of S then $R \cap P$ is a prime ideal of R.)

Problem 4

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 $\mathbb{Q}(i)$.

Comments

For part a, there are lots of answers, depending on how you go about it, and you can check them by hand.

For part b,

$$1105 = (5)(13)(17) = (1 + 2i)(1 - 2i)(2 + 3i)(2 - 3i)(1 + 4i)(1 - 4i).$$

Each factor on the right is a gaussian integer with prime norm, hence prime.

For part c, the element $(1 + i)$ has norm 2 so it is prime. Also, $5 + 3i$ is divisible by $(1 + i)$, which you can see in various ways but the most direct is to compute

$$\frac{5 + 3i}{1 + i} = \frac{(5 + 3i)(1 - i)}{2} = \frac{8 - 2i}{2} = 4 - i.$$

Therefore this is an Eisenstein polynomial for $(1 + i)$ and therefore irreducible.

Problem 5.

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 $i \neq j$.

Comments

For part (a), suppose $f \in V_G$. Let $g_1, \ldots, g_n$ be the elements of G. Then

$$\hat{f} = \sum_{i=1}^{n} f(g_i) \delta_{g_i}$$

satisfies $f(g_i) = \hat{f}(g_i)$ for all i. Therefore the δ_{g_i} span V_G. If

$$h = \sum_{i=1}^{n} c_i \delta_{g_i} = 0$$

then $h(g_i) = c_i = 0$ for all i. This shows the δ_{g_i} are linearly independent.

For part (b), we have $(T_g \delta_h)(x) = \delta_h(g^{-1}x)$ which is 1 if $g^{-1}x = h$ and 0 otherwise. But $g^{-1}x = h$ if and only if $x = gh$, so $T_g \delta_h$ is δ_{gh}.

For part (d), you need to check that it's symmetric, linear in the first variable, positive, and nondegenerate. All of this is straightforward, the positivity comes from the fact that

$$\langle f, f \rangle = \sum_{g} f(g)^2$$

which is positive and zero only if all $f(g) = 0$.

For part (e), calculate

$$\langle T_g f(x), h(x) \rangle = \sum_{x} f(g^{-1}x) h(x) = \sum_{x} f(y) h(gy) = \langle f, T_{g^{-1}} h \rangle.$$

For part (f), we have

$$T_g e_i^+ = \delta_{gk_i} + \delta_{g^2 k_i} = e_i^+$$

and

$$T_g e_i^- = \delta_{gk_i} - \delta_{g^2 k_i} = -e_i^-$$

since $g^2 = 1$, so $e_i^{\pm}$ are eigenvectors with eigenvalues ± 1 respectively.

For the orthogonality,

$$\langle e_i^+, e_j^- \rangle = \sum_{x} e_i^+(x) e_j^-(x) = \sum_{x} (\delta_{k_i} + \delta_{gk_i})(\delta_{k_j} - \delta_{gk_j})$$

Now:

$$\delta_{k_i} \delta_{k_j} = 0$$

unless $k_i = k_j$.

$$\delta_{k_i} \delta_{gk_j} = 0$$

unless $k_i = gk_j$. But this doesn't happen because k_i and gk_j are in different cosets, so this is always zero.

$$\delta_{gk_i} \delta_{k_j} = 0$$

for the same reason.

$$\delta_{gk_i}\delta_{gk_j} = 0$$

unless $i = j$ since only in that case are k_i and k_j in the same coset.

So the dot product is zero if $i \neq j$.