Plan

- Review of Last Lecture
- Section 18. Rings and Fields (continued)
- Section 19. Integral Domains
- About Quiz on Dec 1.

Definition 18.1. A ring $(R, +, \cdot)$ is a set R with two binary operations addition $+$ and multiplication $\cdot$ such that the following axioms are satisfied:

(1). $(R, +)$ is an abelian group.
(2). Multiplication $\cdot$ is associative.
(3). For all $a, b, c \in R$, the left distributive law and the right distributive las hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Example. The familiar number systems $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are rings.

For every positive integer n, $(\mathbb{Z}_n, +, \cdot)$, where $+$ is the modulo n addition and $\cdot$ is the modulo n multiplication.

$(C[0,7], +, \cdot)$ is a ring, where $C[0,7]$ is the space of all continuous functions on interval $[0,7]$.
In general for any interval I, the space of continuous functions on I is a ring under the function addition $+$ and function multiplication $\cdot$.

Definition. A ring $(R, +, \cdot)$ is called a **commutative ring** if the multiplication $\cdot$ is commutative, that is,

$$a \cdot b = b \cdot a \quad \text{for all} \quad a, b \in R.$$

$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $C[0, 7]$, $(\mathbb{Z}_n, +, \cdot)$ are all commutative rings.

Example. Let $n \geq 2$ and $M_n(\mathbb{R})$ be the set of all $n \times n$ matrices with real number entries, $(M_n(\mathbb{R}), +, \cdot)$ is a ring. This ring is **not** a commutative ring, We will often write a ring $(R, +, \cdot)$ simply as R, with the understanding that it has $+$ and $\cdot$.

And we write the identity element for $+$ as 0, the additive inverse of $a \in R$ as $-a$.

Theorem 18.8. If R is a ring with additive identity 0, then for any $a, b \in R$, we have

(1) $0a = a0 = 0$.
(2) $a(-b) = (-a)b = -(ab)$.
(3) $(-a)(-b) = ab$.

Definition 18.9. For rings R and R', a map $\phi : R \to R'$ is a (ring) **homomorphism** if the following two conditions are satisfied for all $a, b \in R$:

(1) $\phi(a + b) = \phi(a) + \phi(b)$.

(2) $\phi(ab) = \phi(a)\phi(b)$.

Example. $\phi : \mathbb{R} \to M_2(\mathbb{R})$ given by

$$\phi(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

is a ring homomorphism.

Example. $\phi : \mathbb{C} \to M_2(\mathbb{R})$ given by

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

is a ring homomorphism.

Definition 18.12. An **isomorphism** $\phi : R \to R'$ from a ring R to a ring R' is a homomorphism that is one-to-one and onto. The rings R and R' are then said to be isomorphic.

Definition 18.14. A ring with a multiplicative identity element is called a **ring with unity**. The multiplicative identity is usually denoted by 1 which is called "**unity**".

Examples. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $C[0, 7]$, $(\mathbb{Z}_n, +, \cdot)$, and $M_n(\mathbb{R})$ are all rings with unity.

Example. $(2\mathbb{Z}, +, \cdot)$ is a commutative ring, it has no unity. So it is NOT a ring with unity.

Definition 18.16. Let R be a ring with unity $1 \neq 0$. An element $u \in R$ is called a **unit** it has a multiplicative inverse, that is, there exists $u' \in R$ such that

$$uu' = u'u = 1.$$

If every non-zero element in R is a unit, then R is called a **division ring.**

Definition 18.16 (continued) A commutative division ring is called a **field**.

Example. $\mathbb{R}$ is a field, because

(1) $\mathbb{R}$ has unity 1, $1 \neq 0$.
(2) $\mathbb{R}$ is a commutative ring.
(3) Every $a \in \mathbb{R}$, $a \neq 0$, has the multiplicative inverse $a^{-1} \in \mathbb{R}$.

Example. Similarly, $\mathbb{Q}$ and $\mathbb{C}$ are fields.

Example. $\mathbb{Z}$ is NOT a field, because only two elements $1, -1$ are units. Other elements are not units.

Integral domains are an important class of commutative rings.

Before introducing the concept, we look at some properties of rings we give earlier.

Let R be any of the commutative rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, it is well-known that for $a, b \in R$, $a \neq 0, b \neq 0$, then $ab \neq 0$.

This property doesn't hold for other rings.

Example. In $\mathbb{Z}_{10}$, $4 \neq 0, 5 \neq 0$, but $4 \cdot 5 = 0$. 4 and 5 are called 0 divisors.

Definition. Let R be a commutative ring, a is called a 0 **divisor** if
(1) $a \neq 0$,
(2) there exists $b \in R$, $b \neq 0$ such that $ab = 0$.

Example. In $\mathbb{Z}_{10}$, $2, 4, 6, 8, 5$ are 0-divisors. The other five elements in $\mathbb{Z}_{10}$ are not 0-divisors.

Example. In ring $C[0,7]$, we let $f(x), g(x) \in C[0,7]$ be the functions

$$f(x) = \begin{cases} x-3 & \text{for } 0 \le x \le 3 \\ 0 & \text{for } 3 \le x \le 7 \end{cases}$$

$$g(x) = \begin{cases} 0 & \text{for } 0 \le x \le 3 \\ x-3 & \text{for } 3 \le x \le 7 \end{cases}$$

$f(x) \neq 0$, $g(x) \neq 0$, but $f(x)g(x) = 0$ So $f(x)$ and $g(x)$ are 0-divisors.

Definition 19.6. A ring D is called an **integral domain** if it satisfied the following three conditions
(1) D is a commutative ring.
(2) D has a unity 1, $1 \neq 0$.
(3) D has no 0-divisors. An integral domain D is a commutative ring

Example. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are integral domains.

Example. $\mathbb{Z}_{10}$ and $C[0, 7]$ are NOT integrals domains, because they have 0-divisors.

Theorem 19.9. Every field is an integral domain.

Theorem 19.3. In the ring $\mathbb{Z}_n$, the 0 divisors are precisely those non-zero elements that are not relatively prime to n.

Examples. In $\mathbb{Z}_{12}$, $2, 3, 4, 6, 8, 9, 10$ are 0 divisors. The other five elements are not 0 divisors.

Corollary 19.3. If p is a prime, then $\mathbb{Z}_p$ has no 0 divisors.

The end