PMATH 445/745 — Assignment 7 solutions

Alex Cowan

1. Let p be a prime. Prove that every group of order p^2 is abelian. [Note: I have given the TA permission to mock *mercilessly* anyone who does not use representation theory to solve this problem.]

Solution: Let G be a group with p^2 elements. Any irreducible representation of G has dimension 1, p, or p^2. The number of one-dimensional representations of G is at least one. And the sum of the squares of the dimensions of the irreducible representations of G is p^2. This means that all the dimensions are one, so G is abelian. ♣

2. Let p be a prime, and let G be a group of order p^3. Prove that either G is abelian, or else G has exactly $p-1$ irreducible representations of dimension p and p^2 irreducible representations of dimension one.

Solution: The number of representations of dimension one is equal to the cardinality of G/N, where N is the commutator subgroup of G. In particular, it must divide the order of G, which is p^3, so there are either 1, p, p^2, or p^3 representations of dimension one.

However, we also know that the dimension of any representation of G must also divide the order of G, and so must also equal 1, p, p^2, or p^3. Since the sum of the squares of the dimensions of the representations equals p^3, we see that all the irreducible representations of G have dimension 1 or p.

Thus, if there are a representations of dimension one and b of dimension p, we must have $a + bp^2 = p^3$. In particular, $p^3 - a$ must be a multiple of p^2, and so a must also be a multiple of p^2. If $a = p^3$, then G is abelian. If $a = p^2$, then $b = p - 1$ and we are done. ♣

3. Let p be a prime, and let G be the group of invertible affine transformations $x \mapsto ax + b$ modulo p. This group can be realized as

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}.$$

Let H denote the subgroup of G generated by translations $x \mapsto x + b$. Let ρ be a nontrivial representation of H of your choice. Determine whether or not $\mathrm{Ind}_H^G(\rho)$ is irreducible.

Solution: The subgroup H is readily seen to be isomorphic to $\mathbb{Z}/p$, via $(x \mapsto x + b) \mapsto b \bmod p$. The irreducible representations of H are thus exactly the homomorphisms

$$\rho_n(x \mapsto x + b) = \exp\left(2\pi i \frac{nb}{p}\right)$$

for $n \in \mathbb{Z}/p$. The choice $n = 0$ gives the trivial representation, so pick $\rho = \rho_n$ any $n \neq 0$.

Let's use Mackey's irreducibility criterion. Recall, $\mathrm{Ind}_H^G(V_\rho)$ is irreducible iff

(i) ρ is an irreducible representation of H, and

(ii) for every nontrivial coset $sH \in G/H$, the conjugated representation $\rho^s : sHs^{-1} \cap H \to \mathrm{GL}(V_{\rho,s})$ given by $\rho^s(g) = \rho(sgs^{-1})$ has no irreducible factors in common with ρ.

(Here $V_{\rho,s}$ is a copy of V_ρ.) In our case, ρ is 1-dimensional, so obviously irreducible. Let's focus on (ii).

Let's do some calculations to gain some insight on the group operation of G. All of the following calculations can be done using the matrix realization of G if you prefer. First, the group operation in G, function composition, works out to be $a(cx+d)+b = acx + (ad+b)$, i.e.

$$(x \mapsto ax+b) \circ (x \mapsto cx+d) = (x \mapsto acx + (ad+b)).$$

Next, let's look at inverses. For a given c, d, we want to find a, b such that $(x \mapsto ax+b) \circ (x \mapsto cx+d) = (x \mapsto x)$. In light of our calculation above for the group operation, we see that we're looking for a, b such that $ac = 1$ and $ad + b = 0$. Hence, as elements of G,

$$(x \mapsto cx+d)^{-1} = (x \mapsto c^{-1}x - c^{-1}d).$$

(Here c^{-1} means the inverse of c in $\mathbb{F}_p^\times = (\mathbb{Z}/p)^\times$.) Finally, let's work out conjugation:

$$\begin{aligned}(x \mapsto cx+d) \circ (x \mapsto ax+b) \circ (x \mapsto cx+d)^{-1} &= (x \mapsto cx+d) \circ (x \mapsto ax+b) \circ (x \mapsto c^{-1}x - c^{-1}d) \\ &= (x \mapsto cx+d) \circ (x \mapsto ac^{-1}x - ac^{-1}d + b) \\ &= (x \mapsto cac^{-1}x + c(-ac^{-1}d + b) + d) \\ &= (x \mapsto ax - (ad - bc) + d).\end{aligned}$$

Let's determine the orbit of the arbitrary element $(x \mapsto ax+b)$ under conjugation. Conjugating $(x \mapsto ax+b)$ by the arbitrary element $(x \mapsto cx+d)$ preserves the linear coefficient a, and transforms the constant coefficient b into $-(ad-bc)+d$. For any given a, b and $k \in \mathbb{Z}/p$, under what conditions do there exist c, d such that $-(ad-bc)+d = bc - (1-a)d = k$? Some case work:

If $a = 1$, then, if $b = 0$ and $k \neq 0$, there is no solution. This is expected: $(a, b) = (1, 0)$ is the identity of G, which forms its own conjugacy class.

If $a = 1$ and $b \neq 0$, then b has an inverse modulo p (because p is prime), and, for any $k \neq 0$, we can take $c = b^{-1}k$.

If $a \neq 1$, take e.g. $d = -(1-a)^{-1}k$ and $c = 0$.

We find that the orbits of conjugation in G are

- The singleton consisting of the identity map $x \mapsto x$,
- The set of maps $x \mapsto x + b$ with $b \neq 0$, and
- For any $a \neq 1$, the set of maps $(x \mapsto ax+b)$ for any $b \in \mathbb{Z}/p$.

The subgroup $H < G$, being the union of the first two conjugacy classes above, is thus seen to be normal in G. Hence the domain $sHs^{-1} \cap H$ of ρ^s is equal to H. This makes life easier. Moreover, the nontrivial cosets $sH \in G/H$ are in bijection with $\{a \in (\mathbb{Z}/p)^\times : a \neq 1\}$. Let's take the coset representatives to be $(x \mapsto sx)$ for $s \in (\mathbb{Z}/p)^\times$. (Indeed, $G/H \cong (\mathbb{Z}/p)^\times$.)

Now let's calculate the action ρ^s. Recall that $\rho(h) = \rho_n(x \mapsto x+b) = \exp(2\pi i n b/p)$. For $(x \mapsto x+b) \in sHs^{-1} \cap H = H$,

$$\begin{aligned}\rho^s(x \mapsto x+b) &= \rho((x \mapsto sx) \circ (x \mapsto x+b) \circ (x \mapsto s^{-1}x)) \\ &= \rho((x \mapsto sx) \circ (x \mapsto s^{-1}x + b)) \\ &= \rho_n(x \mapsto x + sb) \\ &= \exp\left(2\pi i \frac{nsb}{p}\right) \\ &= \rho_{ns}(x \mapsto x+b).\end{aligned}$$

I.e., ρ_n^s (the conjugate of the representation ρ_n of H by the coset $sH \in G/H$) is equal to ρ_{ns} (the representation ρ_{ns} of H).

We have assumed that $n \neq 0$ (since the question asks to pick a nontrivial representation of H), and we also have $s \neq 1$ (since Mackey's criterion asks about conjugates by nontrivial cosets), so $ns \neq n$, i.e. in our case $\rho_n^s \neq \rho_n$. Since these are distinct irreducible representations of H, they have no irreducible components in common. Mackey's criterion thus implies that $\mathrm{Ind}_H^G(\rho_n)$ is irreducible. (We obtain an irreducible representation of dimension $[G : H]\dim(V_\rho) = \#(\mathbb{Z}/p)^\times = p - 1$ of G — pretty neat!).

4. Let H be a subgroup of a finite group G, and let $\rho\colon H \to \mathrm{GL}(V)$ be an irreducible representation. Prove that there is some representation τ of H such that $\mathrm{Res}_H \mathrm{Ind}_H^G(\rho) \cong \tau \oplus \rho$.

Solution: There is more than one short solution to this problem, but I'm going to show you the one that uses the Frobenius Reciprocity Theorem. The number of copies of ρ in the irreducible decomposition of $\mathrm{Res}_H \mathrm{Ind}_H^G(\rho)$ is $\langle \chi_\rho, \mathrm{Res}_H \mathrm{Ind}_H^G(\chi_\rho)\rangle_H = \langle \mathrm{Ind}_H^G(\chi_\rho), \mathrm{Ind}_H^G(\chi_\rho)\rangle_G \geqslant 1$. ♣

5. Let G be a group with exactly five irreducible characters, corresponding to irreducible representations of dimensions 1, 3, 3, 4, and 5. Prove that G is simple.

Solution: Let H be a normal subgroup of G. We want to prove that H is either trivial or G. Any irreducible representation $\rho\colon G/H \to \mathrm{GL}(V)$ corresponds to the irreducible representation $\rho \circ q\colon G \to \mathrm{GL}(V)$, where $q\colon G \to G/H$ is the quotient map. Note that $\rho \circ q$ is irreducible because the G-invariant subspaces of V are precisely the same as the G/H-invariant subspaces of V. Moreover, non-isomorphic representations of G/H correspond in this way to non-isomorphic representations of G, because commuting with the G-action is the same thing as commuting with the G/H-action.

So there is a subset of the irreducible characters of G that are also irreducible characters of G/H. The sum of the squares of the dimensions of the corresponding representations must equal the order of G/H, which must be a divisor of the order of G, namely $1^2 + 3^2 + 3^2 + 4^2 + 5^2 = 60$.

Thus, we're looking for a subset of the numbers 1, 3, 3, 4, and 5 whose squares sum to a divisor of 60. Moreover, this subset must contain 1, since the trivial representation of G comes from the trivial representation of G/H. Here's the list:

$1^2 = 1$	$1^2 + 3^2 = 10$	$1^2 + 4^2 = 17$
$1^2 + 5^2 = 26$	$1^2 + 3^2 + 3^2 = 19$	$1^2 + 3^2 + 4^2 = 26$
$1^2 + 3^2 + 5^2 = 35$	$1^2 + 4^2 + 5^2 = 42$	$1^2 + 3^2 + 3^2 + 4^2 = 35$
$1^2 + 3^2 + 3^2 + 5^2 = 44$	$1^2 + 4^2 + 5^2 = 51$	$1^2 + 3^2 + 3^2 + 4^2 + 5^2 = 60$

The only divisors of 60 in this list are 1, 10, and 60. However, the 10 only appears as the sum of 1^2 and 3^2, and a group of order 10 (like G/H might be) cannot have an irreducible representation of dimension 3, since 3 does not divide 10. This means that the only possible orders of G/H are 1 and 60, corresponding to the normal subgroups $\{1\}$ and G. We conclude that G is simple, as advertised. ♣