Group Members: ____

Definition of a ring
A *ring* R is a nonempty set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all $a, b, c \in R$:

1. (additive commutativity) $a + b = b + a$.
2. (additive associativity) $(a + b) + c = a + (b + c)$.
3. (additive identity) There exists $0 \in R$ such that $a + 0 = a$.
4. (additive inverses) There exists $-a \in R$ shuch that $a + (-a) = 0$.
5. (multiplicative associativity) $a(bc) = (ab)c$.
6. (bidirectional multiplicative distributivity) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

In a *commutative* ring, multiplication is also commutative.

An element $1 \in R$ is a *unity* provided $1a = a1 = a$ for all $a \in R$.

An element $a \in R$ is a *unit* provided there exists $a^{-1} \in R$ such that aa^{-1} is a unity.

---

(1) Let $R = \{0, 2, 4, 6, 8\}$ with addition and multiplication modulo 10 be a ring.
(a) Write out the multiplication table for R in the same layout as a Cayley table.
(b) Find all elements that are a unity of R by inspecting the table.
(c) Find all elements that are units of R by inspecting the table, and group the units in inverse pairs.

(2) Matrices are an excellent source of noncommutative rings. Define $M_2(\mathbb{Z})$ to be the set of 2×2 matrices with integer entries.

(a) Verify that $M_2(\mathbb{Z})$ is noncommutative by exhibiting a non-commuting pair.

(c) For what values of b is $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ a unity of $M_2(\mathbb{Z})$? Verify with a computation.

(c) For what values of b is the above matrix a unit of $M_2(\mathbb{Z})$? Verify with a computation, and give the form of the inverse.

Definition. An *idempotent* of a ring R is an element $a \in R$ such that $a^2 = a$.

---

(3) Find 4 distinct idempotents in $M_2(\mathbb{Z})$. Which of these are a unity or unit?

(4) $\mathbb{Q}[x]$ is the set of all polynomials in the variable x with rational coefficients under ordinary addition and multiplication. Define $R = \mathbb{Q}[x] \setminus \{q | q \in \mathbb{Q}^*\}$ by taking out all constant polynomials except the zero polynomial. Does R have a unity? Give a justification.

Fact. The zero (additive identity) of a ring is unique, because the ring is a group under addition.

Definition. Let $a \in R \setminus \{0\}$ and let $b \in R$. We say that a *divides* b, or $a|b$, if there exists $c \in R$ such that $b = ac$.

Definition. A *zero-divisor* of a ring R is an element $a \in R \setminus 0$ such that $ab = 0$ for some nonzero $b \in R$.

(5) By inspecting the multiplication table in (1):
(a) Find all of the divisors of 2, 4, 6, and 8.
(b) Find all of the zero-divisors.

(6) Find a zero-divisor in $M_2(\mathbb{Z})$ and verify by a computation.

Theorem 12.1: Rules of Multiplication
Let a, b, and c belong to a ring R. Then

1. $a0 = 0a = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

Furthermore, if R has a unity element 1, then

5. $(-1)a = -a$.
6. $(-1)(-1) = 1$.

Theorem 12.2: Uniqueness of the Unity and Inverses
If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Definition. A subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

Theorem 12.3: Subring Test
A subset S of a ring R is a subring of R provided
• (Non-empty) S is nonempty.
• (Closure under subtraction) For all $a, b \in S$, $a - b \in S$.
• (Closure under multiplication) For all $a, b \in S$, $ab \in S$.

(7) Define

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} | a, b \in \mathbb{Z} \right\}.$$

Use Theorem 12.3 to prove that S is a subring of $M_2(\mathbb{Z})$.

(8) If you finished everything else, prove Theorem 12.2.