Math 561/661 **Fall 2023**
Homework 4 **Drew Armstrong**

---

1. Equivalence Modulo a Subgroup. Let $(G, *, \varepsilon)$ be a group and let $H \subseteq G$ be any subgroup. Define the relation $\sim$ on G by

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

(a) Prove that $\sim$ is an equivalence relation on the set G.
(b) For each $a \in G$, consider the equivalence class $[a] := \{b \in G : a \sim b\}$ and the coset $a * H := \{a * h : h \in H\}$. Prove that $[a] = a * H$.
(c) Now suppose that H is a *normal subgroup*. That is, for all $h \in H$ and $a \in G$ we assume that $a * h * a^{-1} \in H$. In this case, prove that the following operation on cosets is well-defined:

$$[a] * [b] := [a * b].$$

2. Order of a Commuting Product. Let $(G, \cdot, 1)$ be a group and let $a, b \in G$ be any elements satisfying $ab = ba$.

(a) Suppose that $a^m = 1$ and $b^n = 1$ for some integers $m, n \geq 1$. In this case, show that

$$(ab)^{\mathrm{lcm}(m,n)} = 1.$$

[Hint: You may assume that $\mathrm{lcm}(m, n) = mn/\gcd(m, n)$.]
(b) Use part (a) to show that the order $\#\langle ab\rangle$ divides $\mathrm{lcm}(m, n)$.

3. Direct Product of Groups. Let $(G, *, \varepsilon_G)$ and $(H, \bullet, \varepsilon_H)$ be groups. Consider the Cartesian product set, which is the set of ordered pairs:

$$G \times H := \{(g, h) : g \in G, h \in H\}.$$

(a) Prove that the following operation makes the set $G \times H$ into a group:

$$(g_1, h_1) \diamond (g_2, h_2) := (g_1 * g_2, h_1 \bullet h_2).$$

(b) For each $g \in G$ we have an element $\tilde{g} := (g, \varepsilon_H) \in G \times H$ and for each $h \in H$ we have an element $\tilde{h} := (\varepsilon_G, h) \in G \times H$. Show that $\tilde{g} \diamond \tilde{h} = \tilde{h} \diamond \tilde{g}$ for all $g \in G$ and $h \in H$.
(c) If $\gcd(m, n) \neq 1$, prove that the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not cyclic. [Hint: A group of size mn is cyclic if and only if it has an element of order mn. If $\gcd(m, n) \neq 1$ then $\mathrm{lcm}(m, n) = mn/\gcd(m, n) < mn$. Use part (b) and Problem 2 to show that every element of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has order dividing $\mathrm{lcm}(m, n)$.]

4. Chinese Remainder Theorem. In this problem we will show that the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic whenever $\gcd(m, n) = 1$. For any integers $a, n \in \mathbb{Z}$ we will write $[a]_n$ for the equivalence class of a with respect to "equivalence mod n". We showed in class that the operation $[a]_n + [b]_n := [a + b]_n$ is well-defined and makes the set of cosets $\mathbb{Z}/n\mathbb{Z}$ into a group.

(a) For any integers $m, n \in \mathbb{Z}$, show that the rule $\varphi([a]_{mn}) := ([a]_m, [a]_n])$ is a well-defined group homomorphism from $\mathbb{Z}/mn\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. [Hint: You must show that $[a]_{mn} = [b]_{mn}$ implies $[a]_m = [b]_m$ and $[a]_n = [b]_n$.]
(b) If $\gcd(m, n) = 1$, prove that φ is **injective**. [Hint: If $\gcd(m, n) = 1$ then we can write $mx + ny = 1$ for some $x, y \in \mathbb{Z}$. Use this to prove that $m|c$ and $n|c$ imply $mn|c$.]
(c) If $\gcd(m, n) = 1$, prove that φ is also **surjective**. [Hint: Write $mx + ny = 1$ for some $x, y \in \mathbb{Z}$. For any integers $a, b \in \mathbb{Z}$, show that $\varphi([any + bmx]_{mn}) = ([a]_m, [b]_n)$.]

(d) **Classical Version.** Consider any integers $a, b, m, n, x, y \in \mathbb{Z}$ with $mx + ny = 1$. For any integer $c \in \mathbb{Z}$, show that

$$\begin{cases} c & \equiv a \bmod m, \\ c & \equiv b \bmod n. \end{cases} \quad \Longleftrightarrow \quad c \equiv any + bmx \bmod mn.$$

[Actually, there is really nothing to "do", so you don't have to do this part.]

5. Permutation Matrices. For any permutation $f \in S_n$ (i.e., for any invertible function $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$) we define the $n \times n$ *permutation matrix* $[f]$ as follows:

$$ij \text{ entry of } [f] = \begin{cases} 1 & f(j) = i, \\ 0 & \text{else.} \end{cases}$$

(a) Write out the six 3×3 matrices corresponding to the elements of S_3.

(b) The definition of $[f]$ can be rephrased to say that $[f]\mathbf{e}_j = \mathbf{e}_{f(j)}$ where $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbb{R}^n$ are the standard basis vectors. Use this fact to prove that

$$[f \circ g] = [f][g] \text{ for all permutations } f, g \in S_n.$$

[Hint: You only need to check that $[f \circ g]\mathbf{e}_j = [f][g]\mathbf{e}_j$ for each basis vector $\mathbf{e}_j$.]

(c) It follows from (b) that the map $f \mapsto [f]$ is a group homomorphism $S_n \to GL_n(\mathbb{R})$. In fact, show that $[f] \in O_n(\mathbb{R})$ for all $f \in S_n$. [Hint: You only need to show that $[f^{-1}] = [f]^T$. For all i, j note that $f(j) = i$ if and only if $f^{-1}(i) = j$.]

(d) For any permutation $f \in S_n$, we define its *sign* as the determinant of its matrix:

$$\text{sgn}(f) := \det([f]).$$

Prove that sgn is a group homomorphism $S_n \to \{\pm 1\}$. [Hint: Every orthogonal matrix $A^T A = I$ satisfies $\det(A) = \pm 1$.]

(e) Prove that the sign homomorphism $S_n \to \{\pm 1\}$ is **surjective** and its kernel is the alternating subgroup A_n. [Hint: You can assume that every transposition t satisfies $\text{sgn}(t) = -1$. We previously showed that every permutation can be expressed as a product of transpositions. By definition, A_n is the set of permutations that can be expressed as a product of evenly-many transpositions.]