Math 306 Topics in Algebra, Spring 2013
Takehome midterm exam solutions

This exam is due Thursday, April 4, by 5 pm. Late exams will not be graded and will receive an automatic zero. Please slide the exam under my door if I am not in my office. You should work alone, and may use notes, homework assignments (and everything proved there), and our textbook.

(1) (10 pts) An action of a group G on a set X is said to be *transitive* if there is only one orbit, i.e. given any $x_1, x_2 \in X$, there is a $g \in G$ such that $gx_1 = x_2$. Now suppose G is finite and the action $G \times X \to X$ is transitive. Choose $x \in X$ and let $H = \mathrm{Stab}_G(x)$ (the stabilizer of x). Show that $|X| = |G/H|$. Then deduce that $|G| = |X| \cdot |H|$. Thus G can only act transitively on a set which is finite and whose order divides the order of G.

Solution: Consider the map

$$\begin{aligned} \psi \colon G/H &\longrightarrow X \\ gH &\longmapsto gx \end{aligned}$$

This map is well-defined: $gH = g'H \iff$ there is some $h \in H$ such that $g' = hg$. But then we have

$$g'x = (gh)x = g(hx) = gx,$$

and so $\psi(g'H) = g'x = gx = \psi(gH)$.

This map is surjective: Given $y \in X$, there is some $g \in G$ such that $y = gx$ (by transitivity), and then $\psi(gH) = gx = y$.

This map is injective: If $\psi(g_1H) = \psi(g_2H)$, we have $g_1x = g_2x$, which implies that $g_1^{-1}(g_2x) = (g_1^{-1}g_2)x = x$. But $g_1^{-1}g_2$ fixes $x \iff g_1^{-1}g_2 \in H$; thus there exists an $h \in H$ such that $g_1^{-1}g_2 = h$, and hence $g_2H = (g_1h)H = g_1H$, as required.

So we have a bijection between G/H and X and hence $|X| = |G/H|$. By Lagrange's Theorem, we have $|G| = |G/H| \cdot |H|$ and so it follows that $|G| = |X| \cdot |H|$.

(Alternatively, one can use the Orbit-Stabilizer Theorem: Since the action is transitive, the orbit of any element is all of X, so $|X| = |\operatorname{Orbit}(x)| = |G/H|$. Then use Lagrange's Theorem as above.)

(2) (7 pts) Section 4.5, problem 9 (p. 146).

Solution: $SL_2(\mathbb{F}_3)$ has order 24 (this can be obtained by various ways, including just writing out the elements). The Sylow 3-subgroups of $SL_2(\mathbb{F}_3)$ satisfy $n_3 \equiv 1 \pmod 3$ and $n_3|8$, so $n_3 = 1$ or 4. The four different subgroups are given by $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$, $\left\langle \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle$, $\left\langle \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix} \right\rangle$, $\left\langle \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix} \right\rangle$. To find them, it suffices to find one of them and then conjugate it to get the others.

(3) (10 pts) Let p and q be distinct odd primes. Show that any group G of order p^3q is not simple.

Solution: We have that $n_p \equiv 1 \pmod p$ and $n_q \equiv 1 \pmod q$. We also have that $n_p|q$, so $n_p = 1$ or q, and similarly $n_q|p^3$, so $n_q = 1, p, p^2$ or p^3.

Case 1: If $n_q = p^3$, then there are $(p^3 - 1)q$ elements of order q, leaving room for just one Sylow p-subgroup, which is then normal.

Case 2: If $n_q = p^2$ and $n_p = q$ (if $n_p = 1$, we are done), then $p^2 \equiv 1 \pmod q$ and $q \equiv 1 \pmod p$. So $p|q-1$ and hence $p < q$. Also $q|(p+1)(p-1)$, so $q|p-1$ or $q|p+1$. The first case gives $q < p$ which contradicts $p < q$. So $q|p+1$. But if $p < q$ and $q|p+1$, the only possiblity is that $p = 2$ and $q = 3$. Since p and q are assumed to be odd primes, this case is excluded.

Case 3: If $n_q = p$ and $n_p = q$, then $p \equiv 1 \pmod q$ and $q \equiv 1 \pmod p$. Then $q | p-1$ and $p | q-1$ and so $p < q$ and $q < p$, a contradiction.

(4) (7 pts) Let σ (rotation by $\pi/2$) and ρ (reflection over the x-axis) be the usual generators of the dihedral group D_4. Define a representation $\phi \colon D_4 \to GL_2(\mathbb{C})$ by

$$\phi(\sigma^k) = \begin{pmatrix} i^k & 0 \\ 0 & (-i)^k \end{pmatrix}, \quad \phi(\rho\sigma^k) = \begin{pmatrix} 0 & (-i)^k \\ i^k & 0 \end{pmatrix}.$$

Show that this is indeed a representation and prove that it is irreducible.

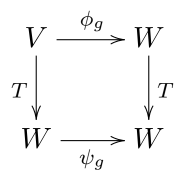
Solution: To show ϕ is a well-defined homomorphism is straightforward. The key observations are that multiplication of diagonal and anti-diagonal matrices produces diagonal and anti-diagonal matrices and that i has order 4.

To show ϕ is irreducible, it suffices to show that the given matrices have no common eigenvectors. In particular, can look at matrices $\phi(\sigma)$ and $\phi(\rho\sigma)$. The eigenvalues of the first are i and $-i$ with eigenspaces generated by $(1,0)$ and $(0,1)$. These, however, are not eigenvectors of $\phi(\rho\sigma)$ since $\phi(\rho\sigma)(1,0) = (0,i)$ and $\phi(\rho\sigma)(0,1) = (i,0)$.

(Alternatively, one could check that $\langle \chi_\phi, \chi_\phi \rangle = 1$, which would mean that ϕ is irreducible.)

(5) (10 pts) Suppose $\phi \colon G \to GL(V)$ is equivalent to a decomposable representation. Show that ϕ is decomposable. (We stated this in class but did not prove it.)

Solution: Let $\psi \colon G \to GL(W)$ be a decomposable representation with $\phi \sim \psi$ and let $T \colon V \to W$ be a vector space isomorphism with $\phi_g = T^{-1}\psi_g T$. Suppose W_1 and W_2 are nontrivial invariant subspaces of W with $W = W_1 \oplus W_2$. Since T is an equivalence, we have a commutative diagram



In other words, $T\phi_g = \psi_g T$ for all $g \in G$. Let $V_1 = T^{-1}(W_1)$ and $V_2 = T^{-1}(W_2)$. Then we have $V = V_1 \oplus V_2$: If $v \in V_1 \cap V_2$, then $Tv \in W_1 \cap W_2 = \{0\}$ and so $Tv = 0$. But T is injective, so $v = 0$. Also, if $v \in V$, then $Tv = w_1 + w_2$ for some $w_1 \in W_1$, $w_1 \in W_2$, and then $v = T^{-1}w_1 + T^{-1}w_2 \in V_1 + V_2$.

Finally we have to show that V_1 and V_2 are G-invariant: If $v \in V_i$, then $\phi_g v = T^{-1}\psi_g Tv$. But $Tv \in W_i$ implies $\psi_g Tv \in W_i$ since W_i is G-invariant. Therefore

$$\phi_g v = T^{-1}\psi_g Tv = T^{-1}\psi_g Tv \in T^{-1}(W_i) = V_i,$$

as required.

(6) (5 pts/part)

(a) Let G be a finite abelian group and $\phi \colon G \to GL_n(\mathbb{C})$ a representation. Show that there exists an invertible matrix T such that $T^{-1}\phi_g T$ is diagonal for all $g \in G$ (so T is independent of g).

(b) Let A be an $n \times n$ matrix of finite order, i.e. $A^k = I$ for some positive integer k. Show that A is diagonalizable, i.e. it is similar to a diagonal matrix. (This is an important theorem in linear algebra.)

Solution:

(a) Since ϕ is completely reducible (as G is a finite group), $\phi \sim \phi_1 \oplus \phi_2 \oplus \cdots \oplus \phi_m$, where the equivalence is given by some matrix T. Since G is abelian, all the ϕ_i are one-dimensional, i.e. complex numbers (and so $m = \dim(V) = n$). Thus the matrix for ϕ_g is a diagonal matrix (it is a block matrix with each block of size one). So, for each g, $T^{-1}\phi_g T$ is diagonal.

(b) Define a representation $\mathbb{Z}/k\mathbb{Z} \to GL_n(\mathbb{C})$ by $1 \mapsto A$. This is well-defined since $A^k = 1$. Since $\mathbb{Z}/k\mathbb{Z}$ is finite and abelian, previous part says that there exists a matrix T such that $T^{-1}\phi_1 T = T^{-1}AT$ is diagonal.

(7) (10 pts) We say a representation is *faithful* if the corresponding group action is. Show that, if G is a finite group and $\phi\colon G \to GL(V)$ is a faithful irreducible complex representation, then $Z(G)$ (the center of G) is cyclic. (Hint: Show that $Z(G)$ is isomorphic to a finite subgroup of $\mathbb{C}^\times$.)

Solution: Unravelling the definitions, a representation ϕ is faithful if different elements g of G are represented by different transformations ϕ_g. In other words, the homomorphism $\phi\colon G \to GL(V)$ is injective.

Now, let $\phi\colon G \to GL(V)$ be a faithful irreducible complex representation. Let $z \in Z(G)$, so $gz = zg$ for all $g \in G$. Consider the automorphism

$$\begin{aligned} \phi_z\colon V &\longrightarrow V \\ v &\longmapsto \phi_z v \end{aligned}$$

This is a G-map and is hence by Schur's Lemma just multiplication by a constant, say μ_z. Then the map

$$\begin{aligned} Z(G) &\longrightarrow \mathbb{C}^\times \\ z &\longmapsto \mu_z \end{aligned}$$

is a representation of $Z(G)$ and is faithful (since ϕ is), i.e. injective. Thus $Z(G)$ is isomorphic to a finite subgroup of $\mathbb{C}^\times$, and is hence cyclic.