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

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

(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:

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

(a): *Reflexive.* Consider any $a \in G$. Since H contains the identity we have $a^{-1} * a = \varepsilon \in H$ and hence $a \sim a$. *Symmetric.* Consider $a, b \in G$ and suppose that $a \sim b$, so that $a^{-1} * b \in H$. Then since H is closed under inversion we have $b^{-1} * a = (a^{-1} * b) \in H$, so that $b \sim a$. *Transitive.* Consider any $a, b, c \in G$ with $a \sim b$ and $b \sim c$, so that $a^{-1} * b \in H$ and $b^{-1} * c \in H$. Then since H is closed under $*$ we have $a^{-1} * c = (a^{-1} * b) * (b^{-1} * c) \in H$, so that $a \sim c \in H$.

(b): First we will show that $[a] \subseteq a * H$. Consider any element $b \in [a]$, so that $a \sim b$ and hence $a^{-1} * b \in H$. Let's write $h = a^{-1} * b$. Then we have $b = a * h \in a * H$. Conversely, we will show that $a * H \subseteq [a]$. Consider any element $b \in a * H$, which can be written as $b = a * h$ for some $h \in H$. We observe that $a^{-1} * b = h \in H$, so that $a * b$ and $b \in [a]$.

(c): Suppose that $H \subseteq G$ is a normal subgroup so that for all $g \in G$ and $h \in H$ there exists some $h' \in H$ satisfying $g*h = h'*g$. Furthermore, suppose that we have $[a] = [a']$ and $[b] = [b']$, so that $a^{-1} * a' \in H$ and $b^{-1} * b' \in H$. In this case we want to show that $[a * b] = [a' * b']$, or, in other words, that $(a * b)^{-1} * (a' * b') \in H$. First observe that

$$(a * b)^{-1} * (a' * b) = b^{-1} * a^{-1} * a' * b'.$$

We have assumed that $a^{-1} * a' \in H$, so let's write $h = a^{-1} * a'$. Then since H is normal there exists some $h' \in H$ satisfying $b^{-1} * h = h' * b^{-1}$. Finally, since $b^{-1} * b' \in H$ and since H is closed under $*$ we have

$$\begin{aligned}(a * b)^{-1} * (a' * b) &= b^{-1} * a^{-1} * a' * b' \\ &= b^{-1} * h * b' \\ &= h' * b^{-1} * b' \in H,\end{aligned}$$

as desired.

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

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

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

(a): The fat that $ab = ba$ implies that

$$(ab)^k = (ab)(ab)\cdots(ab) = (aa\cdots a)(bb\cdots b) = a^k b^k \quad \text{for any } k \in \mathbb{N}.$$

Since $\gcd(n,m)$ is a common divisor of m and n we can write $m = \gcd(m,n)m'$ and $n = \gcd(m,n)n'$ for some $m', n' \in \mathbb{Z}$, which also implies that $\text{lcm}(m,n) = mn' = nm'$. Hence

$$(ab)^{\text{lcm}(m,n)} = a^{\text{lcm}(m,n)} b^{\text{lcm}(m,n)} = a^{mn'} b^{nm'} = (a^m)^{n'} (b^n)^{m'} = 1^{n'} 1^{m'} = 1.$$

(b): You showed on a previous homework that

$$(ab)^k = 1 \iff \#\langle ab\rangle \mid k.$$

Hence from part (a) we have $\#\langle ab\rangle \mid \text{lcm}(m,n)$.

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 $\text{lcm}(m,n) = mn/\gcd(m,n) < mn$. 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 $\text{lcm}(m,n)$.]

(a): *Associative.* Consider any three pairs $(a,\alpha), (b,\beta), (c,\gamma) \in G \times H$. Since $*$ and $\bullet$ are associative operations, we have

$$\begin{aligned}
(a,\alpha) \diamond ((b,\beta) \diamond (c,\gamma)) &= (a,\alpha) \diamond (b * c, \beta \bullet \gamma) \\
&= (a * (b * c), \alpha \bullet (\beta \bullet \gamma)) \\
&= ((a * b) * c, (\alpha \bullet \beta) \bullet \gamma) \\
&= (a * b, \alpha \bullet \beta) \diamond (c, \gamma) \\
&= ((a,\alpha) \diamond (b,\beta)) \diamond (c,\gamma).
\end{aligned}$$

Hence $\diamond$ is an associative operation. *Identity.* For any $(g,h) \in G \times H$, the pair $(\varepsilon_G, \varepsilon_H)$ satisfies

$$(g,h) \diamond (\varepsilon_G, \varepsilon_H) = (g * \varepsilon_G, h \bullet \varepsilon_H) = (g,h)$$

and

$$(\varepsilon_G, \varepsilon_H) \diamond (g,h) = (\varepsilon_G * g, \varepsilon_H \bullet h) = (g,h),$$

hence $(\varepsilon_G, \varepsilon_H) \in G \times H$ is a two-sided identity. *Inverse.* For any pair $(g,h) \in G \times H$ let g^{-1} and h^{-1} denote the inverse elements in G and H. Then we have

$$(g,h) \diamond (g^{-1}, h^{-1}) = (g * g^{-1}, h \bullet h^{-1}) = (\varepsilon_G, \varepsilon_H)$$

and

$$(g^{-1}, h^{-1}) \diamond (g,h) = (g^{-1} * g, h^{-1} \bullet h) = (\varepsilon_G, \varepsilon_H),$$

so that (g^{-1}, h^{-1}) is a two-sided inverse of (g,h).

(b): Note that for any $g \in G$ and $h \in H$ we have

$$\begin{aligned}\tilde{g} \diamond \tilde{h} &= (g, \varepsilon_H) \diamond (\varepsilon_G, h) \\ &= (g * \varepsilon_G, \varepsilon_H \bullet h) \\ &= (g, h) \\ &= (\varepsilon_G * g, h \bullet \varepsilon_H) \\ &= (\varepsilon_G, h) \diamond (g, \varepsilon_H) \\ &= \tilde{h} \diamond \tilde{g}.\end{aligned}$$

From Problem 2(c) it follows that if $g^m = \varepsilon_G$ and $h^n = \varepsilon_H$, so that $\tilde{g}^m = (\varepsilon_G, \varepsilon_H)$ and $\tilde{h}^n = (\varepsilon_G, \varepsilon_H)$, then $\#\langle (g,h)\rangle \,|\, \mathrm{lcm}(m,n)$. In particular, if G and H are finite then we know from Lagrange that $g^{\#G} = \varepsilon_G$ and $h^{\#H} = \varepsilon_H$, hence every element (g,h) of the group $G \times H$ satisfies $\#\langle (g,h)\rangle \leq \mathrm{lcm}(\#G, \#H)$.

(c): From the previous remark we know that every element of the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has order $\leq \mathrm{lcm}(m,n)$. Note that this group has mn elements. If it were a cyclic group then it would have some element of order mn. But if $\gcd(m,n) \neq 1$ then $\mathrm{lcm}(m,n) = mn/\gcd(m,n) < mn$, which is impossible from the previous remark. Hence

$$\gcd(m,n) \neq 1 \quad \Longrightarrow \quad \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ is not cyclic.}$$

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.]

(a): To show that the rule is well-defined, we need to show that $[a]_{mn} = [b]_{mn}$ implies $([a]_m, [a]_n) = ([b]_m, [b]_n)$, i.e., that $[a]_m = [b]_m$ and $[b]_m = [b]_n$. In other words, we need to show that

$$mn|(a-b) \quad \Longrightarrow \quad m|(a-b) \text{ and } n|(a-b).$$

To see that this is true, suppose that $a - b = kmn$ for some $k \in \mathbb{Z}$. Then we have $a - b = (kn)m$ and $a - b = (km)n$, which implies that $m|(a-b)$ and $n|(a-b)$. The fact that φ is a group homomorphism follows direction from the definitions:[1]

$$\begin{aligned}\varphi([a]_{mn}+[b]_{mn}) &= \varphi([a+b]_{mn})\\ &= ([a+b]_m,[a+b]_n)\\ &= ([a]_m+[b]_m,[a]_n+[b]_n)\\ &= ([a]_m,[a]_n)+([b]_m,[b]_n)\\ &= \varphi([a]_{mn})+\varphi([b]_{mn}).\end{aligned}$$

(b): If $\gcd(m,n)=1$ then from Bézout's identity we can write $mx+ny=1$ for some $x,y\in\mathbb{Z}$. It follows from this that $m|c$ and $n|c$ imply $mn|c$ for any integer c. Indeed, suppose that $c=mm'$ and $c=nn'$. Then we have

$$\begin{aligned}mx+ny &= 1\\ cmx+cny &= c\\ nn'mx+mm'ny &= c\\ mn(n'x+m'y) &= c,\end{aligned}$$

hence $mn|c$. We will use this to prove that φ is injective. Indeed, if $\gcd(m,n)=1$ then for all $a,b\in\mathbb{Z}$ we have

$$m|(a-b) \text{ and } n|(a-b) \quad\Longrightarrow\quad mn|(a-b),$$

which translates to the statement that

$$([a]_m,[a]_n)=([b]_m,[b]_n) \quad\Longrightarrow\quad [a]_{mn}=[b]_{mn}.$$

(c): If $\gcd(m,n)=1$ then from parts (a) and (b) we have an injective function $\varphi:\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. Since these two sets have the same size (namely, mn) it follows from the pigeonhole princkple that φ must also be surjective. However, this indirect proof gives no hint of how to compute the inverse: $\varphi^{-1}([a]_m,[b]_n)=??$

Since $\gcd(m,n)=1$ we can write $mx+ny=1$. In this case I claim that

$$\varphi^{-1}([a]_m,[b]_n)=[any+bmx]_{mn}.$$

To show this we only need to show that $\varphi([any+bmx]_{mn})=([a]_m,[b]_n)$, which amounts to showing that $[any+bmx]_m=[a]_m$ and $[any+bmx]_n=[b]_n$. For the first statement, we have (working mod m):

$$\begin{aligned}any+bmx &\equiv any+b0x\\ &\equiv any\\ &\equiv a(1-mx)\\ &\equiv a-amx\\ &\equiv a-a0x\\ &\equiv a.\end{aligned}$$

[1]This typical in abstract algebra. The proof is "trivial" because we have hidden the entire history of the subject within the notation.

For the second statement we have (working mod n):

$$\begin{aligned} any + bmx &\equiv a0x + bmx \\ &\equiv bmx \\ &\equiv b(1 - ny) \\ &\equiv b - bny \\ &\equiv b - b0y \\ &\equiv b. \end{aligned}$$

(d): We discussed this in class.

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.]

(a): Here is a table of cycle notation versus matrix notation:[2]

f	ε	(12)	(13)	(23)	(123)	(132)
$[f]$	$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & & 1 \\ & 1 & \end{pmatrix}$	$\begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}$	$\begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}$

(b): We can think of $[f]$ as a permutation of the standard basis vectors: $[f]\mathbf{e}_j = \mathbf{e}_{f(j)}$. We can also think of $[f]\mathbf{e}_j$ as the jth column of the matrix $[f]$. To show that $[f \circ g] = [f][g]$ it

[2] It is common to omit zeros in matrix notation.

suffices to show that these two matrices have the same column vectors:

$$\begin{aligned} [f \circ g]\mathbf{e}_j &= \mathbf{e}_{(f\circ g)(j)} \\ &= e_{f(g(j))} \\ &= [f]\mathbf{e}_{g(j)} \\ &= [f][g]\mathbf{e}_j. \end{aligned}$$

In other words, the function $f \mapsto [f]$ is a group homomorphism from S_n to $GL_n(\mathbb{R})$, and it follows from this that $[f^{-1}] = [f]^{-1}$.

(c): Note that $f(j) = i$ if and only if $f^{-1}(i) = j$, so that

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

In other words, we have $[f]^T = [f^{-1}] = [f]^{-1}$. We have shown that $[f] \in O_n(\mathbb{R})$, from which is follows that $\det([f]) = \pm 1$.[3]

(d): For any permutation $f \in S_n$ let $\text{sgn}(f) := \det([f])$, which we have shown is a number in the set $\{\pm 1\}$. I claim that the function $\text{sgn} : S_n \to \{\pm 1\}$ is a group homomorphism. Indeed, since the determinant is multiplicative we have

$$\begin{aligned} \text{sgn}(f \circ g) &= \det([f \circ g]) \\ &= \det([f][g]) \\ &= \det([f]) \det([g]) \\ &= \text{sgn}(f)\text{sgn}(g). \end{aligned}$$

(e): Finally, I claim that the sign homomorphism is surjective with kernel A_n. For this we will assume that $\text{sgn}(t) = -1$ for any transposition $t \in S_n$.[4] Then since $\text{sgn}(\varepsilon) = +1$ and $\text{sgn}((12)) = -1$ (for example), we see that sgn is surjective.

To show that $\ker(\text{sgn}) = A_n$, recall the definition:

$$A_n = \{f \in S_n : \text{there exist transpositions } t_1, \ldots, t_{2k} \text{ such that } f = t_1 \circ \cdots \circ t_{2k}\}.$$

Note that every such permutation satisfies

$$\text{sgn}(f) = \text{sgn}(t_1) \cdots \text{sgn}(t_{2k}) = (-1)^{2k} = 1^k = 1,$$

and hence $A_n \subseteq \ker(\text{sgn})$. For the other direction, recall that any permutation f can be expressed as some composition of transpositions $f = t_1 \circ \cdots t_\ell$ so that

$$\text{sgn}(f) = \text{sgn}(t_1) \cdots \text{sgn}(t_\ell) = (-1)^\ell.$$

If $\text{sgn}(f) = 1$ then ℓ must be even, and it follows that f can be expressed as a composition of "evenly-many" transpositions. Hence $\ker(\text{sgn}) \subseteq A_n$.

[3]Recall: If $A^T A = I$ then $\det(A)^2 = \det(A^T A) = \det(I) = 1$.

[4]This follows from fact that switching any two columns of a matrix multiplies the determinant by -1.