Definition:
A commutative ring \( R \) is a set with two operations, addition and multiplication, such that:

(i) \( R \) is an abelian group under addition;
(ii) \( ab = ba \) for all \( a, b \in R \) (commutative law);
(iii) \( a(bc) = (ab)c \) for any \( a, b, c \in R \) (associative law);
(iv) there is an element \( 1 \in R \) with \( 1 \neq 0 \) and with \( 1 \cdot a = a \cdot 1 = a \) for any \( a \in R \);
(v) \( a(b + c) = ab + ac \) for any \( a, b, c \in R \) (distributive law).

Example:
1. \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) are commutative rings.
2. \( \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \) is a commutative ring.
3. \( \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \) is a commutative ring.
4. \( \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \) is not a ring. Moreover, \( \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \) is not a ring.
5. The set of all \( 2 \times 2 \) matrices is a noncommutative ring.
6. \( \mathbb{Z}_m \) is a commutative ring.

Theorem 1:
Let \( R \) be a commutative ring. Then:

(i) \( 0 \cdot a = 0 \) for any \( a \in R \).
(ii) If \( -a \) is that number which, when added to \( a \), gives \( 0 \), then \( (-1)(-a) = a \) for any \( a \in R \).
(iii) \( (-1)a = -a \) for any \( a \in R \).

Definition:
A subset \( S \) of a commutative ring \( R \) is a subring of \( R \) if:

(i) \( 1 \in S \);
(ii) if \( a, b \in S \), then \( a - b \in S \);
(iii) if \( a, b \in S \), then \( ab \in S \).

Example:
1. \( \mathbb{Z} \) is a subring of \( \mathbb{Q} \); \( \mathbb{Q} \) is a subring of \( \mathbb{R} \); \( \mathbb{R} \) is a subring of \( \mathbb{C} \);
2. \( \mathbb{Z}[i] \) is a subring of \( \mathbb{C} \).

Definition:
A domain is a commutative ring \( R \) that satisfies the cancellation law for multiplication:

if \( ca = cb \) and \( c \neq 0 \), then \( a = b \).
Example:
1. \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) are domains.
2. \( \mathbb{Z}_4 \) is not a domain, since from \( [2][2] = [2][0] \) does not follow \( [2] = [0] \).

**Theorem 2:**
A commutative ring \( R \) is a domain if and only if the product of any two nonzero elements of \( R \) is nonzero.
Proof:

$\Rightarrow$) Let $R$ be a domain, i.e. the cancellation law holds. We should prove that the product of any two nonzero elements of $R$ is nonzero. Assume to the contrary that there exist $a \neq 0, b \neq 0$ with

$$ab = 0. \hspace{1cm} (\ast)$$

Note that $0 \cdot b = 0$ by (i) of Theorem 1. Combining this with $(\ast)$, we get

$$ab = 0 \cdot b.$$

Canceling out $b$, we obtain $a = 0$. Contradiction.

$\Leftarrow$) Suppose the product of any two nonzero elements of $R$ is nonzero. We should prove that $R$ is a domain, i.e. the cancellation law holds. In fact, if

$$ca = cb \text{ with } c \neq 0,$$

then

$$0 = ca - cb = c(a - b).$$

Since $c \neq 0$ and the product of any two nonzero elements of $R$ is nonzero, it follows that $a - b = 0$, so $a = b$. ■

Corollary:

$\mathbb{Z}_m$ is a domain if and only if $m$ is a prime.
Proof:

$\implies$) Let $\mathbb{Z}_m$ be a domain. We should prove that $m$ is a prime. In fact, assume to the contrary that $m$ is composite, that is

$$m = ab, \quad \text{where} \quad 1 < a, b < m.$$  

Then

$$[a][b] = [0],$$

which contradicts Theorem 2.

$\iff$) Let $m$ be a prime. We should prove that $\mathbb{Z}_m$ is a domain. In fact, assume to the contrary that

$$[a][b] = [0]$$

for some nonzero $[a], [b] \in \mathbb{Z}_m$. This means

$$m \mid ab.$$  

From this by Euclid’s Lemma we get $m \mid a$ or $m \mid b$, which means

$$[a] = 0 \quad \text{or} \quad [b] = 0.$$  

We get a contradiction. $\blacksquare$
Definition:
A commutative ring $R$ is a set with two operations, addition and multiplication, such that:

(i) $R$ is an abelian group under addition;

(ii) $ab = ba$ for all $a, b \in R$ (commutative law);

(iii) $a(bc) = (ab)c$ for any $a, b, c \in R$ (associative law);

(iv) there is an element $1 \in R$ with $1 \neq 0$ and with $1 \cdot a = a \cdot 1 = a$ for any $a \in R$;

(v) $a(b+c) = ab + ac$ for any $a, b, c \in R$ (distributive law).
Example:
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings.
2. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a commutative ring.
3. $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a commutative ring.
4. $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Z}\}$ is not a ring. Moreover, $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$ is not a ring.
5. The set of all $2 \times 2$ matrices is a noncommutative ring.
6. $\mathbb{Z}_m$ is a commutative ring.
Theorem 1:
Let $R$ be a commutative ring. Then:

(i) $0 \cdot a = 0$ for any $a \in R$.

(ii) If $-a$ is that number which, when added to $a$, gives 0, then $(-1)(-a) = a$ for any $a \in R$.

(iii) $(-1)a = -a$ for any $a \in R$. 
Definition:
A subset $S$ of a commutative ring $R$ is a subring of $R$ if:
(i) $1 \in S$;
(ii) if $a, b \in S$, then $a - b \in S$;
(iii) if $a, b \in S$, then $ab \in S$.

Example:
1. $\mathbb{Z}$ is a subring of $\mathbb{Q}$; $\mathbb{Q}$ is a subring of $\mathbb{R}$; $\mathbb{R}$ is a subring of $\mathbb{C}$;
2. $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. 
Definition:
A domain is a commutative ring $R$ that satisfies the cancellation law for multiplication:

if $ca = cb$ and $c \neq 0$, then $a = b$. 
Example:
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are domains.
2. $\mathbb{Z}_4$ is not a domain, since from
   \[
   [2][2] = [2][0]
   \]
does not follow $[2] = [0]$. 
Theorem 2:
A commutative ring $R$ is a domain if and only if the product of any two nonzero elements of $R$ is nonzero.
Proof:

Let $R$ be a domain, i.e. the cancellation law holds. We should prove that the product of any two nonzero elements of $R$ is nonzero. Assume to the contrary that there exist $a \neq 0$, $b \neq 0$ with

$$ ab = 0. \quad (*) $$

Note that $0 \cdot b = 0$ by (i) of Theorem 1. Combining this with $(*)$, we get

$$ ab = 0 \cdot b. $$

Canceling out $b$, we obtain $a = 0$. Contradiction.
Suppose the product of any two nonzero elements of $R$ is nonzero. We should prove that $R$ is a domain, i.e. the cancellation law holds. In fact, if \( ca = cb \) with \( c \neq 0 \), then

\[
0 = ca - cb = c(a - b).
\]

Since \( c \neq 0 \) and the product of any two nonzero elements of $R$ is nonzero, it follows that \( a - b = 0 \), so \( a = b \). ■
Corollary:
$\mathbb{Z}_m$ is a domain if and only if $m$ is a prime.

Proof:
$\implies$) Let $\mathbb{Z}_m$ be a domain. We should prove that $m$ is a prime. In fact, assume to the contrary that $m$ is composite, that is

$$m = ab, \quad \text{where} \quad 1 < a, b < m.$$  

Then

$$[a][b] = [0],$$

which contradicts Theorem 2.
Let $m$ be a prime. We should prove that $\mathbb{Z}_m$ is a domain. In fact, assume to the contrary that
\[ [a][b] = [0] \]
for some nonzero $[a], [b] \in \mathbb{Z}_m$. This means that
\[ m \mid ab. \]
From this by Euclid’s Lemma we get $m \mid a$ or $m \mid b$, which means
\[ [a] = 0 \quad \text{or} \quad [b] = 0. \]
We get a contradiction. ■