MTH 561/661 **Fall 2018**
Exam 2 — Fri Oct 26 **Drew Armstrong**

Problem 1. Subgroups of $\mathbb{Z}$. Consider the abelian group $(\mathbb{Z}, +, 0)$.

(a) Prove that every subgroup $H \subseteq \mathbb{Z}$ has the form $H = m\mathbb{Z}$ for some $m \geq 0$. [Hint: If $H \neq \{0\}$ then let $m \in H$ be the smallest positive element.]

Proof. If $H = \{0\} = 0\mathbb{Z}$ then we are done. Otherwise, let $m \geq 1$ be the **smallest** positive element of H. First note that $m\mathbb{Z} = \langle m \rangle \subseteq H$. Conversely, let $k \in H$. Then we have $k = qm + r$ for some remainder satisfying $0 \leq r < m$. If $r > 0$ then $r = k - qm$ is a **smaller** positive element of H. Thus we must have $r = 0$ and hence $k = qm \in m\mathbb{Z}$. Since this is true for all $k \in H$ we conclude that $H \subseteq m\mathbb{Z}$. □

(b) For all $m, n \in \mathbb{Z}$ prove that $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if $n|m$.

Proof. Suppose that $m\mathbb{Z} \subseteq n\mathbb{Z}$. Then since $m \in m\mathbb{Z}$ we must have $m \in n\mathbb{Z}$ and hence $m = nk$ for some $k \in \mathbb{Z}$. By definition this means that $n|m$. Conversely, suppose that $n|m$, so that $m = nk$ for some $k \in \mathbb{Z}$. Then for any $m\ell \in m\mathbb{Z}$ we have $m\ell = (nk)\ell = n(k\ell) \in n\mathbb{Z}$, and hence $m\mathbb{Z} \subseteq n\mathbb{Z}$. □

Problem 2. Equivalence Modulo a Subgroup. Let $H \subseteq G$ be a subgroup.

(a) Prove that the relation $a \sim b \Longleftrightarrow a^{-1}b \in H$ is an equivalence on G.

Proof. There are three things to check.

- **Reflexive.** For all $a \in G$ we have $a^{-1}a = \varepsilon \in H$ and hence $a \sim a$.
- **Symmetric.** For all $a, b \in G$ we have

$$a \sim b \Longrightarrow a^{-1}b \in H \Longrightarrow b^{-1}a = (a^{-1}b)^{-1} \in H \Longrightarrow b \sim a.$$

- **Transitive.** For all $a, b, c \in G$ we have

$$\begin{aligned} a \sim b \text{ and } b \sim c &\Longrightarrow a^{-1}b \in H \text{ and } b^{-1}c \in H \\ &\Longrightarrow a^{-1}c = (a^{-1}b)(b^{-1}c) \in H \\ &\Longrightarrow a \sim c. \end{aligned}$$

□

(b) For all $a, b \in G$ prove that $aH = bH$ implies $a \sim b$.

Proof. Suppose that $aH = bH$. Then since $b \in bH$ we have $b \in aH$ and hence $b = ah$ for some $h \in H$. But then $a^{-1}b = h \in H$. □

(c) For all $a, b \in G$ prove that $a \sim b$ implies $aH = bH$.

Proof. Suppose that $a \sim b$, so that $a^{-1}b = h \in H$. Then for all $ah' \in aH$ we have $ah' = (bh^{-1})h' = b(h^{-1}h') \in bH$, hence $aH \subseteq bH$. And for all $bh' \in bH$ we have $bh' = (ah)h' = a(hh') \in aH$, hence $bH \subseteq aH$. □

Problem 3. Image and Preimage. Let $\varphi : G \to H$ be a group homomorphism. For all subsets $S \subseteq G$ and $T \subseteq H$ we define

$$\varphi[S] = \{\varphi(s) : s \in S\} \subseteq H,$$
$$\varphi^{-1}[T] = \{g \in G : \varphi(g) \in T\} \subseteq G.$$

(a) For all subsets $S \subseteq G$ prove that $S \subseteq \varphi^{-1}[\varphi[S]]$.

Proof. For all $s \in S$ we have $\varphi(s) \in \varphi[S]$ and hence $s \in \varphi^{-1}[\varphi[S]]$. □

(b) If $S \subseteq G$ is a subgroup prove that $\varphi[S] \subseteq H$ is a subgroup.

Proof. Let $S \subseteq G$ be a subgroup and consider any $h_1, h_2 \in \varphi[S]$. By definition this means $h_1 = \varphi(s_1)$ and $h_2 = \varphi(s_2)$ for some $s_1, s_2 \in S$. Then since $s_1 s_2^{-1} \in S$ we have

$$h_1 h_2^{-1} = \varphi(s_1)\varphi(s_2)^{-1} = \varphi(s_1 s_2^{-1}) \in \varphi[S].$$

□

(c) If $T \subseteq H$ is a subgroup prove that $\varphi^{-1}[T] \subseteq G$ is a subgroup.

Proof. Let $T \subseteq H$ be a subgroup and consider any $g_1, g_2 \in \varphi^{-1}[T]$. By definition this means $\varphi(g_1) \in T$ and $\varphi(g_2) \in T$. Then since T is a subgroup we have

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} \in T,$$

and hence $g_1 g_2^{-1} \in \varphi^{-1}[T]$. □

Problem 4. Normal Subgroups. Let $\varphi : G \to G'$ be any group homomorphism.

(a) Prove that $\ker\varphi \subseteq G$ is a normal subgroup.

Proof. For all $g \in G$ and $k \in \ker\varphi$ we have

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)\varepsilon\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = \varepsilon,$$

and hence $gkg^{-1} \in \ker\varphi$. □

(b) If $H \subseteq G$ is any subgroup prove that the following set is also subgroup:

$$H(\ker\varphi) := \{hk : h \in H, k \in \ker\varphi\} \subseteq G.$$

Proof. I'll do it the slow way.

- **Identity.** Since $\varepsilon \in H$ and $\varepsilon \in \ker\varphi$ we have $\varepsilon = \varepsilon\varepsilon \in H(\ker\varphi)$.
- **Inverses.** Consider $h \in H$ and $k \in \ker\varphi$. Then from (a) we have $hkh^{-1} = k'$ for some $k' \in \ker\varphi$, and hence

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(k')^{-1} \in H(\ker\varphi).$$

- **Closure.** Consider h_1k_1 and h_2k_2 in $H(\ker\varphi)$. Then from (a) we have $h_2^{-1}k_1h_2 = k'$ for some $k' \in \ker\varphi$, and hence

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k')k_2 = (h_1h_2)(k'k_2) \in H(\ker\varphi).$$

□