1 Integral Domains

Definition 1.1: Zero-Divisors

A **zero-divisor** is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition 1.2: Integral Domain

An **integral domain** is a commutative ring with unity and no zero-divisors.

Remarks:

- Recall that a ring R has **unity** if $1 \in R$ is a multiplicative identity; that is, $1a = a1 = a$.
- Essentially, in an integral domain, a product is 0 only when one of the facts is 0. That is, $ab = 0$ only when $a = 0$ or $b = 0$.

1.1 Examples

Here are some examples of integral domains.

1.1.1 Example 1: The Integers

The ring of integers is an integral domain.

1.1.2 Example 2: Gaussian Integers

The ring of Gaussian integers $Z[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an integral domain.

1.1.3 Example 3: Ring of Polynomials

The ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is an integral domain.

1.1.4 Example 4: Square Root 2

The ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

1.1.5 Example 5: Modulo Prime Integers

The ring $\mathbb{Z}/p\mathbb{Z}$ of integers modulo a prime p is an integral domain.

1.1.6 Non-Example 1: Modulo Integers

The ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n is not an integral domain when n is not prime.

1.1.7 Non-Example 2: Matrices

The ring $M_2(\mathbb{Z})$ of 2×2 matrices over the integers is not an integral domain.

1.1.8 Non-Example 3: Direct Product

$\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain.

1.2 Properties of Integral Domains

Theorem 1.1: Cancellation

Let a, b, and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then:

$$b = c$$

Proof. From $ab = ac$, we know that $a(b - c) = 0$. Since $a \neq 0$, it follows that $b - c = 0$. □

2 Fields

Definition 2.1: Field

A **field** is a commutative ring with unity in which every nonzero element is a unit.

Remark: To verify that every field is an integral domain, observe that if a and b belong to a field with $a \neq 0$ and $ab = 0$, we can multiply both sides of the last expression by a^{-1} to obtain $b = 0$.

Theorem 2.1

A finite integral domain is a field.

Corollary 2.1

For every prime p, $\mathbb{Z}/p\mathbb{Z}$, the ring of integers modulo p is a field.