Math 561/661 **Fall 2023**
Homework 1 **Drew Armstrong**

---

1. Group Axioms. Let G be a set with a binary operation $(a,b) \mapsto a * b$. Consider the following four possible axioms:

(G1) For all $a,b,c \in G$ we have $a*(b*c) = (a*b)*c$.
(G2) There exists some $\varepsilon \in G$ such that $a * \varepsilon = \varepsilon * a = a$ for all $a \in G$.
(G3) For each $a \in G$ there exists some $b \in G$ such that $a * b = b * a = \varepsilon$.
(G4) For each $a \in G$ there exists some $c \in G$ such that $a * c = \varepsilon$.

The element ε in (G2) is called a *two-sided identity*. The element b in (G3) is called a *two-sided inverse* for a and the element c in (G3) is called a *right inverse* for a.

(a) If (G1) and (G2) hold, prove that the two-sided identity element is unique.
(b) If (G1), (G2) and (G3) hold, prove that the two-sided inverse is unique.
(c) Assuming that (G1) and (G2) hold, prove that that (G3) and (G4) are equivalent. [Hint: One direction is obvious. The hard part is to prove that the existence of right inverses implies the existence of two-sided inverses.]

(a) Assume that (G1) and (G2) hold and suppose that the elements $\varepsilon, \varepsilon' \in G$ both satisfy (G2). Then we have

$$\varepsilon = \varepsilon * \varepsilon' = \varepsilon'.$$

[Remark: Actually I didn't need to use (G1).]

(b) Assume that (G1), (G2) and (G3) hold and suppose that the elements $b, b' \in G$ both satisfy (G3). Then we have

$$b = b * \text{id} = b * (a * b') = (b * a) * b' = \text{id} * b' = b'.$$

(c) Assume that (G1) and (G2) hold. Then (G3) clearly implies (G4). On the other hand, suppose that (G4) holds. Then for all $a \in G$ there exists some $c \in G$ such that $a * c = \varepsilon$. But we can also apply (G4) to this c to obtain some $d \in G$ such that $c * d = \varepsilon$. Putting these together gives

$$d = \text{id} * d = (a * c) * d = a * (c * d) = a * \text{id} = a,$$

so that $c * d = c * a = \varepsilon$ and hence c is a two-sided inverse for a. Finally, since $a \in G$ was arbitrary we conclude that (G3) holds.

2. Groups of Matrices. Let R be a commutative ring. Prove that each of the following sets of matrices is a subgroup of $GL_n(R)$:

$$\begin{aligned} SL_n(R) &= \{A \in \text{Mat}_n(R) : \det A = 1\}, \\ O_n(R) &= \{A \in \text{Mat}_n(R) : A^T A = I\}, \\ SO_n(R) &= \{A \in \text{Mat}_n(R) : A^T A = I \text{ and } \det A = 1\}. \end{aligned}$$

[Hint: You will need the matrix identities $\det(AB) = \det(A)\det(B)$ and $(AB)^T = B^T A^T$.]

[Remark: I originally stated this problem in terms of the real numbers $\mathbb{R}$ but it applies equally well to any commutative ring R.]

Special Linear Group. Note that $\det(A) = 1 \in R^\times$ implies that A^{-1} exists, hence $SL_n(R)$ is a subset of $GL_n(R)$. We need to show that it is a subgroup. To see this we first note that $A, B \in SL_n(R)$ implies $AB \in SL_n(R)$ because $\det(A) = 1$ and $\det(B) = 1$ implies

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1.$$

Next we note that I is in $SL_n(R)$ becuase $\det(I) = 1$. Finally, if $A \in SL_n(R)$ we note that A^{-1} (which exists because SL_n is a subset of GL_n) is also in $SL_n(R)$ because

$$\begin{aligned} AA^{-1} &= I \\ \det(A)\det(A^{-1}) &= \det(I) \\ 1 \cdot \det(A^{-1}) &= 1 \\ \det(A^{-1}) &= 1. \end{aligned}$$

Orthogonal Group. If $AA^T = I$ then we have

$$\begin{aligned} \det(AA^T) &= \det(I) \\ \det(A)\det(A^T) &= 1 \\ \det(A)^2 &= 1, \end{aligned}$$

which implies that $\det(A) = \pm 1$. Since $\pm 1 \in R^\times$ this implies that $O_n(R)$ is a subset of $GL_n(R)$. We need to show that it is a subgroup. To see this we first note that $I \in O_n(R)$ because $I^T I = II = I$. Next we note that $A, B \in O_n(R)$ implies $AB \in O_n(R)$ since $A^T A = I$ and $B^T B = I$ imply

$$(AB)^T(AB) = B^T A^T AB = B^T IB = B^T B = I.$$

Finally, we will show that $A \in O_n(R)$ implies $A^{-1} \in O_n(R)$ to do this we will use the (highly nontrivial) fact that

$$AB = I \quad \Longrightarrow \quad BA = I.$$

Suppose that $A \in O_n(R)$ so that $A^T A = I$. Then we must have $AA^T = I$ and we can take the inverse of both sides to get

$$\begin{aligned} (AA^T)^{-1} &= I^{-1} \\ (A^T)^{-1}A^{-1} &= I \\ (A^{-1})^T A^{-1} &= I, \end{aligned}$$

which implies that $A^{-1} \in O_n(R)$.

[Remark: We discussed in class the fact that

$$A^T A = I \quad \Longleftrightarrow \quad \text{The columns of } A \text{ are orthonormal.}$$

The equivalence of $A^T A = I$ and $AA^T = I$ tells us that

$$\text{The columns of } A \text{ are orthonormal.} \quad \Longleftrightarrow \quad \text{The rows of } A \text{ are orthonormal.}$$

You will never find an elementary proof of this fact. This is an example of the mysterious influence between rows and columns of a matrix.]

Special Orthogonal Group. It is easy to show that the intersection of subgroups is a subgroup. Since $SL_n(R)$ and $O_n(R)$ are both subgroups of $GL_n(R)$, and since

$$SO_n(R) = SL_n(R) \cap O_n(R),$$

we conclude that $SO_n(R)$ is a subgroup of $GL_n(R)$.

3. Groups of Permutations. Let S_3 be the set of all permutations of the set $\{1, 2, 3\}$, i.e., all invertible functions

$$f : \{1, 2, 3\} \to \{1, 2, 3\}.$$

(a) List all 6 elements of the set. [I recommend using cycle notation.]
(b) We can think of $(S_3, \circ, \mathrm{id})$ as a group, where $\circ$ is functional composition and id is the identity function. Write out the full 6×6 group table.
(c) Let S_n be the group of permutations of $\{1, 2, \ldots, n\}$. An element of S_n is called a *transposition* if it switches two elements of the set and sends every other element to itself. We denote the transposition that switches $i \leftrightarrow j$ by $(ij) \in S_n$. Let $A_n \subseteq S_n$ be the subset of permutations that can be expressed as a composition of an **even** number of transpositions. Prove that $A_n \subseteq S_n$ is a subgroup.
(d) List all elements of the subgroup $A_3 \subseteq S_3$ and draw its group table.

(a) Here are the six permutations of $\{1, 2, 3\}$ in word notation and cycle notation:

word notation	cycle notation
123	ε
132	(23)
213	(12)
231	(123)
312	(132)
321	(13)

(b) Here is the group table:

$\circ$	ε	(12)	(13)	(23)	(123)	(132)
ε	ε	(12)	(13)	(23)	(123)	(132)
(12)	(12)	ε	(132)	(123)	(23)	(13)
(13)	(13)	(123)	ε	(132)	(12)	(23)
(23)	(23)	(132)	(123)	ε	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	ε
(132)	(132)	(23)	(12)	(13)	ε	(123)

(c) By the notation $(i_1, i_2, \ldots, i_k) \in S_n$, I mean the permutation that sends sends i_j to i_{j+1} for all $1 \le j < k$, sends i_k to i_1, and sends every other element of $\{1, 2, \ldots, n\}$ to itself. We call this kind of permutation a *k-cycle*. [Example: Transpositions are 2-cycles.] The cycle notation tells us that every element of S_n can be expressed as a composition of (commuting) cycles. Thus we will be done if we can show that every cycle is a composition of transpositions.

Here is the proof:

$$(i_1, i_2, \ldots, i_k) = (i_1, i_2) \circ (i_2, i_3) \circ \cdots \circ (i_{k-1}, i_k).$$

[Example: The permutation $f = 615432$ in word notation can be expressed as $f = (162)(35) = (162) \circ (35)$ in cycle notation, hence we have $f = (16) \circ (62) \circ (35)$.]

(d) Let $A_n \subseteq S_n$ be the subset consisting of permutations which can be expressed as a composition of an **even number** of transpositions. I claim that this is a subgroup. *Proof.*

- **Closure.** Suppose that $f, g \in A_n$. Then by definition we can write
$$f = s_1 \circ s_2 \circ \cdots \circ s_k \qquad \text{and} \qquad g = t_1 \circ t_2 \circ \cdots \circ t_\ell,$$
for some transpositions s_i and t_i, where k, ℓ are even numbers. But then
$$f \circ g = s_1 \circ s_2 \circ \cdots \circ s_k \circ t_1 \circ t_2 \circ \cdots \circ t_\ell$$
is a composition of $k + \ell$ transpositions, where $k + \ell$ is an even number.
- **Identity.** By convention we will say that the identity ε is a composition of zero transpositions. Since zero is an even number this means that $\varepsilon \in A_n$. If you don't buy that, let $t \in S_n$ be **any** transposition. Then we have
$$\varepsilon = t \circ t,$$
which is in A_n because 2 is an even number.
- **Inverses.** For any transposition $t \in S_n$ we have $t^2 = t \circ t = \varepsilon$ and hence $t^{-1} = t$. More generally, if $f = t_1 \circ t_2 \circ \cdots \circ t_k$ is any composition of transpositions then we have
$$f^{-1} = t_k \circ t_{k-1} \circ \cdots \circ t_2 \circ t_1.$$
It follows that $f \in A_n$ implies $f^{-1} \in A_n$. □

[Jargon: The subgroup $A_n \subseteq S_n$ is called the *alternating subgroup* of S_n.]

(e) Note that $(123) = (12) \circ (23)$ and $(132) = (12) \circ (13)$ are both in A_3. It is a bit harder to check that the elements $(12), (13), (23)$ are **not** in A_3. *Check.* Let's write $c = (123)$ so that $c^2 = c^{-1} = (132)$. Now assume for contradiction that (12) **can** be expressed as a composition of evenly many transpositions:
$$(12) = (t_1 \circ t_2) \circ \cdots \circ (t_{2k-1} \circ t_{2k}).$$
But from the group table we see that any two transpositions compose to ε, $c = (123)$ or $c^{-1} = (132)$. This implies that (12) is a power of c. Contradiction. /// We conclude that
$$A_3 = \{\varepsilon, (123), (132)\}.$$
Here is the group table:

$\circ$	ε	(123)	(132)
ε	ε	(123)	(132)
(123)	(123)	(132)	ε
(132)	(132)	ε	(123)

[Exercise: In general we have $\#A_n = n!/2$. Later we will give a short proof which depends on the identity $\det(AB) = \det(A)\det(B)$ for determinants.]