Homework 1

1. For each of the following examples, either show that it is a group, or explain why it fails to be a group. If the example is a group, also determine whether it is abelian.

   (a) The integers $\mathbb{Z}$ with the operation $a \circ b = a - b$.

   (b) The integers $\mathbb{Z}$ with the operation $a \circ b = a + b + 1$.

   (c) The following set of 2×2 matrices with matrix multiplication:

$$\left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \quad a, b, c, d \in \mathbb{Z}, \quad ad - bc = 1, \quad a, d \text{ odd}, \quad b, c \text{ even} \right\}$$

2. For which subsets of integers $S \subset \mathbb{Z}$ does the set S with the operation of multiplication define a group? Explain your reasoning.

3. Consider the set $G = \{e, r, b, g, y, o\}$ with operation defined in Lecture 1. In this exercise you will verify that the operation defined by the Cayley table makes G a group.

   (a) Explain why Axiom 2 holds.

   (b) Write down the inverse of each element in G. Conclude Axiom 3 holds.

   (c) Verify Axiom 1, associativity. For example, check $r \circ (b \circ g) = (r \circ b) \circ g$ using the Cayley table. Write down at least 3 other examples verifying this axiom.

4. Let G be an arbitrary group. Given the equations $ax^2 = b$ and $x^3 = e$, solve for x.

5. For each of the following examples, show that the subset is a subgroup.

   (a) The subset $\{5k : k \in \mathbb{Z}\}$ of the group $(\mathbb{Z}, +)$.

   (b) The subset $\{3^k : k \in \mathbb{Z}\}$ of the group $(\mathbb{Q}^\times, \times)$.

   (c) The subset $\{a + b\sqrt{2} : a, b \in \mathbb{Q}, \ \ a, b \text{ not both } 0\}$ of the group $(\mathbb{R}^\times, \times)$.

6. Suppose a group G has the property that $a^2 = e$ for all $a \in G$. Show that G is abelian.

7. Show that the intersection of two subgroups of a group is again a subgroup.

8. Determine whether the following is the Cayley table of a group. Explain!

	a	b	c
a	a	b	c
b	b	c	a
c	c	b	c

9. Let a and b be elements of a group G. Prove that $ab^n a^{-1} = (aba^{-1})^n$ for any $n \in \mathbb{Z}$.