Math 562/662 **Spring 2022**
Homework 3 **Drew Armstrong**

---

1. Normal Subgroups. Let $(G, *, \varepsilon)$ and let $H \subseteq G$ be a subgroup. Prove that the following two statements are equivalent:

(N1) For all $g \in G$ and $h \in H$ we have $g * h * g^{-1} \in H$.
(N2) For all $g \in G$ we have $g * H = H * g$.

2. Kernel and Image. Let $\varphi : (G, *, \varepsilon) \to (G', \bullet, \delta)$ be a group homomorphism and define the *kernel* and *image* as follows:

$$\ker \varphi := \{a \in G : \varphi(a) = \delta\} \subseteq G,$$
$$\operatorname{im} \varphi := \{\varphi(a) : a \in G\} \subseteq G'.$$

(a) Prove that $\ker \varphi \subseteq G$ is a normal subgroup.
(b) Prove that $\operatorname{im} \varphi \subseteq G'$ is a subgroup.
(c) Given an example to show that the image need not be a normal subgroup. [Hint: The easiest example uses a homomorphism from $(\mathbb{Z}, +, 0)$ to S_3. See Problem 3.]

3. The Order of an Element. Let $(G, *, \varepsilon)$ be a group and fix some element $a \in G$. Then for any integer k we define the element $a^n \in G$ as follows:

$$a^k := \begin{cases} \overbrace{a * a * \cdots * a}^{k \text{ times}} & \text{if } k \geq 1, \\ \varepsilon & \text{if } k = 0, \\ \underbrace{a^{-1} * a^{-1} * \cdots * a^{-1}}_{-k \text{ times}} & \text{if } k \leq -1. \end{cases}$$

(a) Prove that the function $\varphi(k) := a^k$ is a group homomorphism $(\mathbb{Z}, +, 0) \to (G, *, \varepsilon)$.
(b) Prove that any group homomorphism $\varphi : (\mathbb{Z}, +, 0) \to (G, *, \varphi)$ sending 1 to a must be equal to the homomorphism in part (a). We use the following notation for the image:

$$\langle a \rangle := \operatorname{im} \varphi = \{a^k : k \in \mathbb{Z}\} \subseteq G,$$

and we call this the *cyclic subgroup of G generated by a*. [Hint: Induction.]
(c) Use the First Isomorphism Theorem to prove that either $\langle a \rangle \cong \mathbb{Z}$ or $\langle a \rangle \cong \mathbb{Z}/n\mathbb{Z}$ for some integer $n \geq 1$. This n is called the *order of a as an element of G*.
(d) If G is finite, conclude from Lagrange's Theorem that the order of a divides $\#G$.

4. The Order of a Power. Let $(G, *, \varepsilon)$ and let $a \in G$ be an element of order n. It follows from Problem 4(c) that $\langle a \rangle \cong \mathbb{Z}/n\mathbb{Z}$ and hence

$$a^k = a^\ell \text{ in } G \quad \Longleftrightarrow \quad k \equiv \ell \bmod n.$$

(a) For all $k \in \mathbb{Z}$, prove that $\langle a^k \rangle = \langle a^d \rangle$, where $d = \gcd(k, n)$. [Hint: Since $d|k$ we see that a^k is a power of a^d, hence $\langle a^k \rangle \subseteq \langle a^d \rangle$. Conversely, use Bézout's Identity to show that a^d is a power of a^k, hence $\langle a^d \rangle \subseteq \langle a^k \rangle$.]
(b) For any positive divisor $d|n$, show that $\#\langle a^d \rangle = n/d$. [Hint: Let $m = n/d$. The goal is to show that the elements m elements $\varepsilon, a^d, (a^d)^2, \ldots, (a^d)^{m-1}$ are distinct. Use the fact that $a^{dk} = a^{d\ell}$ if and only if $dk \equiv d\ell \bmod n$.]
(c) Combine (a) and (b) to prove that for all $k \in \mathbb{Z}$ we have

$$\#\langle a^k \rangle = n / \gcd(k, n).$$