Problem Set 7
solutions

Problem 1. Let p be prime and let G be a group of order p^m for some $m \geqslant 1$. Show that if N is a nontrivial normal subgroup of G, then $N \cap Z(G) \neq \{e\}$. In fact, show that $|N \cap \mathrm{Z}(G)| = p^j$ for some $j \geqslant 1$.

Proof 1. Since N is normal, the rule $g \cdot n := gng^{-1}$ defines an action of G on N. Given $n \in N$, if n is a fixed point for the action, then for all $g \in G$

$$g \cdot n = n \iff gng^{-1} = n \iff gn = ng \iff n \in \mathrm{Z}(G).$$

Thus the number of fixed points for this action is $|N \cap \mathrm{Z}(G)|$.

Now consider the Orbit Equation for this action. To do that, fix elements $n_1, \ldots, n_r$ in each one of the orbits with more than one element. Then

$$|N| = |N \cap \mathrm{Z}(G)| + \sum_i^r |\operatorname{Orb}_G(n_i)|.$$

By the Orbit-Stabilizer Theorem, for each n_i we have

$$|\operatorname{Orb}_G(n_i)| = [G : \operatorname{Stab}_G(n_i)],$$

so

$$|N| = |N \cap \mathrm{Z}(G)| + \sum_i^r [G : \operatorname{Stab}_G(n_i)].$$

Since n_i is not a fixed point, $\operatorname{Stab}_G(n_i) \neq G$, so $[G : \operatorname{Stab}_G(n_i)] > 1$. Note that by Lagrange's Theorem $[G : \operatorname{Stab}_G(n_i)]$ must divide $|G| = p^m$, so in particular p divides $[G : \operatorname{Stab}_G(n_i)]$. Since N is a nontrivial subgroup of G, its order must be also divisible by p. Thus

$$|N \cap \mathrm{Z}(G)| = |N| - \sum_i^r [G : \operatorname{Stab}_G(n_i)]$$

is a multiple of p. In particular, $|N \cap \mathrm{Z}(G)| > 1$.

Since $\mathrm{Z}(G) \cap N$ is a subgroup of G, its order must divide p^m, and we conclude that $|\mathrm{Z}(G) \cap N| = p^j$ for some $j \geqslant 1$. □

Proof 2. Since N is a normal subgroup of G, it must be the union of conjugacy classes of G. The conjugacy classes with one element are precisely the elements in $\mathrm{Z}(G)$; thus N can be written as

$$N = (N \cap \mathrm{Z}(G)) \bigcup_{i=1}^{s} [g_i]_c,$$

where $g_1, \ldots, g_s$ are representatives of distinct conjugacy classes with more than one element. Thus

$$|N| = |N \cap \mathrm{Z}(G)| + \sum_{i=1}^{s} |[g_i]_c|.$$

We proved in class that the order of each conjugacy class must divide $|G| = p^m$, so each $|[g_i]_c|$ must be a power of p. By assumption, $|[g_i]_c| \neq 1$, so for each i we have $|[g_i]_c| = p^j$ for some $j \geqslant 1$. In particular, p divides $|[g_i]_c|$.

Since N is a subgroup of G, by Lagrange's Theorem its order must divide $|G| = p^m$. But N is nontrivial, so we conclude that $|N|$ must be divisible by p. Therefore,

$$|N \cap \mathrm{Z}(G)| = |N| - \sum_i^r [G : \mathrm{Stab}_G(n_i)]$$

is a multiple of p. In particular, $|N \cap \mathrm{Z}(G)| > 1$.

Since $\mathrm{Z}(G) \cap N$ is a subgroup of G, its order must divide p^m, and we conclude that $|\mathrm{Z}(G) \cap N| = p^j$ for some $j \geqslant 1$. ☐

Problem 2. Prove the converse to Lagrange's theorem is false: find a group G and an integer $d > 0$ such that d divides the order of G but G does not have any subgroups of order d.

Solution. Consider $G = A_5$, which has order

$$|A_5| = \frac{|S_5|}{2} = \frac{120}{2} = 60.$$

Let $d = 30$, which divides $|A_5|$. If A_5 had a subgroup H with $|H| = 30$, then

$$[A_5 : H] = \frac{60}{30} = 2,$$

so H must be normal in A_5. But we have shown in class that A_5 is simple, so this is a contradiction. We conclude that A_5 has no subgroup of order 30 despite the fact that 30 divides the order of A_5.

Problem 3. Let G be a group and H a subgroup of G. Show that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of the automorphism group $\mathrm{Aut}(H)$ of H.

Proof. Consider the action of $N_G(H)$ on H given by

$$n \cdot h := nhn^{-1}.$$

By definition of the normalizer, $nhn^{-1} \in H$ for all $h \in H$, so this is well-defined. Moreover,

$$e \cdot h = ehe^{-1} = h$$

and

$$(ab) \cdot h = (ab)h(ab)^{-1} = a(bhb^{-1})b^{-1} = a \cdot (b \cdot h),$$

so this is indeed an action.

Let $\rho \colon N_G(H) \to \mathrm{Perm}(H)$ be the corresponding permutation representation. For each $n \in N_G(H)$, we claim that $\rho_n := \rho(n)$ is a group homomorphism. Indeed, for all $h_1, h_2 \in H$ we have

$$\rho_n(h_1 h_2) = n(h_1 h_2)n^{-1} = (nh_1 n^{-1})(nh_2 n^{-1}) = \rho_n(h_1)\rho_n(h_2).$$

Thus $\rho(n)$ is a group homomorphism for all $n \in H$. But $\rho(n)$ is also a bijection, and thus $\rho(n)$ must be an isomorphism. We can now restrict the codomain of ρ to $\mathrm{Aut}(H)$, and we get a group homomorphism $\rho \colon N_G(H) \to \mathrm{Aut}(H)$. Finally,

$$n \in \ker(\rho) \iff \rho(n) = \mathrm{id} \iff nhn^{-1} = n \text{ for all } h \in H \iff nh = hn \text{ for all } h \in H \iff n \in C_G(H).$$

Thus $\ker \rho = C_G(H)$. By the First Isomorphism Theorem,

$$N_G(H)/C_G(H) \cong \mathrm{im}\, \rho,$$

and $\mathrm{im}\, \rho$ is a subgroup of $\mathrm{Aut}(H)$. ☐

Problem 4. Let G be a nonabelian group of order 21. Find the number and the sizes of the conjugacy classes of G, with justification.

Solution. We will first show that if G is nonabelian, then $\mathrm{Z}(G) = \{e\}$. First, note that $|\mathrm{Z}(G)|$ must divide $|G| = 21$, by Lagrange's Theorem. Moreover, if $|Z(G)| = 21$, then G would be abelian, so $|\mathrm{Z}(G)| \in \{3, 7, 21\}$. If $|\mathrm{Z}(G)| \neq 1$, then $|Z(G)| \in \{3, 7\}$. Thus

$$\left|\frac{G}{Z(G)}\right| \in \{3, 7\}.$$

Every group of prime order is cyclic, by a midterm problem, and thus $\frac{G}{\mathrm{Z}(G)}$ is cyclic. Since we know by a previous homework problem that if $\frac{G}{Z(G)}$ is cyclic then G is abelian, this would also result in a contradiction. We are left with $|\mathrm{Z}(G)| = 1$ as the only possibility.

The class equation for G has the form

$$21 = |Z(G)| + n_1 + \cdots + n_j = 1 + n_1 + \cdots + n_j,$$

where $n_i \geqslant 2$ are the sizes of each of the conjugacy classes with more than one element. Note that we have shown that $|\mathrm{Z}(G)| = 1$, and that $n_i < 21$ for all i. We have $n_i \mid 21$ by LOIS, and hence $n_i \in \{3, 7\}$ for all i, since 1 and 21 are impossible.

There is only one way to get 20 by adding up any number of terms equal to 3 or 7, and thus

$$21 = 1 + 3 + 3 + 7 + 7$$

is the only class equation that is possible. To justify this, one could note that we want to add some copies of 3 and 7 to add up to 20, but $3 \cdot 7 = 21 > 20$, so we can only use at most two copies of 7. On the other hand, $20 \equiv 2 \pmod 3$ and $7 \equiv 1 \pmod 3$, so we must have exactly two copies of 7, leaving us with two copies of 3 necessarily.

We conclude that there are 5 conjugacy classes, of sizes 1, 3, 3, 7, and 7.

Problem 5. Let G be a group acting on a set S.

(5.1) Let $s, t \in S$ be elements in the same orbit. Show that there exists $g \in G$ such that

$$\mathrm{Stab}_G(s) = g \cdot \mathrm{Stab}_G(t) \cdot g^{-1}.$$

Proof. Since s and t are in the same orbit, there exists $g \in G$ such that

$$t = g \cdot s, \quad \text{or equivalently,} \quad s = g^{-1}t.$$

Then given any $h \in \mathrm{Stab}_G(t)$, since $\mathrm{Stab}_G(t)$ is a subgroup of G, then

$$\begin{aligned}
(g^{-1}hg) \cdot s &= (g^{-1}h) \cdot (g \cdot s) \\
&= (g^{-1}h) \cdot t \\
&= g^{-1} \cdot (ht) \\
&= g^{-1} \cdot t && \text{since } h \in \mathrm{Stab}_G(t) \\
&= s.
\end{aligned}$$

Thus $g^{-1}hg \in \mathrm{Stab}_G(s)$. This shows that

$$g^{-1}\,\mathrm{Stab}_G(t) g \subseteq \mathrm{Stab}_G(s).$$

Moreover, the same argument but switching the roles of s and t shows that

$$g \operatorname{Stab}_G(s) g^{-1} \subseteq \operatorname{Stab}_G(t),$$

and multiplying by g^{-1} on the left and g on the right gives

$$\operatorname{Stab}_G(s) \subseteq g^{-1} \operatorname{Stab}_G(t) g.$$

We conclude that

$$\operatorname{Stab}_G(s) = g^{-1} \operatorname{Stab}_G(t) g. \quad \square$$

(5.2) Show that if the action is transitive, then the kernel of the associated permutation representation $\rho \colon G \to \operatorname{Perm}(S)$ is

$$\ker(\rho) = \bigcap_{g \in G} g \operatorname{Stab}_G(s) g^{-1}.$$

Proof. Fix $s \in S$. If the action is transitive, then there is only one orbit, so that by the previous part, for every $t \in S$ there exists $g \in G$ such that

$$\operatorname{Stab}_G(t) = g^{-1} \operatorname{Stab}_G(s) g.$$

Moreover, if we fix $s \in S$, given any $g \in G$, the element $t = g \cdot s \in S$ satisfies

$$\operatorname{Stab}_G(t) = g^{-1} \operatorname{Stab}_G(s) g,$$

so the collection of all stabilizers of elements in S is the collection of all

$$g^{-1} \operatorname{Stab}_G(s) g$$

where g ranges over all the elements in G.

Now note that

$$x \in \ker(\rho) \iff x \cdot t = t \text{ for all } t \in S \iff x \in \operatorname{Stab}_G(t) \text{ for all } t \in S.$$

Thus

$$\ker(\rho) = \bigcap_{t \in S} \operatorname{Stab}_G(t) = \bigcap_{g \in G} g^{-1} \operatorname{Stab}_G(s) g. \quad \square$$

(5.3) Show that if G is finite, the action is transitive, and S has at least two elements, then there is $g \in G$ which has no fixed point, meaning that $gs \neq s$ for all $s \in S$.

Proof. Fix any $s \in S$. Since S has at least two elements and the action is transitive, there is some element of G that does not fix s, so $\operatorname{Stab}_G(s) \neq G$. By a theorem from class,

$$\bigcup_{g \in g} g \operatorname{Stab}_G(s) g^{-1} \neq G.$$

In the previous part we showed that this is just the union of all the stabilizers of elements of S, meaning

$$\bigcup_{t \in S} \operatorname{Stab}_G(t) \neq G.$$

In particular, there exists some element $g \in G$ that is not in the stabilizer of any element in S, and thus g has no fixed points. $\square$