Math 344 - Day 6: Examples and Proofs

So far, we have studied the **dihedral group** D_{2n}, which consists of the symmetries of a regular n-gon, under function composition. It is time to learn a few more examples.

Example 1. Fix any integer $n > 1$. Let $\mathbb{Z}_n$ denote the group whose elements are the integers $\{0, 1, \ldots, n-1\}$ and where the operation is addition (mod n). Why do you think these groups are called **cyclic groups**?

$$5 + 9 = 2 \pmod{12} \qquad \text{and} \qquad 6 + 11 = 5 \pmod{12}.$$

Example 2. Fix any integer $n > 1$. Let $\mathbb{U}_n$ denote the group whose elements are the integers in $\{0, 1, \ldots, n-1\}$ that are *relatively prime* to n, and where the operation is multiplication (mod n). The group $\mathbb{U}_n$ is called the (multiplicative) **group of units** mod n. How many elements does $\mathbb{U}_{18}$ have?

$$5 \cdot 9 = 13 \pmod{16} \qquad \text{and} \qquad 6 \cdot 11 = 2 \pmod{16}.$$

Example 3. Fix any integer $n > 1$. Let $M(n, \mathbb{R})$ denote the group whose elements are the $n \times n$ matrices whose entries are real numbers, and where the operation is matrix addition. This group is called the **additive matrix group** (over the reals). What is the identity of this group?

$$\begin{bmatrix} 1 & 2 \\ 5 & -2 \end{bmatrix} + \begin{bmatrix} 3 & -6 \\ 0 & 7 \end{bmatrix} = \begin{bmatrix} 4 & -4 \\ 5 & 5 \end{bmatrix}.$$

Example 4. Fix any integer $n > 1$. Let $GL(n, \mathbb{R})$ denote the group whose elements are the *invertible* $n \times n$ matrices whose entries are real numbers, and where the operation is matrix multiplication. This group is called the **general linear group** (over the reals). How could you quickly test an $n \times n$ matrix to see if it is invertible?

$$\begin{bmatrix} 1 & 2 \\ 5 & -2 \end{bmatrix} \cdot \begin{bmatrix} 1/6 & 1/6 \\ 5/12 & -1/12 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Example 5. Fix any integer $n > 1$. Let $SL(n, \mathbb{R})$ denote the group whose elements are the $n \times n$ matrices with real entries whose determinant equals 1, and where the operation is matrix multiplication. This group is called the **special linear group** (over the reals). What property of determinants guarantees closure for this group?

$$\begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \cdot \begin{bmatrix} 5 & -2 \\ -7 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Example 6. Fix any integer $n > 1$. Let S_n denote the group whose elements are the n! different permutations of the numbers $\{1, 2, \cdots, n\}$, and where the operation is function composition. This group is called the **symmetric group**. Can you find an element of largest order in S_5?

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

Direct proofs. Let G be a group. Suppose that $a, b \in G$, that $|a| = 2$, $|b| = 4$, and $ab = b^3a$.

a. Prove that $bab = a$.

b. Prove that $ab^2 = b^2a$.

b. Prove that $(ab)^{-1} = b^{-1}a^{-1}$. What assumptions about G did you need in your proof? Based on your proof, how could you state this result as a theorem?

If and only if proofs. Let G be a group.

a. Prove that G is commutative if and only if $(ab)^2 = a^2b^2$.

b. Prove that G is commutative if and only if $(ab)^{-1} = a^{-1}b^{-1}$.