Group Members: ______________________________

Defn. A *binary operation* on a set G is a function that assigns to each ordered pair $(a, b) \in G$ an element c of G.

$$\begin{aligned} * : G \times G &\rightarrow G \\ (a, b) &\xrightarrow{*} c, \qquad \text{in other words, } a * b = c. \end{aligned}$$

Defn. A *group* is a nonempty set G together with a binary operation mapping each $(a, b) \in G \times G$ to $ab \in G$, along with the properties:
1. *Associativity.* For all $a, b, c \in G$, $(ab)c = a(bc)$.
2. *Identity.* There exists an element $e \in G$, called the *identity*, such that $ae = ea = a$ for all $a \in G$.
3. *Inverses.* For each element $a \in G$, there is an element $b \in G$, called the *inverse* of a, such that $ab = ba = e$.

(1) Examples and counterexamples of binary operations.
(a) List two binary operations which could be applied to $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, and $\mathbb{Z}$.
(b) List two binary operations on $\mathbb{Z}_n$, the integers $\mod n$ for some integer $n > 0$.
(c) List two binary operations on $M(2, \mathbb{R})$, the set of 2×2 matrices over the real numbers, along with the formulas describing the result of the binary operations.

(2) Show by counterexample that division over the nonzero reals $\mathbb{R}^*$ and subtraction over $\mathbb{Z}$ are not associative.

(3) Give the identity element for the following G and binary operation:
(a) Multiplication over nonzero rationals, $\mathbb{Q}^*$ **(b)** Addition over $\mathbb{Z}$, **(c)** Multiplication over $M(2, \mathbb{R})$.
(d) The positive rationals $\mathbb{Q}^+$ under the binary operation $(a, b) \rightarrow ab/2$.

(4) Describe the inverse element for the following G and binary operation:
(a) The complex numbers with modulus 1 $\{e^{i\theta} : 0 \leq \theta < 2\pi\}$ under multiplication,
(b) The positive rationals $\mathbb{Q}^+$ under the binary operation $(a, b) \to ab/2$.
(c) Explain why we shouldn't even look for inverses in the integers under subtraction.

Break. Matrix groups.

---

(5) Mimic the proof of Euclid's Lemma to prove this minor extension: Let a, b, c be positive integers. If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Break. Uniqueness of inverses for the integers under multiplication mod n.

Defn. The group $U(n)$ is defined to be the the set $U(n) = \{a \in \{0, 1, \ldots, n-1\} : \gcd(a, n) = 1\}$ under multiplication mod n.

---

(6) (On an attached sheet) Construct the Cayley tables for $U(8)$ and $U(10)$. Next to each Cayley table, list the elements in pairs with their inverses.