CHAPTER 13

Integral Domains

Definition and Examples

**Example.** In $\mathbb{Z}_{12}$, $9 \cdot 4 = 0$.

**Definition (Zero-Divisors).** A zero-divisor is a nonzero element $a$ of a commutative ring $R$ such that there is a nonzero element $b \in R$ such that $a \cdot b = 0$.

**Definition (Integral Domain).** An integral domain is a commutative ring with identity and no zero-divisors.

**Example.**

1. The integers $\mathbb{Z}$ are an integral domain.
2. The Gaussian integers $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ is an integral domain.
3. The ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is an integral domain.
4. $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$ is an integral domain.

5. For $p$ prime, $\mathbb{Z}_p$ is an integral domain. The proof for this is in the Corollary to Theorem 13.2, which follows later. For $n$ not prime, the ring $\mathbb{Z}_n$ is not an integral domain.

6. $M_2(\mathbb{Z})$ is not an integral domain since
$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

7. $\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain since $(1, 0)(0, 1) = (0, 0)$. 
**Theorem** (13.1 — Cancellation). Let $D$ be an integral domain with $a, b, c \in D$. If $a \neq 0$ and $ab = ac$, then $b = c$.

**Proof.**

$$ab = ac \implies ab - ac = 0 \implies a(b - c) = 0.$$  
Since $a \neq 0$, $b - c = 0 \implies b = c$. 

**Fields**

**Definition** (Field). A **field** is a commutative ring with identity in which every nonzero element is a unit.

**Corollary.** A field is an integral domain.

**Proof.**

Suppose $a \neq 0$ and $ab = 0$. Since $a \neq 0$, $a^{-1}$ exists and

$$a^{-1}ab = a^{-1}0 \implies 1b = 0 \implies b = 0.$$  
Thus we have an integral domain. 

**Note.**

One can think of $ab^{-1}$ as $\frac{a}{b}$ in the same way we think of $a + (-b) = a - b$. In a field, addition, subtraction, multiplication, and division (except by 0) are closed.

**Example.** $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.
**Theorem (13.2 — Finite Integral Domains are fields).** A finite integral domain $D$ is a field.

**Proof.**

Let $a \in D$, $a \neq 0$. If $a = 1$, $a^{-1} = 1$ and $a$ is a unit, so suppose $a \neq 1$.

Consider the following sequence of elements of $D$: $a, a^2, a^3, \ldots$.

Since $D$ is finite, $\exists i, j \in \mathbb{N}$ with $i > j$ and $a^i = a^j$.

By cancellation, $a^{i-j} = 1$. Since $a \neq 1$, $i - j > 1 \implies a^{i-j-1} = a^{-1}$.

Thus $a$ is a unit. Since $a$ was arbitrary, $D$ is a field. \qed

**Corollary ($\mathbb{Z}_p$ is a field).** For $p$ prime, $\mathbb{Z}_p$ is a field.

**Proof.**

Suppose $a, b \in \mathbb{Z}_p$, and $ab = 0$. Then $ab = pk$ for some $k \in \mathbb{Z}$. By Euclid’s Lemma, $p|a$ or $p|b \implies a = 0 \mod p$ or $b = 0 \mod p \implies a = 0$ or $b = 0$. Thus $\mathbb{Z}_p$ is an integral domain, and so is also a field by Theorem 13.2. \qed

**Example.** Let $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. That $\mathbb{Q}[\sqrt{3}]$ is a commutative ring with identity is fairly clear. Suppose $a + b\sqrt{3} \neq 0$. Then $a - b\sqrt{3} \neq 0$ also since $a \neq 0$ or $b \neq 0$. With $a + b\sqrt{3}$ viewed as an element of the superset $\mathbb{R}$,

$$
(a + b\sqrt{3})^{-1} = \frac{1}{a + b\sqrt{3}} = \frac{1}{a + b\sqrt{3}} \cdot \frac{a - b\sqrt{3}}{a - b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \in \mathbb{Q}[\sqrt{3}].
$$

Thus $a + b\sqrt{3}$ is a unit and $\mathbb{Q}[\sqrt{3}]$ a field.
Example (A Field with 9 Elements).

\( \mathbb{Z}_3[i] = \{a + bi | a, b \in \mathbb{Z}_3\} = \{0, 1, 2, i, 1 + i, 2 + i, 1 + 2i, 2 + 2i\}, i^2 = -1, \)

the ring of Gaussian integers modulo 3 is a field, with the multiplication table for the nonzero elements below:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>i</th>
<th>1 + i</th>
<th>2 + i</th>
<th>2i</th>
<th>1 + 2i</th>
<th>2 + 2i</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>i</td>
<td>1 + i</td>
<td>2 + i</td>
<td>2i</td>
<td>1 + 2i</td>
<td>2 + 2i</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2i</td>
<td>2 + 2i</td>
<td>1 + 2i</td>
<td>2i</td>
<td>1 + i</td>
<td>1 + i</td>
</tr>
<tr>
<td>i</td>
<td>i</td>
<td>2i</td>
<td>2</td>
<td>2 + i</td>
<td>2 + 2i</td>
<td>1</td>
<td>1 + i</td>
<td>1 + i</td>
</tr>
<tr>
<td>1 + i</td>
<td>1 + i</td>
<td>2 + 2i</td>
<td>2 + i</td>
<td>2i</td>
<td>1</td>
<td>1 + 2i</td>
<td>2i</td>
<td>i</td>
</tr>
<tr>
<td>2 + i</td>
<td>2 + i</td>
<td>1 + 2i</td>
<td>2 + 2i</td>
<td>1</td>
<td>i</td>
<td>1 + i</td>
<td>2i</td>
<td>2</td>
</tr>
<tr>
<td>2i</td>
<td>2i</td>
<td>i</td>
<td>1</td>
<td>1 + 2i</td>
<td>1 + i</td>
<td>2</td>
<td>2 + 2i</td>
<td>2 + i</td>
</tr>
<tr>
<td>1 + 2i</td>
<td>1 + 2i</td>
<td>2 + i</td>
<td>1 + i</td>
<td>2</td>
<td>2i</td>
<td>2 + 2i</td>
<td>i</td>
<td>1</td>
</tr>
<tr>
<td>2 + 2i</td>
<td>2 + 2i</td>
<td>1 + i</td>
<td>1 + 2i</td>
<td>i</td>
<td>2</td>
<td>2 + i</td>
<td>1</td>
<td>2i</td>
</tr>
</tbody>
</table>

Note. For any \( x \in \mathbb{Z}_3[i] \), \( 3x = x + x + x = 0 \mod 3 \). In the subring \( \{0, 4, 8, 12\} \) of \( \mathbb{Z}_{12} \), \( 4x = x + x + x + x = 0 \).

Characteristic of a Ring

Definition (Characteristic of a Ring). The characteristic of a ring \( R \) is the least positive integer \( n \) such that \( nx = 0 \) for all \( x \in R \). If no such integer \( n \) exists, we say \( R \) has characteristic 0. The characteristic of \( R \) is denoted as \( \text{char} R \).

Example.

\( \mathbb{Z} \) has characteristic 0, \( \mathbb{Z}_n \) has characteristic \( n \), and \( \text{char} \mathbb{Z}_2[x] = 2 \) (an infinite ring with a nonzero characteristic).
Theorem (13.3 — Characteristic of a Ring with Unity). Let $R$ be a ring with unit 1. If 1 has infinite order under addition, then char $R = 0$. If 1 has order $n$ under addition, then char $R = n$.

Proof.

If $|1| = \infty$, $\not\exists n \ni n \cdot 1 = 0$, so char $R = 0$.

Suppose $|1| = n$. Then $n \cdot 1 = 0$ and $n$ is the least positive integer with this property. Then, for all $x \in R$,

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ terms}} = \underbrace{1x + 1x + \cdots + 1x}_{n \text{ terms}} = \underbrace{(1 + 1 + \cdots + 1)x}_{n \text{ terms}} = 0x = 0.$$  

Thus char $R = n$. \hfill $\Box$

Lemma (Page 251 # 15). If $m, n \in \mathbb{Z}$ and $a, b \in R$, a ring, then

$$(m \cdot a)(n \cdot b) = (mn) \cdot (ab).$$

Proof.

For $m, n > 0$,

$$(m \cdot a)(n \cdot b) = \underbrace{(a + a + \cdots + a)}_{m \text{ terms}} \underbrace{(b + b + \cdots + b)}_{n \text{ terms}} = \underbrace{(ab + ab + \cdots + ab)}_{mn \text{ terms}} = (mn) \cdot (ab).$$

The other cases are similar. \hfill $\Box$

Theorem (13.4 — Characteristic of an integral domain). If $D$ is an integral domain, then char $D = 0$ or char $D$ is prime.

Proof.

Suppose the additive order of 1 is finite. Suppose $|1| = n$ and $n = st$ with $1 \leq s, t \leq n$. Then, by the Lemma,$0 = n \cdot 1 = (st) \cdot (1) = (s \cdot 1)(t \cdot 1)$. Thus $s \cdot 1 = 0$ or $t \cdot 1 = 0$.

Since $n$ is the least positive integer such that $n \cdot 1 = 0$, $s = n$ or $t = n$. Thus, $n$ is prime. \hfill $\Box$
Note. In high school algebra, we learned to solve polynomial equations like \(x^2 - 5x + 6 = 0\) by first factoring the left side to get \((x - 3)(x - 2) = 0\) and then setting each factor equal to 0 to get \(x - 3 = 0\) and \(x - 2 = 0\), and thus \(x = 3\) and \(x = 2\) as the solution set.

But suppose we try to solve the same equation in \(\mathbb{Z}_{12}\). We do get 2 and 3 as solutions just as above. But now \(x = 6\) is also a solution that we cannot find by factoring.

\[(6 - 3)(6 - 2) = 3 \cdot 4 = 12 = 0 \mod 12.\]

The issue is that \(\mathbb{Z}_{12}\) is not an integral domain. We can be sure that the factoring method gives us all the solutions of a polynomial equation only if we know we are working in an integral domain.

Following is a table of some of the rings and their properties.

<table>
<thead>
<tr>
<th>Ring</th>
<th>Form of Element</th>
<th>Unity</th>
<th>Commutative</th>
<th>Integral Domain</th>
<th>Field</th>
<th>Characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\mathbb{Z})</td>
<td>(k)</td>
<td>1</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>0</td>
</tr>
<tr>
<td>(\mathbb{Z}_n, \text{ n composite})</td>
<td>(k)</td>
<td>1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>(n)</td>
</tr>
<tr>
<td>(\mathbb{Z}_p, \text{ p prime})</td>
<td>(k)</td>
<td>1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>(p)</td>
</tr>
<tr>
<td>(\mathbb{Z}[x])</td>
<td>(a_nx^n + \cdots + a_1x + a_0)</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>0</td>
</tr>
<tr>
<td>(n\mathbb{Z}, n &gt; 1)</td>
<td>(nk)</td>
<td>None</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>0</td>
</tr>
</tbody>
</table>
| \(M_2(\mathbb{Z})\) | \[
\begin{bmatrix}
    a & b \\
    c & d
\end{bmatrix}
\] | \[
\begin{bmatrix}
    1 & 0 \\
    0 & 1
\end{bmatrix}
\] | No           | No             | No    | 0              |
| \(M_2(2\mathbb{Z})\) | \[
\begin{bmatrix}
    2a & 2b \\
    2c & 2d
\end{bmatrix}
\] | None  | No           | No             | No    | 0              |
| \(\mathbb{Z}[i]\) | \(a + bi\)      | 1     | Yes         | Yes             | No    | 0              |
| \(\mathbb{Z}_3[i]\) | \(a + bi; a, b \in \mathbb{Z}_3\) | 1     | Yes         | Yes             | Yes   | 3              |
| \(\mathbb{Z}[\sqrt{2}]\) | \(a + b\sqrt{2}; a, b \in \mathbb{Z}\) | 1     | Yes         | Yes             | No    | 0              |
| \(\mathbb{Q}[\sqrt{2}]\) | \(a + b\sqrt{2}; a, b \in \mathbb{Q}\) | 1     | Yes         | Yes             | Yes   | 0              |
| \(\mathbb{Z} \oplus \mathbb{Z}\) | \((a, b)\)      | (1, 1) | Yes         | No              | No    | 0              |