Homework 9

Submission Instructions: You are responsible to read these instructions. Failure to submit correctly as described below will result in point deductions or loss of credit for entire problems. Submit these problems on Gradescope by Thursday, April 4th, at 11:59pm. Each problem should be on a separate page (or pages). **You will need to scan a PDF of the assignment AND select the pages belonging to each problem when you submit on gradescope.**

1. (a) Prove Fermat's Little Theorem: if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.
   (b) If G is a group of prime order p, then G is cyclic.
   (c) A nontrivial group G has no nontrivial proper subgroups if and only if G is finite and of order p where p is prime.

   (a) In general, if G is a group of order n, then $g^n = e$ for any $g \in G$, since the order of g divides n by Lagrange's Theorem. Since $\mathbb{Z}_p^\times$ is as group of order $p-1$, every element in $\mathbb{Z}_p^\times$ verifies $g^{p-1} = 1$. Given an integer a such that $p \nmid a$, the class of a is an elment of $\mathbb{Z}_p^\times$, and thus $a^{p-1} \equiv 1$.

   (b) Suppose that G is a group of order p, and let $g \in G$ be an element that is not the identity in G. By Lagrange's Theorem, the order of g divides $|G| = p$, and since the order of g cannot be 1, we conclude it must be p. Therefore, $\langle g \rangle = G$, and G is cyclic.

   (c) Suppose that G has no nontrivial subgroups. Given any $g \in G$ that is not the identity, $\langle g \rangle$ is a nontrivial subgroup of G, and so the only possibility is that $\langle g \rangle = G$. We conclude that G is cyclic. If G is infinite, then g has infinite order, and the powers $g, g^2, g^3, \cdots$ are all distinct. In particular, $g \notin \langle g^2 \rangle$, wicih implies that $\langle g^2 \rangle$ is a proper subgroup of G. Therefore, G must be finite. We conclude that G is isomorphic to $\mathbb{Z}_n$ for some $n = |G|$. If $n = ab$, then $[a]$ has order b, and since G has no nontrivial proper subgroups, we conclude that either $a = 1$ and $b = n$ or $a = n$ and $b = 1$. In other words, n must be prime.

   On the other hand, suppose that G is a finite group of order p. We have seen that G must then be cyclic, so isomorphic to $\mathbb{Z}_p$. Consider any $a \in \mathbb{Z}$ such that $p \nmid a$. There exist $u, v \in \mathbb{Z}$ such that $au + pv = 1$, so $au \equiv 1 \mod p$ for some u. In particular, $\langle [a] \rangle = \langle [1] \rangle = \mathbb{Z}_p$. This shows there are no nontrivial proper subgroups of $\mathbb{Z}_p$.

2. For each of the following parts, K is a subgroup of the group G. Write down every element of every (distinct) right coset AND every distinct left coset. You do not need to prove that you have found every coset.
   (a) $K = \{r_{0^\circ}, r_{90^\circ}, r_{180^\circ}, r_{270^\circ}\}$, G is D_4, the set of symmetries of the square.
   For the sake of notation, denote the reflections of the square as s_v, s_h, s_{NW} and s_{NE}.
   (b) $K = \{e, (12)\}$, $G = S_3$
   (c) $K = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$, $G = {}_2(\mathbb{Z}_2)$. For your convenience, the elements of ${}_2(\mathbb{Z}_2)$ are given below. You may use the given letters to refer to them:

$$ {}_2(\mathbb{Z}_2) = \left\{ I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, b = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, c = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, d = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} f = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\} $$

(d) $K = \langle 5 \rangle$, $G = \mathbb{Z}_{12}^{\times}$

(a)
$$eK = \{r_{0^\circ}, r_{90^\circ}, r_{180^\circ}, r_{90^\circ}\} = Ke.$$
$$s_vK = \{s_v, s_h, s_{NW}, s_{NE}\} = Ks_v$$

(b) There are three left cosets and three right cosets.
LEFT COSETS:
I. $eK = \{e, (1\,2)\} = (1\,2)K$
II. $(1\,3)K = \{(1\,3), (1\,2\,3)\} = (1\,2\,3)K$
III. $(2\,3)K = \{(2,\ 3), (1\,3\,2)\} = (1\,3\,2)K$

RIGHT COSETS:
I. $Ke = \{e, (1\,2)\} = K(1\,2)$
II. $K(1\,3) = \{(1\,3), (1\,3\,2)\} = K(1\,3\,2)$
III. $K(2\,3) = \{(2\,3), (1\,2\,3)\} = K(1\,2\,3)$

(c) First notice that
$$K = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$
There are three left and three right cosets of K in G.
LEFT COSETS:
(a) $IK = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} = aK$
(b) $bK = \{b, c\} = cK$
(c) $dK = \{d, f\} = fK$

RIGHT COSETS:
(a) $Ke = Ka = \{I, A\}$
(b) $Kb = \{b, d\} = Kd$
(c) $Kc = \{c, f\} = Kf$

(d) Since G is abelian, the left and right cosets will be the same. Since $5^2 \equiv 1 \mod 12$, $\langle 5 \rangle = \{1, 5\}$. The set $\mathbb{Z}_{12} = \{1, 5, 7, 11\}$. There are thus two cosets:
- $1K = \{1, 5\} = K1 = 5K = K5$
- $7K = \{7, 11\} = K7 = 11K = K11$

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

1. Show $h \in Z(G)$ if and only h is a fixed point of the conjugation action.
2. Show a subgroup H of G is normal if and only if it is a disjoint union of conjugacy classes.
3. Describe the partition of $\mathcal{S}_5$ into its conjugacy classes.
4. Show that the only nontrivial normal subgroup of $\mathcal{S}_5$ is $\mathcal{A}_5$.[1]

[1]Hint: By (b), a normal subgroup is a union of conjugacy classes, one of which is the identity. Use the sizes of

1. 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 $g \in Z(G)$.

2. 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.

3. 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

4. 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 this means that we must include the conjugacy class $(\bullet\bullet)(\bullet\bullet)$. 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 $(\bullet\ \bullet\ \bullet\ \bullet\ \bullet)$.

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 $\mathcal{A}_5$.

Now, the union of the classes e, $(\bullet\bullet)(\bullet\bullet)$, and $(\bullet\ \bullet\ \bullet\ \bullet\ \bullet)$ 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 $(\bullet\ \bullet\ \bullet)$ as well.

So far we have shown that any normal subgroup must contain all of the conjugacy classes e, $(\bullet\bullet)(\bullet\bullet)$, $(\bullet\ \bullet\ \bullet)$, and $(\bullet\ \bullet\ \bullet\ \bullet\ \bullet)$. 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.

4. Let p be a prime, and G be a finite group with $p \,|\, |G|$. 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: $[i]_p \cdot (g_1, \ldots, g_p) = (g_{1+i}, \ldots, g_p, g_1, \ldots, g_i)$.

1. Show that X has $|G|^{p-1}$ elements, so $p \,|\, |X|$.
2. 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 $|g| = p$.
3. Show that G contains an element of order p.

1. 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.
2. 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.
3. 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.