# Lecture 2: Integral Domains and Fields

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

# Division rings and Fields

**Definition**

A ring with unity is called a **division ring** (skew-field) if every nonzero element of $R$ is a unit. A commutative division ring $R$ is called a **field**.

A ring $R$ is a division ring$\Leftrightarrow$ $(R^*, .)$ is a group.
A ring $R$ is a field$\Leftrightarrow$ $(R^*, .)$ is a commutative group.

**Examples:**

**1.** $\mathbb{Z}$ is not a field. Since the only invertible elements are 1 and $-1$.
**2.** $\mathbb{R}, \mathbb{Q}$, and $\mathbb{C}$ are fields.
**3.** $\mathbb{Z}[i]$ is not a field.
**4.** $\mathbb{Q}[i]$ is a field.

**5.** Let $\mathbb{H} = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in \mathbb{R}\}$ be a set of real quaternions. $\mathbb{H}$ is a ring with the operations quaternion addition and quaternion multiplication that are defined as:

$$\begin{aligned} & (a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k) \\ = \; & (a_0 + b_0) + (a_1 + b_1)\, i + (a_2 + b_2)\, j + (a_3 + b_3)\, k \end{aligned}$$

$$\begin{aligned} & (a_0 + a_1 i + a_2 j + a_3 k) \times (b_0 + b_1 i + b_2 j + b_3 k) \\ = \; & (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) \\ & + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)\, i \\ & + (a_1 b_3 + a_3 b_1 + a_4 b_2 - a_2 b_4)\, j \\ & + (a_1 b_4 + a_4 b_1 + a_2 b_3 - a_3 b_2)\, k. \end{aligned}$$

The ring $(\mathbb{H}, +, \times)$, which is called the quaternion ring, is a division ring. Note that $(\mathbb{H}, +, \times)$ is not a field, since $(\mathbb{H}, +, \times)$ is not commutative.

# Zero Divisor

## Definition

An element $0_R \neq a \in R$ is called a **zero divisor** if there exists $0_R \neq b \in R$ such that either $ab = 0_R$ or $ba = 0_R$. A ring $R$ has no zero divisors if for all $a, b \in R$, $ab = 0_R$ implies $a = 0_R$ or $b = 0_R$.

We do not call the element $0_R$ a zero divisor. An element can not be a zero divisor and a unit simultaneously.

**Examples:**

**1.** $\mathbb{Z}$ is a ring without zero divisors.

**2.** $M_2(\mathbb{Z})$ has zero divisors. For example, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ are zero divisors, since $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \odot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

**3.** $\mathbb{Z}_6$ has zero divisors. In particular, $\overline{2}, \overline{3}, \overline{4}$ are zero divisors in $\mathbb{Z}_6$.

**4.** The subring $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\} \leq \mathbb{Z}_8$ has zero divisors.

**5.** The subring $\{\overline{0}, \overline{2}, \overline{4}\} \leq \mathbb{Z}_6$ has no zero divisors.

**6.** All nonzero nilpotent elements are zero divisors.

# Zero Divisor

**Remark:**

- Every nonzero element in a finite commutative ring with unity is either a unit or a zero divisor. Therefore, in $\mathbb{Z}_n$ the zero divisors are precisely those nonzero elements that are not relatively prime to $n$.
- If $R$ is a ring without zero divisors, then every subring of $R$ has no zero divisor also. But if a ring $R$ has zero divisors, then a subring of R may have zero divisors or not. In Example 5, $\mathbb{Z}_6$ has zero divisors but its subring $\left\{\overline{0}, \overline{2}, \overline{4}\right\}$ has no zero divisors.

# Integral Domain

## Definition

Let $R$ be a commutative ring with unity. $R$ is called an **integral domain** if $R$ has no zero divisors.

**Examples:**

**1.** $\mathbb{Z}$ is an integral domain.
**2.** $M_2(\mathbb{Z})$ is not an integral domain.
**3.** $\mathbb{Z}_n$ is an integral domain$\Leftrightarrow$ $n$ is a prime.
**4.** $\mathbb{Z}[i]$ is an integral domain.
**5.** $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain, since it has zero divisors;
$(1,0)(0,1) = (0,0)$.

## Theorem

*The cancellation laws hold in a ring $R \Leftrightarrow R$ has no zero divisors.*

# Integral Domain and Fields

**Theorem**

1. *Every field is an integral domain.*
2. *Every finite integral domain is a field.*

**Corollary**

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

All idempotent elements of an integral domain $D$ are $0_D$ or $1_D$.

**Remark:**

- There is an integral domain with $n$ elements $\Leftrightarrow$ $n$ is a power of a prime number.
- Let $D$ be a finite integral domain, with $|D| = n$ . Then $D$ is a finite field, and we must have $n = p^k$, with prime $p$ and $k \in \mathbb{Z}^+$. Conversely, for any prime power $p^k$, there is an integral domain $F_{p^k}$.

**Example:** There is not any integral domain with 6 elements. There is an integral domain with 4 elements.

# Subfields

## Definition

Let $(F, +, .)$ be a field and $K \subseteq F$. $(K, +, .)$ is called a subfield of $F$ if $K$ is a field with the operations of $F$.

## Theorem

*Let $(F, +, .)$ be a field and $K \subseteq F$.*

$$K \text{ is a subfield of } F \Leftrightarrow \begin{array}{l} (i)\ K^* \neq \emptyset \\ (ii)\ \forall a, b \in K,\ \ a - b \in K \\ (iii)\ \forall a, b \in K,\ \ ab \in K \\ (iv)\ \ x \in K^* \Rightarrow x^{-1} \in K^* \end{array}$$

**Examples:**

**1.** $\mathbb{Q}$ is a subfield of $\mathbb{R}$, $\mathbb{R}$ is a subfield of $\mathbb{C}$.

**2.** $\mathbb{Z}[i]$ is not a subfield of $\mathbb{C}$.

**3.** $\mathbb{Q}[i]$ is a subfield of $\mathbb{C}$.