MTH 561/661 **Fall 2023**
Exam 2 — Thurs Oct 26 **Drew Armstrong**

Problem 1. Equivalence Modulo a Subgroup. Let $(G, *, \varepsilon)$ be a group and let $H \subseteq G$ be a subgroup. For all $a, b \in G$ we define

$$a \sim b \quad \Longleftrightarrow \quad a^{-1} * b \in H.$$

You may assume that $\sim$ is an equivalence relation. For any element $a \in G$ we define the set

$$[a] := \{b \in G : a \sim b\}.$$

(a) Prove that $[\varepsilon] = H$.

First suppose that $a \in [\varepsilon]$, so that $\varepsilon \sim a$. By definition this means that $a = \varepsilon^{-1} * a \in H$. Conversely, suppose that $a \in H$, so that $\varepsilon^{-1} * a \in H$. By definition this means that $\varepsilon * a$ and hence $a \in [\varepsilon]$. [Alternatively, you can prove (b) first and then take $a = \varepsilon$.]

(b) For any $a \in G$ we define the set $a * H := \{a * h : h \in H\}$. Prove that $[a] = a * H$.

First suppose that $b \in [a]$. By definition this means that $a \sim b$ and hence $a^{-1} * b \in H$. Let $h := a^{-1} * b$. Then we have $b = a * h \in a * H$. Conversely, consider any element $b \in a * H$. By definition this means that $b = a * h$ for some $h \in H$. Then since $a^{-1} * b = h \in H$ it follows that $a \sim b$ and hence $b \in [a]$.

Problem 2. Lagrange's Theorem. Let $(G, *, \varepsilon)$ be a group and let $H \subseteq G$ be a subgroup. For each $a \in G$ we consider the set $a * H = \{a * h : h \in H\}$ as in Problem 1(b).

(a) For any $a, b \in G$ prove that there exists a bijection between $a * H$ and $b * H$. [Hint: It suffices to show that there exists a bijection between $a * H$ and H for each $a \in H$.]

For any element $a \in G$ we consider the function $\tau_a : H \to G$ defined by $\tau_a(h) = a * h$. This function is injective because $a * b = a * c$ implies $b = c$ after multiplying on the left by a^{-1}. And the image of τ_a is $a * H$. Hence τ_a is a bijection $H \to a * H$.

The composition $\tau_b \circ \tau_{a^{-1}}$ is a bijection $a * H \to b * H$.

(b) If G is a finite group, use part (a) to prove that $\#H$ is a divisor of $\#G$.

Since $\sim$ is an equivalence relation we know that the set G is a disjoint union of equivalence classes $G = \coprod_i [a_i]$ for some arbitrary class representatives $a_1, \ldots, a_k \in G$. From 1(b) and 2(a) we know that $\#[a] = \#H$ for any $a \in G$. Hence

$$\begin{aligned}
\#G &= \#[a_1] + \#[a_2] + \cdots + \#[a_k] \\
&= \#H + \#H + \cdots + \#H \\
&= k \cdot \#H.
\end{aligned}$$

Problem 3. Applications of Lagrange. Given a group $(G, *, \varepsilon)$ and an element $a \in G$ we let $\langle a \rangle \subseteq G$ denote the smallest subgroup of G that contains a.

(a) Suppose that G is finite. For any $a \in G$ you may assume that $a^{\#\langle a\rangle} = \varepsilon$. Combine this fact with Problem 2(b) to show that $a^{\#G} = \varepsilon$.

Since $\langle a\rangle \subseteq G$ is a subgroup we know from 2(b) that $\#\langle a\rangle$ divides $\#G$. Let's say $\#G = \#\langle a\rangle \cdot m$. Then we have

$$a^{\#G} = a^{\#\langle a\rangle \cdot m} = (a^{\#\langle a\rangle})^m = \varepsilon^m = \varepsilon.$$

(b) We say that G is cyclic if there exists some element such that $\langle a\rangle = G$. If $\#G = p \geq 2$ is prime, use Problem 2(b) to prove that G is cyclic. [Hint: Pick any non-identity element $a \in G$.]

Let $\#G = p \geq 2$ be prime. Since $\#G \geq 2$ there exists some non-identity element $a \in G$. Consider the subgroup $\langle a\rangle \subseteq G$. From 2(b) we know that $\#\langle a\rangle$ divides p. Since p is prime and $\#\langle a\rangle \geq 2$ this implies that $\#\langle a\rangle = p$, and it follows that $\langle a\rangle = G$.