Homework 10

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 Sunday, April 14th 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. Let G be a group and let N and K be normal subgroups of G.
   (a) Show that $N \cap K \lhd K$.
   (b) Prove that $NK = \{nk | n \in N, k \in K\}$ is a normal subgroup of G.
   (c) Prove that $N \lhd NK$.
   (d) Prove that the function $f : K \to NK/N$ given by $f(k) = Nk$ is a surjective homomophism with kernel $K \cap N$.
   (e) Prove that $K/(N \cap K) \cong NK/N$.

(a) We first note that $N \cap K$ is a subgroup of K because e is in both N and K and therefore $N \cap K$ and if $g \in N \cap K$, then $g \in N$ and $g \in K$ implies that $g^{-1} \in N$ and $g^{-1} \in K$, so $g^{-1} \in N \cap K$. Finally $N \cap K$ is closed because if $g, h \in N \cap K$, then $g, h \in N$, so $gh \in N$ and $g, h \in K$ so $gh \in K$.

Let $k \in K$ and let $g \in N \cap K$. Then $g \in N$ and $g \in K$. Because K is a subgroup, we have that $kgk^{-1} \in K$ for all $g \in N \cap K$. Because $N \lhd G$, we have that for all $h \in G$ that $hgh^{-1} \in N$. In particular, if $h = k \in K$, then $kgk^{-1} \in N$. Therefore $kgk^{-1} \in N \cap K$ for all $k \in K$. Because $g \in N \cap K$ was arbitrary, we have that $N \cap K \lhd K$.

(b) To see NK is a subgroup, we first observe that $e = ee \in NK$ since $e \in N$ and $e \in K$. If $nk \in NK$, then $(nk)^{-1} = k^{-1}n^{-1}$. Since K is normal in G, there exists k_1 so that $(nk)^{-1} = k^{-1}n^{-1} = n^{-1}k_1 \in NK$. Finally, to see NK is closed, let $n_1k_1, n_2k_2 \in NK$. Since N is normal in G, there exists k' such that

$$(n_1k_1)(n_2k_2) = n_1(k_1n_2)k_2 = n_1(n_2k')k_2 \in NK.$$

Thus NK is closed.

To see NK is normal, we see that for all $g \in G$,

$$gNKg^{-1} = gN(gg^{-1})Kg^{-1} = (gNg^{-1})(gKg^{-1}) = NK.$$

(c) We know that N is normal in G, therefore for any element $g \in G$, we have that $gNg^{-1} = N$. This is true if $g \in NK$, therefore N is also normal in NK.

(d) Because N is normal in NK, left and right cosets are of N are equivalent in NK, so we will work with right cosets out of convenience. Every element of NK/N is a coset Ng with $g \in NK$. Therefore g is of the form $g = nk$ with $n \in N$ and $k \in K$. That is, every coset $Ng = N(nk)$ for some $n \in N$ and $k \in K$. Since $n \in N$, we have that $N(nk) = Nk$. Since k can take on any value of K, all elements of NK/N are of the form Nk with $k \in K$. Therefore the map that sends $k \mapsto NK/N$ surjective function.

To see the map f is a homomorphism, let $k_1, k_2 \in K$. Then

$$f(k_1 k_2) = N(k_1 k_2) = N k_1 N k_2 = f(k_1) f(k_2)$$

where the second equality follows from the defintion of the binary operation on NK/N. Finally, we show that the kernel of f is $K \cap N$. We observe that if $k \in K \cap N$, then the coset $f(k) = Nk = N$, therefore $K \cap N \subset \ker f$. We also observe that if $g \in \ker f \subset K$, then $f(g) = N$. By definition of f, this means that $N = f(g) = Ng$, which implies that $g \in N$. Then $g \in K \cap N$. Therefore $\ker f = K \cap N$.

(e) This follows by applying first isomorphism theorem to part (d).

2. In the following problem, it may help to use the first isomorphism theorem.

   (a) Prove that $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^\times$ (HINT: consider the function $e^{2\pi i z}$).

   (b) Prove that $\mathbb{R}/\mathbb{Z} \cong S^1$.

   (c) Prove that the subset $N = \{e, (12)(34), (13)(24), (14)(23)\} \subset A_4$ is a normal subgroup. What familiar group is the quotient A_4/N isomorphic to?

(a) The map $\varphi\colon \mathbb{C} \to \mathbb{Z}$ sending $z \mapsto e^{2\pi i z}$ is a homomorphism. If $z = a + bi$ then $\varphi(z) = e^{-2\pi b} e^{2\pi a i}$. So $\varphi(z)$ has (1) $||z|| = e^{-2\pi b}$ and (2) argument (angle) a. Any radius and angle is possible, so φ is surjective. The kernel of φ is the a, b such that $e^{-2\pi b} = 1$ and $e^{2\pi a i} = 1$. This happens when $b = 0$ (so z is a real number) and $a \in \mathbb{Z}$.

(b) $\mathbb{R}$ is a subgroup of $\mathbb{C}$. Under the homomorphism above, $\mathbb{R}$ maps to the unit circle. The kernel is the same, so we have: $\mathbb{R}/\mathbb{Z} \cong S^1$.

(c) Observe that for any cycle $(ab)(cd) \in N$ and any permutation $\sigma \in A_4$ we have: $\sigma \circ (ab)(cd) \circ \sigma^{-1} = (\sigma(a)\sigma(b))(\sigma(c)\sigma(d))$. This shows that N is closed under conjugation. Every element in N has order 1 or 2, so it's closed under inverses. Finally, a computation shows:

$$(12)(34) \circ (13)(23) = (14)(23) = (13)(24) \circ (12)(34)$$

and it works similarly for the other pairs. A_4/N has order 3, so it must be isomorphic to $\mathbb{Z}_3$.

3. Let p be a prime number. The goal of this problem is to prove that any group G of order p^2 is abelian.

   (a) Let the group G act on itself by the conjugacy action defined in the previous problem set. Prove that $h \in Z(G)$ if and only if the orbit (AKA the conjugacy class) of h has exactly 1 element.

   (b) Use the Class Equation to deduce that p divides $|Z(G)|$. (Thus there are two possibilities $|Z(G)| = p$ or $|G|$, in the latter case G is abelian.)

(c) Suppose that $|Z(G)| = p$ and let $g \in G$ with $g \notin Z(G)$. Define $\langle Z(G), g\rangle$ to be the group generated by g and every element of $Z(G)$. Show that $\langle Z(G), g\rangle$ is abelian.

(d) Suppose that $|Z(G)| = p$ and let $g \in G$ with $g \notin Z(G)$. Define $\langle Z(G), g\rangle$ to be the group generated by g and every element of $Z(G)$. Show that $\langle Z(G), g\rangle = G$.

(e) Deduce (in one line) that G is abelian.

(f) Give an example of a group with p^3 elements that is not abelian.

(g) Use the Class Equation to conclude that any p-group[1] H satisfies p divides $|Z(H)|$.

(a) Suppose that $h \in Z(G)$. Then $ghg^{-1} = hgg^{-1}$, because h commutes with g. Thus $ghg^{-1} = h$. Therefore the orbit of h under the action of conjugation has only on element; h.
Conversely, suppose that the orbit of h under the action of conjugation has only one element. Then $ehe^{-1} = h$ is in the orbit of h, so the orbit of h must be exactly $\{h\}$. By definition of orbit, $\{ghg^{-1}|g \in G\} = h$. Thus $ghg^{-1} = h$ for all $g \in G$, so $gh = gh$ for all $g \in G$. Therefore h commutes with all elements of G, so $h \in Z(G)$.

(b) Recall that $\sum_{\text{distinct orbits}} |\mathcal{O}(x)| = |X|$ so in this case

$$\sum_{\text{distinct orbits}} |\mathcal{O}(x)| = p^2.$$

If $Z(G) = 1$, then there is exactly one element in G with order size 1. The sizes of the remaining orbits must add up to $p^2 - 1$. However, each orbit must be size p or p^2, since the size of each orbit must be a divisor of p^2 and cannot be 1 (by part (a)). Certainly the size of any orbit cannot be p^2. But it is also not possible to form a sum of orbits of size p and end up with $p^2 - 1$ because p does not divide p^2.

(c) Let $h, f \in \langle Z(G), g\rangle$. Then each can be written as a finite product of elements in $Z(G)$ and powers of g. Call them

$$\begin{aligned} h &= z_1 g^{a_1} z_2 g^{a_2} \cdots z_n g^{a_n} \\ f &= \zeta_1 g^{b_1} \zeta_2 g^{b_2} \cdots \zeta_m g^{b_m} \end{aligned}$$

where $z_i, \zeta_j \in Z(G)$ and $a_i, b_j \in \mathbb{Z}$. Because $z_i, \zeta_j \in Z(G)$ and thus commute with all elements, we can rewrite the product

$$\begin{aligned} hf &= z_1 g^{a_1} z_2 g^{a_2} \cdots z_n g^{a_n} \zeta_1 g^{b_1} \zeta_2 g^{b_2} \cdots \zeta_m g^{b_m} \\ &= z_1 \cdots z_n \zeta_1 \cdots \zeta_m g^{a_1} g^{a_2} \cdots g^{a_n} g^{b_1} \cdots g^{b_m} \\ &= z_1 \cdots z_n \zeta_1 \cdots \zeta_m g^{\sum_{i=1}^n a_i + \sum_{j=1}^m b_j} \\ &= \zeta_1 \cdots \zeta_m z_1 \cdots z_n g^{\sum_{j=1}^m b_j + \sum_{i=1}^n a_i} \\ &= g^{b_1} \zeta_2 g^{b_2} \cdots \zeta_m g^{b_m} z_1 g^{a_1} z_2 g^{a_2} \cdots z_n g^{a_n} \\ &= fh \end{aligned}$$

(d) Since $Z(G)$ is a subgroup, by LaGrange's theorem, $|Z(G)|$ divides p^2 and so must be $1, p$ or p^2. From part b we've deduced that it cannot be size 1. From part c we've deduced that if $|Z(G)| = p$, then G is commutative, which would indicate that actually $Z(G)$ is all of G and thus is actually of order p^2. Thus $Z(G)$ can only be of size p^2.

[1] A p-group H is a group such that $|H| = p^k$ for some $k > 0$ and p a prime number.

(e) D_4 is size 8 which is 2^3 and D_4 is not abelian.

Theorem 9.7: Fundamental Structure Theorem for Finite Abelian Groups: Let G be a finite abelian group. Then G is isomorphic to a group of the form

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \mathbb{Z}_{p_3^{a_3}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$$

where $p_1, p_2, \ldots p_n$ are (not necessarily distinct!) prime numbers. Moreover, the product is unique, up to re-ordering the factors.

4. (a) Suppose that G is abelian and has order 8. Use the Structure Theorem for Finite Abelian Groups to show that up to isomorphism, G must be isomorphic to one of three possible groups, each a product of cyclic groups of prime power order.
   (b) Determine the number of abelian groups of order 18, up to isomorphism.
   (c) For p prime, how many isomorphism types of abelian groups of order p^4?
   (d) If an abelian group of order 100 has no element of order 4, prove that G contains a Klein 4-group.

(a) By the Structure Theorem, G is isomorphic to either $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) There are 2: $\mathbb{Z}_3 \times \mathbb{Z}_4$ and $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) We just need to count all the ways to write p^5 as a product of prime powers: $p^5,\ p^4 \times p,\ p^3 \times p^2,\ p^3 \times p \times p,\ p^2 \times p^2 \times p,\ p^2 \times p \times p \times p,\ p \times p \times p \times p \times p$. So there are 7 abelian groups of order p^5 (up to isomorphism).

(d) An abelian group of order 100 that does not contain an element of order 4 must be isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. The first contains the Klein 4-group $\{(a, b, 0) \mid a, b \in \mathbb{Z}_2\}$, and the second contains a subgroup isomorphic to the Klein 4-group $\{(a, b, 0, 0) \mid a, b \in \mathbb{Z}_2\}$.