Math 594. Solutions to Exam 1

1. (20 pts) Let G be a group. We define its *automorphism group* $\mathrm{Aut}(G)$ to be the set of group isomorphisms $\phi : G \simeq G$.

(*i*) (5 pts) Prove that using composition of maps, $\mathrm{Aut}(G)$ is a group.

(*ii*) (5 pts) For $g \in G$, define $c_g : G \simeq G$ to be the left conjugation action: $c_g(g') = gg'g^{-1}$. Prove that $c_g \in \mathrm{Aut}(G)$ and that $g \mapsto c_g$ is a group homomorphism $G \to \mathrm{Aut}(G)$ with kernel $Z(G)$ (the center of G). The image of this map is denoted $\mathrm{Inn}(G)$ and its elements are called the *inner automorphisms* of G.

(*iii*) (10 pts) Prove $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is denoted $\mathrm{Out}(G)$, and is called the *outer automorphism group* of G (though its elements are not actually automorphisms of G, but are merely coset classes by the inner automorphism group).

It is an important problem to know when the outer automorphism group is trivial, or to understand its structure. By considering how an element of $\mathrm{Aut}(S_3)$ acts on the three transpositions in S_3, construct an injection of groups $\mathrm{Aut}(S_3) \to S_3$ and use the triviality of the center to conclude by pure thought (i.e., without grungy calculations) that $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3)$. That is, $\mathrm{Out}(S_3)$ is trivial.

Solution

(*i*) Applying ϕ^{-1} to the equation $\phi(gh) = \phi(g)\phi(h)$ yields $gh = \phi^{-1}(\phi(g)\phi(h))$. But $g = \phi^{-1}(\phi(g))$ and $h = \phi^{-1}(\phi(h))$, so for $g' = \phi(g)$ and $h' = \phi(h)$ we have $\phi^{-1}(g'h') = \phi^{-1}(g')\phi^{-1}(h')$. Since ϕ is bijective, (g', h') ranges over all of $G \times G$. Hence, $\phi^{-1} \in \mathrm{Aut}(G)$, and clearly $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = \mathrm{id}_G$. Likewise, $\phi^{-1}\psi^{-1}$ is an inverse to $\psi \circ \phi$ for $\psi, \phi \in \mathrm{Aut}(G)$. Since a composite of two group homomorphisms is a group homomorphism, we conclude that $\mathrm{Aut}(G)$ equipped with composition admits 2-sided inverses and identity element for composition (with associativity being clear from general principles of composition of set maps).

(*ii*) One computes $c_g \circ c_{g'} = c_{gg'}$, so since $c_1 = \mathrm{id}_G$ we see that $c_{g^{-1}}$ is an inverse to c_g and $g \mapsto c_g$ is a group homomorphism from G to $\mathrm{Aut}(G)$ (as the group homomorphism property only requires checking compatibility with the group law). Since $c_g = \mathrm{id}_G$ if and only if $gg'g^{-1} = g'$ for all $g' \in G$, we see that c_g is the identity precisely when g commutes with all $g' \in G$ (i.e., $g \in Z(G)$).

(*iii*) For $\phi \in \mathrm{Aut}(G)$, one computes

$$\phi \circ c_g \circ \phi^{-1} : g' \mapsto \phi(g\phi(g')g^{-1}) = \phi(g)g'\phi(g)^{-1} = c_{\phi(g)}(g'),$$

so $\phi \circ c_g \circ \phi^{-1} = c_{\phi(g)}$. Thus, $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$.

In the case $G = S_3$, since G is generated by the transpositions we see that an automorphism of G is uniquely determined by how it moves the transpositions around (recall that transpositions in S_3 are precisely the elements of order 2, so automorphisms must carry transpositions to transpositions). There are three of these, so $\mathrm{Aut}(G)$ therefore *injects* into the permutation group on this triplet. This is an injection of groups $\mathrm{Aut}(S_3) \hookrightarrow S_3$. But $\mathrm{Inn}(S_3)$ is a subgroup of $\mathrm{Aut}(S_3)$ and $\mathrm{Inn}(G) \simeq G/Z(G) = G$ since S_n has trivial center for $n \geq 3$. By counting, $\mathrm{Inn}(G) \hookrightarrow \mathrm{Aut}(G)$ is forced to be an equality.

2. (20 pts) Give examples of each of the following, briefly indicating why your examples satisfy the requirements, or explain (with brief argument) why no such example exists.
(*i*) (4 pts) A cyclic group which is a product of two non-trivial groups.
(*ii*) (4 pts) A group acting transitively on a set with trivial stabilizer at one point and non-trivial stabilizer at another point.
(*iii*) (4 pts) Two non-isomorphic non-abelian groups of order 20.
(*iv*) (4 pts) An infinite non-abelian solvable group.
(*v*) (4 pts) A non-normal subgroup H in a finite group G such that H is not equal to its normalizer in G.

Solution

(*i*) $\mathbf{Z}/nm = \mathbf{Z}/n \times \mathbf{Z}/m$ when $\gcd(n, m) = 1$ (and $n, m > 1$).

(*ii*) Impossible since stabilizers at points of a common orbit are conjugate subgroups, and a non-trivial subgroup cannot be conjugate to a trivial subgroup.

(*iii*) Since $(\mathbf{Z}/5)^\times$ is cyclic of order 4, we can define action maps $\phi_1, \phi_2 : \mathbf{Z}/4 \to (\mathbf{Z}/5)^\times$ where ϕ_1 is an isomorphism and ϕ_2 has order 2 kernel. The resulting semidirect products $\mathbf{Z}/4 \ltimes_{\phi_j} \mathbf{Z}/5$ are non-abelian since the ϕ_j's are non-trivial. But in one case the unique order 2 subgroup of a 2-sylow acts trivially on the unique (normal) 5-Sylow, and in the other case this does not happen for any 2-Sylow (since the triviality property is inherited under passage to a conjugate subgroup, so to rule it out we may check on a single 2-Sylow).

(*iv*) Upper triagular 2×2 matrices over an infinite field, with strictly upper triangulars forming an abelian normal subgroup with abelian quotient.

(*v*) Let $G = (\mathbf{Z}/p) \ltimes (\mathbf{Z}/p \times \mathbf{Z}/p)$ be a semidirect product where $\mathbf{Z}/p = H$ acts on $\mathbf{Z}/p \times \mathbf{Z}/p$ through some matrix in $\mathrm{GL}_2(\mathbf{Z}/p)$ of order p (as on an old homework). In this case, H cannot be normal, either by computation or because otherwise we'd have an action map of $\mathbf{Z}/p \times \mathbf{Z}/p$ on H, with such an action necessarily trivial (as $\mathrm{Aut}(H)$ has order $p-1$ prime to p), so all of G would conjugate trivially on H, an absurdity since H is non-central. But in a p-group any proper subgroup has strictly bigger normalizer.

3. (20 pts) Let G be a non-trivial finite p-group (i.e., $p | \# G$) and let V be a nonzero finite-dimensional vector space over $\mathbf{F}_p$. Suppose G acts linearly on V on the left (i.e., we're given a group homomorphism $G \rightarrow \mathrm{GL}(V)$).
(*i*) (7 pts) Prove that the orbits of G with more than 1 point have size a power of p, and conclude that $\{v \in V \,|\, \mathrm{Stab}_G(v) = G\}$ is divisible by p. Using that this set is non-empty (it contains 0!), show G fixes some nonzero $v \in V$.
(*ii*) (6 pts) Choose a nonzero $v_0 \in V$ fixed by G, say spanning a line L. By considering the induced action of G on V/L and using induction on $\dim V$, prove the existence of a basis of V with respect to which the image of G in $\mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbf{F}_p)$ lies in the subgroup of strictly upper triangular matrices.
(*iii*) (7 pts) Let $H = \mathrm{GL}_n(\mathbf{F}_p)$ and let G be a p-subgroup. Using (*ii*) for an appropriate V, but not using the Sylow theorems, deduce that some conjugate of G lies inside the subgroup of strictly upper triangular matrices.

Solution

(*i*) Each orbit has size equal to the index in G of the stabilizer of a point in the orbit, so as long as such a stabilizer is not all of G (i.e., not a singleton orbit), the size is a factor of $|G|$ larger than 1, hence is divisible by p. But the class formula shows that the number of singleton orbits is the difference of $|G|$ and the sum of sizes of the non-singleton orbits, both of which are multiples of p. Hence, the number of singleton orbits is a multiple of p. This nonnegative integer is positive, as $\{0\}$ is such an orbit, so since $p > 1$ there must be another singleton orbit $\{v\}$.

(*ii*) If $\dim V = 1$, then $V = F.v_0$, so G acts trivially on V (so use any basis of V). If $\dim V > 1$, then $0 < \dim V/L < \dim V$ and by induction we can find a basis of V/L with respect to which the induced action of G (which makes sense, as G carries L back to itself) lands in the upper triangular matrix group. Now lift this back to a linearly independent set in V and stick on v_0 as the first basis vector to get strictly upper triangular form for the G-action on V relative to some basis.

(*iii*) Consider G acting on $V = \mathbf{F}_p^n$. By (*ii*), there exists a basis of V with respect to which G acquires strictly upper triangular form. But conjugating G by the change of basis matrix relating this new basis to the standard basis serves to put G in strictly upper triangular matrix form relative to the new basis, so this provides the desired conjugate of G which is inside the strictly upper triangular matrix subgroup.

4. (20 pts) Let C be the cube in $\mathbf{R}^3$ with side length 2 and the 8 vertices at the points $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ with $\varepsilon_j \in \{\pm 1\}$. Let Γ denote the group of "orientation-preserving symmetries of the cube", by which we mean permutations of the 8 vertices which preserve the relation "joined by a common edge" for pairs of vertices and "lie on a common face" for pairs of edges, and preserve the orientation formed by 3 edges emanating from a common vertex.
(*i*) (10 pts) Observe that there are 4 "long diagonals" on the cube. Use this to define a group homomorphism $\Gamma \rightarrow S_4$, and explain why it is injective. Then by either using stabilizers of a long diagonal (watch the orientation!) to compute $\#\Gamma$, or by hunting for transpositions in the image (or using some other geometric method), prove this group map is an isomorphism.

(*ii*) (10 pts) Suppose a finite group G acts on a finite set X. For each $g \in G$, define $\mathrm{Fix}(g) = \#\{x \in \mid g.x = x\}$ to be the number of points fixed by g. Prove

$$\sum_{g \in G} \mathrm{Fix}(g) = \#\{(g,x) \in G \times X \mid g.x = x\} = \sum_{x \in X} \#\{g \in G \mid g.x = x\} = \sum_{x \in X} |G|/|G.x|,$$

and by breaking up the final sum over orbits deduce *Burnside's Lemma*: the number of orbits is the average number of fixed points (i.e., $|G|^{-1} \sum_{g \in G} \mathrm{Fix}(g)$).

(**Extra Credit**) (10 pts) Imagine we paint the 6 faces of the cube with 2 red faces, 2 blue faces, and 2 green faces. Let P be the set of such ways of painting the cube. There is an obvious action of G on P, and we regard two colorings as "equivalent" if they lie in the same G-orbit (why is this reasonable?). Thus, the number of "essentially different" colorings is the number of G-orbits. Use Burnside's Lemma to determine this number (hint: $\mathrm{Fix}(\gamma)$ only depends on the conjugacy class of γ, and in $\Gamma \simeq S_6$ we know the conjugacy classes!).

Solution

(*i*) The long diagonals are characterized by their endpoints $\{p, p'\}$ which are pairs of vertices such that no edge through p touches an edge through p'. Note moreover that this breaks up the set of 8 edges into 4 disjoint pairs. This provides a description entirely in the language of the vertices of the cube and the relations of "joined by a common edge", and since Γ is a group preserving such properties, it follows that Γ must carry such pairs of endpoints to another such pair of endpoints. Thus, we get a permutation action on a 4 elements set, hence a group map $\Gamma \to S_4$.

To see that this group map is injective, assume $\gamma \in \Gamma$ carries each long diagonal back to itself (a priori perhaps swapping the orientation on such diagonals). We want to prove γ is the identity (i.e., fixes all vertices). Assume not, so $\gamma(p) \neq p$ for some vertex p. If p' is the opposite vertex (i.e., $\{p, p'\}$ is the long diagonal through p), then γ must carry $\{p, p'\}$ back to itself, so $\gamma(p) = p'$. But then each vertex q on a common edge with p must have $\gamma(q)$ sharing a common edge with p'. It follows that $\gamma(q) \neq q$, so $\gamma(q) = q'$ is the vertex opposite q'. Playing the same game with each of these new vertices eventually exhausts all vertices, so we see that for *every* vertex v, $\gamma(v)$ is the vertex opposite v. But this is not orientation-preserving.

We thereby get an injection of groups $\Gamma \hookrightarrow S_4$, and to show surjectivity we count. The action of Γ on the set of long diagonals is clearly transitive, so if $D = \{p, p'\}$ is a long diagonal then $\#\Gamma = 4\#H_D$ where H_D is the stabilizer of D in Γ. Since there is an element in Γ which swaps the endpoints of D (draw a picture, and then write out the action combinatorially), we get $\#H_D = 2\#H'_D$ where H'_D is the subgroup of Γ that fixes the endpoints of D. It is geometrically clear that rotating about the axis D provides an element of order 3 in Γ, so we conclude that $\#\Gamma$ is divisible by $24 = \#S_4$. Hence, we must have an isomorphism.

(*ii*) The first equality comes from counting pairs (g, x) with $g.x = x$ by breaking up according to fibers of the projection $G \times X \to G$ and noting that the set of interest meets $\{g_0\} \times X$ in exactly the set of pairs (g_0, x) with $g_0.x = x$. The second equality is obtained similarly, counting fibers relative to the projection $G \times X \to X$. Finally, the third equality comes from the formula $|G.x| = |G|/|\mathrm{Stab}_G(x)|$.

Now breaking up the final sum over orbits and dividing by $|G|$ throughout, we get

$$|G|^{-1} \sum_{g \in G} \mathrm{Fix}(g) = \sum_{x \in X} |G.x|^{-1} = \sum_{O} \sum_{x \in O} |G.x|^{-1} = \sum_{O} \sum_{x \in O} |O|^{-1},$$

where O runs over orbits. But the inner sum collapses to 1, so we get exactly the number of orbits as the total sum.

5. (20 pts) Classify all finite groups of order 40 with non-commutative 2-sylow subgroup, and prove that your list does not contain any repetitions (up to isomorphism). You may use the classification of finite groups of order 8.

Solution Let G be a finite group of order 40. Let P_2 be a 2-sylow and let P_5 be a 5-sylow. By Sylow's theorems, the number n_5 of 5-sylows has to be congruent to 1 mod 5 and must divide 40. Consider $1, 6, 11, 16, 21, 26 \ldots$ shows $n_5 = 1$. Hence, $G = P_2 \ltimes_\phi P_5$, with $\phi : P_2 \to \mathrm{Aut}(P_5) = (\mathbf{Z}/5)^\times$ the action map. Passing to another 2-sylow corresponds to applying a conjugating within G, and hence carries the kernel of this ϕ over to the kernel of the "new" ϕ. Hence, the structure of the kernel of this action map is independent of P_2. In particular, the property of ϕ being trivial is intrinsic to G. Hence, we can separate the cases of trivial and non-trivial ϕ. For trivial ϕ, we have $G = P_2 \times \mathbf{Z}/5$ as P_2 runs over the various groups of order 8 (with different P_2's giving non-isomorphic groups, since the isomorphism class of a p-sylow is intrinsic to a group, by the conjugacy of all p-sylows).

The non-commutative groups of order 8 are D_4 and Q (the quaternion group of order 8). This gives 2 examples.

Now consider the remaining option that ϕ is non-trivial. As we noted, the structure of $\ker \phi$ is intrinsic to G. If $P_2 = Q$, then there is only one index 4 subgroup (the center, $\langle \pm 1 \rangle$), the quotient by which is not cyclic, so there is no surjection $Q \twoheadrightarrow (\mathbf{Z}/5)^\times$. Hence, the only non-trivial possibility when $P_2 = Q$ is that $\ker \phi$ be an order 4 subgroup of Q. These are the three cyclic groups generates by i, j, and $k = ij$, and there are automorphisms of Q carrying these to each other. Hence, having each of these as $\ker \phi$ gives isomorphic results, so we may suppose $\ker \phi = \langle i \rangle$. The resulting map $\phi : Q \to \langle -1 \rangle \subseteq (\mathbf{Z}/5)^\times$ is unique, since groups of order 2 have no non-trivial automorphisms. Hence, we get *one* more example with non-trivial ϕ when $P_2 = Q$.

Finally, suppose $P_2 = D_4 = \langle \sigma, \tau \rangle$. The order 4 subgroups are $H_1 = \langle \sigma \rangle$, $H_2 = \langle \sigma\tau \rangle$, and $H_3 = \langle \sigma^2, \tau \rangle$, and the order 2 subgroups are the center $Z = \langle \sigma^2 \rangle$ and $H' = \langle \tau \rangle$. The perspective of generators and relations shows that there is an automorphism of D_4 carrying H_1 to H_2, so when considering possibilities for $\ker \phi$ we can ignore H_2. But H_1 is cyclic while H_3 is not, so these two options for $\ker \phi$ cannot give isomorphic semidirect products (as the structure of $\ker \phi$ is intrinsic to G). Once again using that groups of order 2 have no non-trivial automorphisms, we get *two* more examples, for $P_2 = D_4$ and $\ker \phi = H_1, H_3$. In the case when $\ker \phi$ has order 2, then ϕ induces an isomorphism of $G/\ker \phi$ onto the cyclic group $(\mathbf{Z}/5)^\times$. This rules out $\ker \phi = Z$ (since $D_4/Z \simeq C_2 \times C_2$ is non-cyclic), so leave only the possibility $\ker \phi = H' = \langle \tau \rangle$, but this is not a normal subgroup.

6. (20 pts) Let V be a vector space of finite dimension $n > 0$ over a field F. Define $\mathrm{Aff}(V)$ to be the group of "affine transformations" of V: this is the group generated by $\mathrm{GL}(V)$ together with translations $t_{v_0} : v \mapsto v + v_0$ for $v_0 \in V$ (note that t_{-v_0} is an inverse to t_{v_0}).
(*i*) (6 pts) In the special case $V = F$ (so $n = 1$), explain how to identify $\mathrm{Aff}(V)$ with the group of linear polynomials $ax + b$ under "composition of functions", and show that this is isomorphic to the group of matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

with $a, b \in F$ and $a \neq 0$. This is often called the "$ax + b$ group".
(*ii*) (8 pts) Viewing V as an additive group, consider the natural map of sets

$$\phi : \mathrm{GL}(V) \times V \to \mathrm{Aff}(V)$$

defined by $(T, v) \mapsto t_v \circ T$. Show that the composite of $g_1 = t_{v_1} \circ T_1$ and $g_2 = t_{v_2} \circ T_2$ can be written in "$t_v \circ T$" form for a unique $v \in V$ and $T \in \mathrm{GL}(V)$ (depending on the v_j's and T_j's), and likewise we can write $g_1^{-1} = t_{v_1'} \circ T_1'$ for some unique v_1', T_1' depending on v_1 and T_1. Conclude that ϕ is a bijection of sets, and explain how it describes $\mathrm{Aff}(V)$ as a semi-direct product of $\mathrm{GL}(V)$ and V (= translation group), with V normal in $\mathrm{Aff}(V)$.
(*iii*) (6 pts) Consider the natural (left) action of $G = \mathrm{Aff}(V)$ on V (via $g.v = g(v)$), and prove $\mathrm{GL}(V)$ is the stabilizer of the origin. Compute the stabilizer group at any $v_0 \in V$ as the conjugate of $\mathrm{GL}(V)$ by an explicit element of G (depending of course on v_0).

Solution

(*i*) The action of $\mathrm{GL}(F)$ is just the nonzero scalar multiplications. Thus, the resulting group of affine automorphisms of $V = F$ is generated by $x \mapsto ax$ for $a \neq 0$ (this is $\mathrm{GL}(V)$) and $x \mapsto x + b$ for $b \in F$ (these are the translations). Composing $x \mapsto ax$ and $x \mapsto x + b$ yields $x \mapsto ax + b$, and the collection of such latter maps is checked to be stable under function composition (with inverse $x \mapsto a^{-1}x - b/a$). By calculation,

$a'(ax+b)+b' = a'ax + (a'b+b')$, and also

$$\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a'a & a'b+b' \\ 0 & 1 \end{pmatrix}.$$

One likewise computes the inverse matrix (when $a \neq 0$) so as to see that

$$(x \mapsto ax+b) \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

is a bijective homomorphism of groups.

(*ii*) We compute

$$g_1(g_2(v)) = v_1 + T_1(g_2(v)) = v_1 + T_1(v_2 + T_2(v)) = (v_1 + T_1(v_2)) + T_1T_2(v) = (t_v \circ T)(v),$$

where $v = v_1 + T_1(v_2)$, $T = T_1 \circ T_2$. This is unique since if $t_{v'} \circ T' = t_{v''} \circ T''$ then evaluating at 0 shows $v' = v''$ and then applying the inverse of translation by this common vector gives $T' = T''$. Hence, ϕ is an injective map with image which is stable under composition. Moreover, clearly the image of ϕ contains the identity, and it is also stable under inversion: one checks that $t_{-T^{-1}(v)} \circ T^{-1}$ is an inverse to $t_v \circ T$. We conclude that the image of ϕ is a subgroup of $\mathrm{Aff}(V)$, yet it visibly contains both $\mathrm{GL}(V)$ and the translation group V, which by definition generate $\mathrm{Aff}(V)$. Hence, the image of ϕ is the entire affine transformation group, so ϕ is a bijection.

Using this bijection, we can transport over the group structure to the set $\mathrm{GL}(V) \times V$, and the subsets $\mathrm{GL}(V) \times \{0\}$ and $\{1\} \times V$ clearly inherit their *usual* group structure (e.g., $t_v \circ t_{v'} = t_{v+v'}$, t_{-v} is inverse to t_v, $t_0 = \mathrm{id}$). As such, we therefore get a description as a semidirect product in the desired manner as long as V is a normal subgroup. But one computes that $T \circ t_v \circ T^{-1} = t_{T(v)}$, so we do have normality, and the action map of $\mathrm{GL}(V)$ on V is the usual one (though the definition of $\mathrm{GL}(V)$ as the group of linear automorphisms of V).

(*iii*) By calculation, $(t_v \circ T)(0) = t_v(T(0)) = t_v(0) = v$, so this equal 0 if and only if $v = 0$. This shows $\mathrm{GL}(V)$ to be the stabilizer of the origin. Since the element $t_{v_0} \in \mathrm{Aff}(V)$ carries 0 to v_0, the stabilizer of v_0 is the conjugate $t_{v_0}\mathrm{GL}(V)t_{-v_0}$ of the stabilizer of the origin. Since

$$t_{v_0} \circ T \circ t_{-v_0} = t_{v_0} \circ t_{-T(v_0)} \circ T = t_{v_0 - T(v_0)} \circ T,$$

we can also describe the stabilizer of v_0 as the set pairs $(T, v_0 - T(v_0))$ in $\mathrm{GL}(V) \ltimes V$.