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 $g * H = H * g$.

(N2)⇒(N1): Suppose that (N2) is true. In order to prove (N1), consider any $g \in G$ and $h \in H$. Our goal is to show that $g * h * g^{-1} \in H$. Since $g * h \in g * H$ and since $g * H = H * g$ by (N2), we must have $g * h \in H * g$ and hence $g * h = h' * g$ for some $h' \in H$. Finally, we have

$$g * h * g^{-1} = h' \in H.$$

(N1)⇒(N2): Suppose that (N1) is true. In order to prove (N2), consider any $g \in G$. Our goal is to prove the following inclusions:

(i) $g * H \subseteq H * g$
(ii) $H * g \subseteq g * H$

To prove (i), consider any element $a \in g * H$, which must have the form $a = g * h$ for some $h \in H$. Then by (N1) we have $g * h * g^{-1} = h'$ for some $h' \in H$ and it follows that

$$a = g * h = h' * g \in H * g.$$

The proof of (ii) is similar.

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.]

Our proof will use the following facts, proved in the notes:

(1) $\varphi(\varepsilon) = \delta$,
(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(a): First we prove that $\ker \varphi \subseteq G$ is a subgroup:

- **Identity.** By (1) we have $\varphi(\varepsilon) = \delta$ and hence $\varepsilon \in \ker \varphi$.
- **Inversion.** Suppose that $a \in \ker \varphi$, so that $\varphi(a) = \delta$. Then from (2) we have
$$\varphi(a^{-1}) = \varphi(a)^{-1} = \delta^{-1} = \delta,$$
so that $a^{-1} \in \ker \varphi$.
- **Closure under group operation.** Suppose that $a, b \in \ker \varphi$ so that $\varphi(a) = \delta$ and $\varphi(b) = \delta$. Then from the definition of group homomorphism we have
$$\varphi(a * b) = \varphi(a) \bullet \varphi(b) = \delta \bullet \delta = \delta,$$
so that $a * b \in \ker \varphi$.

Next we prove that $\ker\varphi \subseteq G$ is normal. To do this, consider any $g \in G$ and $h \in \ker\varphi$, so that $\varphi(h) = \delta$. Then from the definition of homomorphism and property (2) we have

$$\begin{aligned}\varphi(g * h * g^{-1}) &= \varphi(g) \bullet \varphi(h) \bullet \varphi(g)^{-1} \\ &= \varphi(g) \bullet \delta \bullet \varphi(g)^{-1} \\ &= \varphi(g) \bullet \varphi(g)^{-1} \\ &= \delta.\end{aligned}$$

It follows that $g * h * g^{-1} \in \ker\varphi$, hence $\ker\varphi$ is normal by property (N1).

(b): We verify that $\operatorname{im}\varphi \subseteq G'$ satisfies the subgroup axioms:

- **Identity.** By (1) we have $\delta = \varphi(\varepsilon) \in \operatorname{im}\varphi$.
- **Inversion.** Let $a' \in \operatorname{im}\varphi$, so that $a' = \varphi(a)$ for some $a \in G$. Then from (2) we have
$$(a')^{-1} = \varphi(a)^{-1} = \varphi(a^{-1}) \in \operatorname{im}\varphi.$$
- **Closure under group operation.** Suppose that $a', b' \in \operatorname{im}\varphi$ so that $a' = \varphi(a)$ and $b' = \varphi(b)$ for some $a, b \in G$. Then from the definition of group homomorphism we have
$$a' \bullet b' = \varphi(a) \bullet \varphi(b) = \varphi(a * b) \in \operatorname{im}\varphi.$$

(c): To see that the image need not be normal, consider the group homomorphism from $(\mathbb{Z}, +, 0)$ to $(S_3, \circ, \mathrm{id})$ defined by[1]

$$\varphi(k) = (12)^k = \begin{cases} \mathrm{id} & \text{if } k \text{ is even,} \\ (12) & \text{if } k \text{ is odd.} \end{cases}$$

The image is the subgroup $\{\mathrm{id}, (12)\} \subseteq S_3$ an we proved in class that this is not normal.

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 $\#G$.

[1] The fact that this is a homomorphism can be checked directly, or we can quote Problem 3(a).

(a): Our goal is to show that $a^{k+\ell} = a^k * a^\ell$ for any integers $k, \ell \in \mathbb{Z}$. This is a surprisingly annoying case-by-case check. Most textbooks just assume this fact without even acknowledging that something needs to be proved.

(b): Consider any group homomorphism $\varphi : (\mathbb{Z}, +, 0) \to G$ and let $a := \varphi(1)$. Our goal is to prove that $\varphi(k) = a^k$ for all $k \in \mathbb{Z}$, and we can do this by induction on k. First we observe that $\varphi(0) = \varepsilon$ by property (1) of group homomorphisms. Hence $\varphi(0) = a^0$ as desired. Now let $k \geq 1$ and assume for induction that $\varphi(k) = a^k$. Then it follows by definition that

$$\varphi(k+1) = \varphi(k) * \varphi(1) = a^k * a = a^{k+1}.$$

Hence we have shown that $\varphi(k) = a^k$ for all $k \geq 0$. Finally, for any integer $\ell < 0$ we let $k = -\ell > 0$. Then it follows from property (2) of homomorphisms that[2]

$$\varphi(\ell) = \varphi(-k) = \varphi(k)^{-1} = (a^k)^{-1} = a^{-k} = a^\ell.$$

(c): For any element $a \in G$, consider the unique homomorphism $\varphi : \mathbb{Z} \to G$ satisfying $\varphi(1) = a$. We will denote the image by

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

Hence the First Isomorphism Theorem tells us that

$$\langle a \rangle \cong \mathbb{Z}/\ker \varphi.$$

The kernel of φ, being a subgroup of $(\mathbb{Z}, +, 0)$ must have the form $n\mathbb{Z}$ for some (unique) integer $n \geq 0$. In the special case $\ker \varphi = 0\mathbb{Z} = \{0\}$, the quotient group $\mathbb{Z}/0\mathbb{Z}$ is just isomorphic to $\mathbb{Z}$, because the cosets of the subgroup $\{0\}$ are just the integers $n + \{0\} = \{n\}$ and the group operation is just addition of integers:

$$\begin{aligned}(m + \{0\}) + (m + \{0\}) &= (m + n) + \{0\}\\ \{m\} + \{n\} &= \{m + n\}.\end{aligned}$$

(d): Since $\langle a \rangle \subseteq G$ is the image of a homomorphism it is necessarily a subgroup. If G is finite then Largange's Theorem tells us that

$$\#\langle a \rangle | \#G.$$

Remark: We will write $\text{ord}_G(a) := \#\langle a \rangle$ and call this the *order of a as an element of G*. If $\#\langle a \rangle$ then because of the group isomorphism $\mathbb{Z}/m\mathbb{Z} \to \langle a \rangle$ we have $a^k = a^\ell$ if and only if $k \equiv \ell \bmod m$. It follows that every element of $\langle a \rangle$ has a unique representation of the form a^r for some $0 \leq r < m$:

$$\langle a \rangle = \{\varepsilon, a, a^2, \ldots, a^{m-1}\rangle.$$

Now consider the case $G = (\mathbb{Z}/n\mathbb{Z})^\times$, where $\#G$ is Euler's phi function $\phi(n)$. For any element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ part (d) gives

$$\text{ord}(a) | \#\phi(n),$$

say $\text{ord}(a)d = \phi(n)$ for some $d \in \mathbb{Z}$. Then it follows that

$$a^{\phi(n)} = a^{\text{ord}(a)d} = (a^{\text{ord}(a)})^d = 1^d = 1 \text{ in } (\mathbb{Z}/n\mathbb{Z})^\times,$$

which is just Euler's Totient Theorem.

---

[2] Oops, I didn't ask you to prove that $(a^k)^{-1} = a^{-k}$. That is another annoying case-by-case proof.

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

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

(a): Let $a \in (G, *, \varepsilon)$ be an element of order n, so that $a^n = \varepsilon$. Consider any integers $k \in \mathbb{Z}$ with $d = \gcd(k, n)$ and $k = dk'$. Our goal is to show that $\langle a^k \rangle = \langle a^d \rangle$. To prove $\langle a^k \rangle \subseteq \langle a^d \rangle$, consider any power of a^k, say $(a^k)^m = a^{km}$. Then we have

$$a^{km} = a^{dk'm} = (a^d)^{k'm} \in \langle a^d \rangle.$$

To prove $\langle a^d \rangle \subseteq \langle a^k \rangle$, consider any power of a^d, say $(a^d)^m = a^{dm}$. Since $d = \gcd(k, n)$ we know from Bézout's Identity that $d = kx + ny$ for some $x, y \in \mathbb{Z}$. Hence we have

$$a^{dm} = a^{(kx+ny)m} = (a^k)^{xm} * (a^n)^{ym} = (a^k)^{xm} * (\varepsilon)^{ym} = (a^k)^{xm} \in \langle a^k \rangle.$$

(b): Let $a \in (G, *, \varepsilon)$ have order n so that $a^x = a^y$ if and only if $x \equiv y \bmod n$. Consider any positive divisor $d|n$ with $n = dm$, so that m is also positive Our goal is to show that $\#\langle a^d \rangle = m$. Since $(a^d)^m = a^{dm} = a^n = \varepsilon$, it is enough to show that the elements

$$\varepsilon, a^d, (a^d)^2, \ldots, (a^d)^{m-1}$$

are all distinct. So let us assume for contradiction that there exist integers $0 \leq k < \ell < m$ such that $(a^d)^k = (a^d)^\ell$, and hence

$$\begin{aligned}
(a^d)^\ell &= (a^d)^k \\
a^{d\ell} &= a^{dk} \\
a^{d(\ell - k)} &= \varepsilon.
\end{aligned}$$

Since $0 \leq k < \ell < m$ we have $0 < \ell - k < m$ and hence $0 < d(\ell - k) < dm = n$. But since a has order n, the identity $a^{d(k-\ell)} = \varepsilon$ implies that $d(k - \ell)$ is a multiple of n. Contradiction.

(c): For any $k \in \mathbb{Z}$ we showed in part (a) that

$$\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle.$$

Then since $\gcd(k, n)$ is a positive divisor of n, it follows from part (b) that

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