Math 561/661 **Fall 2018**
Homework 1 **Drew Armstrong**

---

1. An Example Cubic. Consider the cubic equation

$$x^3 - 6x - 6 = 0.$$

(a) Apply Cardano's formula to find **one specfic root** of the equation.
(b) Now apply Lagrange's method to find **all three roots**. [Hint: Follow the steps in the course notes. There will be a lot of simplification.]

2. Working With 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.

3. Working With 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.]

4. Groups of Matrices. Matrix multiplication is necessarily associative because it corresponds to composition of linear functions. You may recall from linear algebra that a real $n \times n$ matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ has a (unique) two-sided inverse precisely when $\det A \neq 0$. Now consider the following sets of matrices:

$$\begin{aligned}
GL_n(\mathbb{R}) &= \{A \in \mathrm{Mat}_n(\mathbb{R}) : \det A \neq 0\} \\
SL_n(\mathbb{R}) &= \{A \in \mathrm{Mat}_n(\mathbb{R}) : \det A = 1\} \\
O_n(\mathbb{R}) &= \{A \in \mathrm{Mat}_n(\mathbb{R}) : AA^T = I\} \\
SO_n(\mathbb{R}) &= \{A \in \mathrm{Mat}_n(\mathbb{R}) : AA^T = I \text{ and } \det A = 1\}.
\end{aligned}$$

Prove that each one of these sets is a group under matrix multiplication. [Hint: It is helpful to remember that $\det(AB) = \det(A)\det(B)$ and $(AB)^T = B^T A^T$ for all matrices $A, B \in \mathrm{Mat}_n(\mathbb{R})$.]

5. Order of an Element. Let $(G, *, \varepsilon)$ be a group and let $g \in G$ be any element. Then for all integers $n \in \mathbb{Z}$ we define the exponential notation

$$g^n := \begin{cases} \overbrace{g * g * \cdots * g}^{n \text{ times}} & \text{if } n > 0, \\ \varepsilon & \text{if } n = 0, \\ \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{-n \text{ times}} & \text{if } n < 0. \end{cases}$$

(a) Check that $g^{m+n} = g^m * g^n$ for all $m, n \in \mathbb{Z}$.
(b) Use this to prove that $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ is a subgroup of G.
(c) If $\langle g \rangle$ is a finite set, prove that there exists some $n \geq 1$ such that $g^n = \varepsilon$.
(d) If $\langle g \rangle$ is finite, and if $r \geq 1$ is the smallest number such that $g^r = \varepsilon$, prove that

$$\#\langle g \rangle = r.$$

This r is called the *order* of the element $g \in G$. If the set $\langle g \rangle$ is infinite we will say that g has *infinite order*.

6. Matrices of Finite and Infinite Order. Consider the matrices

$$J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ for any } \theta \in \mathbb{R}.$$

(a) Show that J is invertible and has infinite order.
(b) Show that $R_\theta R_{-\theta} = I$, hence R_θ is invertible.
(c) More generally, show that $R_\alpha R_\beta = R_{\alpha+\beta}$ for all angles $\alpha, \beta \in \mathbb{R}$.
(d) Conclude that for each integer $n \geq 1$ the matrix $R_{2\pi/n}$ has order n.
(e) For which angles θ does the matrix R_θ have infinite order?