Homework #10

Problems to hand in on Thursday, April 11, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) The **center** of a group G is the set

$$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}$$

(a) Show that the center of G is an abelian subgroup of G.

(b) Show that the center of G is a normal subgroup of G.

(c) Show that $Z(G) = G$ if and only if G is abelian.

(d) Compute the center of D_4.

(e) Compute the center of S_3.

(f) Compute the center of $GL_2(\mathbb{R})$.

Solution.

(a) If $z, z' \in Z(G)$, and $g \in G$, then $g(zz') = (gz)z' = (zg)z' = z(gz') = z(z'g) = (zz')g$, so $zz' \in Z(G)$. Also, if $z \in Z(G)$ and $g \in G$, then $zz^{-1}gz = gz = zg = zgz^{-1}z$. Multiplying by z^{-1} on the left and right gives $z^{-1}g = gz^{-1}$, so $z^{-1} \in Z(G)$. Finally, $e \in Z(G)$, so it is a subgroup. It's clear that it's abelian, since all the elements commute with each other by definition.

(b) If $g \in G$ and $z \in Z(G)$, then $gzg^{-1} = zgg^{-1} = z \in Z(G)$. It follows that $Z(G)$ is normal.

(c) Both conditions mean that any pair of elements commute.

(d) We can use an operation table that we made before to find that the center is the identity and the rotation by π.

(e) We can use an operation table to see that the center consists only if the identity.

(f) The center is the set of diagonal matrices $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ with $a \neq 0$. It is clear that these are in the center, since multiplying such a matrix by M on the left or the right yields aM. To see that nothing else is in the center, let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. If M is in the center, then $AM - MA = \begin{bmatrix} c & d-a \\ 0 & -c \end{bmatrix}$ and $BM - MB = \begin{bmatrix} -b & 0 \\ a-d & b \end{bmatrix}$ are zero, which implies that M is of the correct form.

2) Any group G acts on itself by conjugation: $g \cdot h = ghg^{-1}$. The orbits of this action are called **conjugacy classes**.

(a) Show $h \in Z(G)$ if and only h is a fixed point of the conjugation action.

(b) Show a subgroup H of G is normal if and only if it is a disjoint union of conjugacy classes.

(c) Describe the partition of $\mathcal{S}_5$ into its conjugacy classes.

(d) Show that the only nontrivial normal subgroup of $\mathcal{S}_5$ is $\mathcal{A}_5$.[1]

Solution.

(a) If $h \in Z(G)$, then for all $g \in G$, $ghg^{-1} = hgg^{-1} = h$, so h is a fixed point of the conjugation action. Conversely, if h is a fixed point of the conjugation action, then $ghg^{-1} = h$ for all $g \in G$, so $gh = hg$ for all $g \in G$, so $g \in Z(G)$.

(b) Let H be normal. Let $h \in H$. We need to show that the orbit of h under the conjugation action is contained in H. This follows immediately from the fact that $gHg^{-1} \subseteq H$ for a normal subgroup H.

Conversely, suppose that the subgroup H is a disjoint union of conjugacy classes. If $h \in H$, this means that its entirely conjugacy class is contained in H, so $g \cdot h = ghg^{-1} \in H$ for all $g \in G$. Thus, $gHg^{-1} \subseteq H$, so H is normal.

(c) We showed in an earlier problem set that $\tau(\ 1\ 2\ )\tau^{-1} = (\ \tau(1)\ \tau(2)\ )$. We observe more generally that for any $a \leq 5$, $\tau(\ 1\ \cdots\ a\ )\tau^{-1} = (\ \tau(1)\ \cdots\ \tau(a)\ )$. We check this by plugging in the elements $1, 2, 3, 4, 5$ to the two functions, in two separate cases.

Case 1: if $i \neq \tau(j)$ for $j = 1, \ldots, a$, then $\tau^{-1}(i) \neq 1, \ldots, a$, so the cycle $(\ 1\ \cdots\ a\ )$ fixes $\tau^{-1}(i)$. Altogether, we see that $\tau(\ 1\ \cdots\ a\ )\tau^{-1}(i) = i$ in this case. Similarly, $(\ \tau(1)\ \cdots\ \tau(a)\ )$ also fixes i, since it is cyclically permuting a things, none of which is i.

Case 2: if $i = \tau(j)$ for some $j = 1, \ldots, a$, then $\tau^{-1}(i) = j$. Then, the element $(\ 1\ \cdots\ a\ )\tau^{-1}$ sends i to $j+1$ if $j < a$ and 1 if $j = a$. Finally, composing with τ, $\tau(\ 1\ \cdots\ a\ )\tau^{-1}$ sends $i = \tau(j)$ to $\tau(j+1)$ if $j < a$ and $\tau(1)$ if $j = a$. This is the same value as $(\ \tau(1)\ \cdots\ \tau(a)\ )$.

The identity is in the center, so it is its own conjugacy class. Now, by conjugating $(\ 1\ 2\ )$ we can obtain any 2-cycle, and we only obtain 2-cycles, so the set of 2-cycles is a conjugacy class. Similarly, by conjugating $(\ 1\ 2\ 3\ )$ we can obtain any 3-cycle, and only 3-cycles, so the set of 3-cycles is a conjugacy class. Likewise with 4-cycles and 5-cycles. The other two conjugacy classes are: pairs of disjoint 2-cycles and products of a disjoint 3-cycle and 2-cycles. We compute the sizes as on the worksheets in class:

e	1
$(\bullet\bullet)$	10
$(\bullet\ \bullet\ \bullet)$	20
$(\bullet\ \bullet\ \bullet\bullet)$	30
$(\bullet\ \bullet\ \bullet\ \bullet\ \bullet)$	24
$(\bullet\bullet)(\bullet\bullet)$	15
$(\bullet\ \bullet\ \bullet)(\bullet\bullet)$	20

(d) Let H be a normal subgroup of $\mathcal{S}_5$. A normal subgroup is a disjoint union of conjugacy classes, including the identity. The order of H must divide 120 by Lagrange, so we need numbers from the above table that add up to a divisor of 120.

First, the only odd divisors are $1, 3, 5, 15$. No combination of the numbers above that includes the number 1 adds up to any of these. Thus, the sum must be even, and

[1]Hint: By (b), a normal subgroup is a union of conjugacy classes, one of which is the identity. Use the sizes of these conjugacy classes from (c), plus Lagrange's Theorem, to narrow down the list, and finally show that on your shortlist, the only collection closed under products is $\mathcal{A}_5$.

this means that we must include the conjugacy class (••)(••). Now we consider the divisors of 120 that are at least 16, and not 120 itself: these are $20, 24, 30, 40, 60$. None of these is congruent to 6 modulo 10, so we must also include the class (• • • • •).

Now, the union of the classes e, (••)(••), and (• • • • •) has order 40, but it isn't a subgroup! To see this, note that (1 2)(3 4)(1 2 3 4 5) = (2 4 5). This computation shows that H must contain the conjugacy class (• • •) as well.

So far we have shown that any normal subgroup must contain all of the conjugacy classes e, (••)(••), (• • •), and (• • • • •). The union of these classes is $\mathcal{A}_5$, which we know is a normal subgroup. Its order is 60, and there are no larger proper divisors of 120, so this must be the only proper normal subgroup.

3) Let p be a prime, and G be a finite group with $p \,\big|\, |G|$. Consider the set

$$X = \{(g_1, \ldots, g_p) \in \underbrace{G \times \cdots \times G}_{p-\text{times}} \mid g_1 g_2 \cdots g_p = e\}.$$

The group $\mathbb{Z}_p$ acts on X by rotating elements: $[i]_p \cdot (g_1, \ldots, g_p) = (g_{1+i}, \ldots, g_p, g_1, \ldots, g_i)$.

(a) Show that X has $|G|^{p-1}$ elements, so $p \,\big|\, |X|$.

(b) Show that the orbits of the action of $\mathbb{Z}_p$ on X either have 1 or p elements, and the orbits of order 1 are either $(e, e, \ldots, e)$ or of the form $(g, g, \ldots, g)$ with $|g| = p$.

(c) Show that G contains an element of order p.

Solution.

(a) A tuple $(g_1, \ldots, g_p) \in X$ is completely determined by its first $p-1$ coordinates, which can be anything. Given $g_1, \ldots, g_{p-1}$, $g_p = (g_1 \cdots g_{p-1})^{-1}$. There are $|G|$ possibilities for each one of those $p-1$ coordinates. Then $|X| = |G|^{p-1}$, which is divisible by p.

(b) By the Orbit-Stabilizer Theorem, the number of elements in an order divides $|\mathbb{Z}_p| = p$, so the only possibilities for the sizes of each order are 1 or p. Orbits of size 1 correspond to fixed points of our action; clearly, $(e, \ldots, e)$ is a fixed point. Otherwise, if $(g_1, \ldots, g_p)$ is a fixed point for our action, then $(g_1, \ldots, g_p) = [1]_p \cdot (g_1, \ldots, g_p) = (g_2, \cdot, g_p, g_1)$, so $g_1 = g_2 = \ldots g_p := g$. Moreover, $g^p = g_1 \cdots g_p = e$. We conclude that orbits of size one (besides the obvious one) correspond to elements of G of order p.

(c) There exists an element of order p if and only if there are at least two orbits of size 1. Say there are n orbits of size 1 and m orbits of size p. Then $n + pm = |X|$. Since $|X|$ and pm are divisible by p, so is n. Since $p \geqslant 2$ and $n \geqslant 1$, we conclude that $n \geqslant 2$. This shows there is at least one non-trivial element of G of order p — in fact, we showed there are at least $p-1$ elements of order p.