1 Integral Domains

Recall that rings do not have multiplicative cancellation. That is, $ab = ac$ does not imply that $b = c$. However, there are exceptions to this rule.

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 $ab = 0$.

For example, $2 \in \mathbb{Z}/4\mathbb{Z}$ is a zero divisor. That is:

$$2 \cdot 2 \equiv 0 \pmod 4$$

Another example is $M_2(\mathbb{R})$. Take $A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. Then:

$$A \cdot B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

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. This is because:

$$ab \equiv 0 \pmod p \iff p|ab \implies p|a \text{ or } p|b \implies a \equiv 0 \pmod p \text{ or } b \equiv 0 \pmod p$$

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. If we write $n = ab$, then $1 < a$ and $b < n$ implies that $ab \equiv 0 \pmod{b}$.

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. The reason why is because, for:

$$\mathbb{Z} \oplus \mathbb{Z} = \{(x, y) \mid x, y \in \mathbb{Z}\}$$

Take $(0, 1) \in \mathbb{Z} \oplus \mathbb{Z}$ and $(1, 0) \in \mathbb{Z} \oplus \mathbb{Z}$. Then:

$$(0, 1) \cdot (1, 0) = (0, 0)$$

1.2 Properties of Integral Domains

Theorem 1.1: Cancellation

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

$$a = 0 \text{ or } b = c$$

Proof. From $ab = ac$, we know that $ab - ac = 0$. Then, we know that $a(b - c) = 0$. There are two cases to consider:

- If $a \neq 0$, it follows that $b - c = 0$.
- Otherwise, $a = 0$ and it's trivial.

So, we are done. $\square$

2 Fields

Definition 2.1: Field

A **field** is a commutative ring with unity in which every nonzero element is a unit (i.e. every nonzero element has a multiplicative inverse).

Remarks:

- 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 $b = 0$.
- In other words, you can never have an x such that $0x = 1$.

2.1 Examples of Fields

Here are some examples and non-examples of fields.

2.1.1 Example 1: Infinite Sets

$\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$ are all fields.

2.1.2 Non-Example 1: Integers

$\mathbb{Z}$ is not a field because 2 does not have a multiplicative inverse.

2.1.3 Example 2: Matrices

$M_2(\mathbb{R})$ is not a field because not all matrcies have an inverse.

2.1.4 Non-Example 2: Polynomials

$\mathbb{R}[x]$ is not a field. This is because not all functions have a *polynomial* inverse. For example, the inverse of $x+3$ is $\frac{1}{x+3}$, which isn't a polynomial. However, $\mathbb{R}[x]$ is an integral domain.

2.2 Properties of Fields

Theorem 2.1

A finite integral domain is a field.

Proof. Let R be a finite integral domain and suppose $a \in R \setminus \{0\}$. Consider the set:

$$\{a, a^2, a^3, a^4, \dots\} \subseteq R$$

Because R is finite, there must be some overlap, i.e. there exists two integers $j < i$ such that $a^j = a^i$. This implies that $a^j = a^{i-j}a^j$. Since we have an integral domain, we can perform multiplicative cancellation; so:

$$1 = a^{i-j} \text{ for } i - j \geq 1$$

Then, $i - j - 1 \geq 0$ with $(a)(a^{i-j-1}) = a^{i-j} = 1$. So, $a^{-1} = a^{i-j-1}$ is a multiplicative inverse of a. $\square$

Corollary 2.1

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

Remark: This is often denoted $\mathbb{F}_p$ in this context.

Some other examples are:

- Fields with 9 elements: $\mathbb{F}_3[i] = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$. Recall that $i^2 = -1 \equiv 2 \pmod 3$.
- Fields witih 4 elements: $\{0, 1, a, b\}$.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

- $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ is a field. First, to show that it's a field, we need to show that every nonzero element has multiplicative inverses. Suppose $a + b\sqrt{5} \neq 0$. Then:

  $$a + b\sqrt{5} \neq 0 \iff b\sqrt{5} \neq a \iff (a, b) \neq (0, 0)$$

  In other words, a, b are not both zero. Note that since $\sqrt{5}$ is irrational, $\sqrt{5} \neq \frac{a}{b}$. So, $\frac{1}{a+b\sqrt{5}} \in \mathbb{R}$ by $a + b\sqrt{5}$ is not zero and $\mathbb{R}$ is a field.