Math 476 - Abstract Algebra 1
Day 10 Group Assignment **Name:**_____

Order and Powers of Elements in a Group

Recall: Definition 20.10 Let G be a group. If G contains only a finite number of elements, then G has **finite order** and we say $G$is a **finite group**. If G contains exactly m distinct elements, then the **order** of G, denoted $|G|$, is m. If G contains infinitely many elements, then G has **infinite order** and we say G is an **infinite group**.

1. Find the order of $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, and $\mathbb{Z}_8$ (under the operation of **addition** on congruence classes).

2. Find the order of U_4, U_5, U_6, and U_8 (under the operation of **multiplication** on congruence classes).

Definition 21.2 Let G be a group with identity e, and let $a \in G$. Then for each integer m, we define a^m as follows:

- $a^0 = e$
- $a^1 = a$
- If m is a positive integer, then $a^m = a^{m-1}a$.

3. Consider U_9 (under the operation multiplication of congruence classes)
   (a) Find $[4]^1$, $[4]^2$, and $[4]^3$.

   (b) Find $[5]^1$, $[5]^2$, and $[5]^3$.

Theorem 21.4 Let G be a group with identity e, and let $a, b \in G$ such that $ab = ba$. Then $(ab)^m = a^m b^m$ for every integer m.

Note: We proved that the $m = 2$ case hold in any Abelian group on our last homework assignment. The full proof requires induction on m (see p. 297 in your textbook). Note that here we only require that the elements a and b commute (not the entire group). The hypothesis that $ab = ba$ is vital, as even the $m = 2$ case is not true in general when a and b do not commute.

Theorem 21.5 Let G be a group. For every $a \in G$ and every $m, n \in \mathbb{Z}$:

(i) $a^{-m} = \left(a^{-1}\right)^m = (a^m)^{-1}$ (or, using additive notation, $(-m)a = m(-a) = -(ma)$).
(ii) $a^m a^n = a^{m+n}$ (or, using additive notation, $ma + na = (m + n)a$).
(iii) $(a^m)^n = a^{mn}$ (or, using additive notation, $n(ma) = (nm)a$).

4. To begin the proof of part (ii), show that $a^m a^n = a^{m+n}$ when $n = 0$.

5. Next, show that $a^m a^n = a^{m+n}$ when $n = 1$. Be sure to clearly justify each step.

6. Complete the proof by proving the inductive step – assume that the result holds for $n = k$ and prove that it holds when $n = k + 1$.

Definition 22.2 A subset H of a group G is a **subgroup** of G if H is a group using the same operation as in G.

7. For each of the following, determine whether or not the set H is a subgroup of the given group G (assume the operation for G is standard addition). Briefly justify your answers.

   (a) $H = \mathbb{E}$, $G = \mathbb{Z}$

   (b) $H = \{3n, n \in \mathbb{Z}\}$, $G = \mathbb{Z}$

   (c) $H = \{3n + 1, n \in \mathbb{Z}\}$, $G = \mathbb{Z}$

   (d) $H = \mathbb{Z}_5$, $G = \mathbb{Z}$

   (e) $H = \mathbb{Z}_4$, $G = \mathbb{Z}_8$

Theorem 22.4(The Subgroup Test). A subset H of a group G is a subgroup of G if and only if

(i) H is closed under the operation from G;
(ii) H contains the identity element e from G; and
(iii) H contains the inverse of each of its elements – that is, if $h \in H$, and h^{-1} is the inverse of h in G, then $h^{-1} \in H$.

8. Use the Subgroup Test to prove that $H = \{[0], [2], [4]\}$ is a subgroup of $G = \mathbb{Z}_6$ (with operation addition).

9. Find a non-trivial, proper subgroup of U_9.