



# Lecture 9

## Introduction of Rings (環) & Fields (体)

## 9.1 Rings (環) & Fields (体)

# 9.1 Rings (環) & Fields (体)

## Definition 9.1 (1)

A **ring (環)** is an **ordered triple**  $(R, +, \cdot)$  such that  $R$  is a **nonempty set** and  $+$  and  $\cdot$  are **two binary operations** (which we call addition and multiplication) **on**  $R$  (i.e.  $R \times R \rightarrow R$ ) **satisfying the following axioms.**

Closure Property

(R1)  $(a + b) + c = a + (b + c)$  for all  $a, b, c \in R$ . (Addition is associative.)

(R2) There exists an element  $0$  in  $R$  such that  $a + 0 = a$  for all  $a \in R$ . (Identity element exists for Addition.)

(R3) For all  $a \in R$ , there exists an element  $-a \in R$  such that  $a + (-a) = 0$ . (Inverse element exists for Addition.)

(R4)  $a + b = b + a$  for all  $a, b \in R$ . (Addition is commutative/abelian.)

(R5)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in R$ . (Multiplication is associative.)

(R6)  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  for all  $a, b, c \in R$ . (Left Distributive Law)

(R7)  $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$  for all  $a, b, c \in R$ . (Right Distributive Law)

## 9.1 Rings (環) & Fields (体)

### Definition 9.1 (2)

A **ring (環)** is an **ordered triple**  $(R, +, \cdot)$  such that  $R$  is a **nonempty set** and  $+$  and  $\cdot$  are **two binary operations** (which we call addition and multiplication) **on**  $R$  (i.e.  $R \times R \rightarrow R$ ) **satisfying the following axioms.**

Closure Property

(New R1)  $(R, +)$  is an **abelian group**.

(New R2)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in R$ . (Multiplication is associative.)

(New R3)  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  for all  $a, b, c \in R$ . (Left Distributive Law)

(New R4)  $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$  for all  $a, b, c \in R$ . (Right Distributive Law)

## 9.1 Rings (環) & Fields (体)

During the development of the theory of rings, we will use the following conventions.

1. Multiplication is assumed to be performed before addition.
2. We write  $ab$  for  $a \cdot b$ .
3. We write  $a - b$  for  $a + (-b)$ .
4. We refer to a ring  $(R, +, \cdot)$  as a ring  $R$ .

## 9.1 Rings (環) & Fields (体)

### Example 9.1

We are well aware that **axioms for a ring hold in any subset of the complex numbers that is a group under addition and that is closed under multiplication.** It can be shown that  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ , and  $(\mathbb{C}, +, \cdot)$  are rings.

Notice: The ring  $(\mathbb{Z}, +, \cdot)$  is called the **ring of integers**.

**This ring plays an important role in the study of ring theory.** One of the basic problems in ring theory is to determine rings, which satisfy the same type of properties as the ring of integers.

## 9.1 Rings (環) & Fields (体)

### Example 9.2

Recall that in group theory,  $n\mathbb{Z}$  is the cyclic subgroup of  $\mathbb{Z}$  under addition consisting of all integer multiples of the integer  $n$ .

For  $r, s \in \mathbb{Z}$ , we have  $nr, ns \in n\mathbb{Z}$ , since  $(nr)(ns) = n(nrs)$ , we see that  $n\mathbb{Z}$  is closed under multiplication.

The associative and distributive laws which hold in  $\mathbb{Z}$  then assure us that  $(n\mathbb{Z}, +, \cdot)$  is a ring.

## 9.1 Rings (環) & Fields (体)

### Theorem 9.1

Let  $R$  be a ring and  $a, b, c \in R$ . Then

(i)  $a0 = 0a = 0$ ,

(ii)  $a(-b) = (-a)b = -(ab)$ ,

(iii)  $(-a)(-b) = ab$ ,

(iv)  $a(b - c) = ab - ac$  and  $(b - c)a = ba - ca$ .

### Proof



## 9.1 Rings (環) & Fields (体)

### Definition 9.2

Let  $R$  be a ring. An element  $e \in R$  is called an **identity element** if  $ea = a = ae$  for all  $a \in R$ .

### Definition 9.3

A ring  $R$  is called a **ring with identity** (単位元持つ環) if it has an identity element.

**Example** The ring  $(\mathbb{Z}, +, \cdot)$  of integers is a ring with identity. The integer 1 is the identity element of  $\mathbb{Z}$ .

### Definition 9.4

A ring  $R$  for which  $ab = ba$  for all  $a, b \in R$  is called a **commutative ring** (可換環).

### Definition 9.5

A nonzero element  $a$  in a ring  $R$  is called a **zero divisor** (零因子) if there is a nonzero element  $b$  in  $R$  such that  $ab = 0$ .

## 9.1 Rings (環) & Fields (体)

### Definition 9.6

A commutative ring  $R$  with identity is called an **integral domain** (整域) if, for every  $a, b \in R$  such that  $ab = 0$ , either  $a = 0$  or  $b = 0$ . Namely,  $R$  has no **zero divisor**.

### Definition 9.7

Let  $R$  be a ring with identity. An element  $a \in R$  and  $a \neq 0$  is called a **unit** (単元) (or an **invertible element** (可逆元)) if there exists  $b = a^{-1} \in R$  such that  $aa^{-1} = e = a^{-1}a$ .

### Definition 9.8

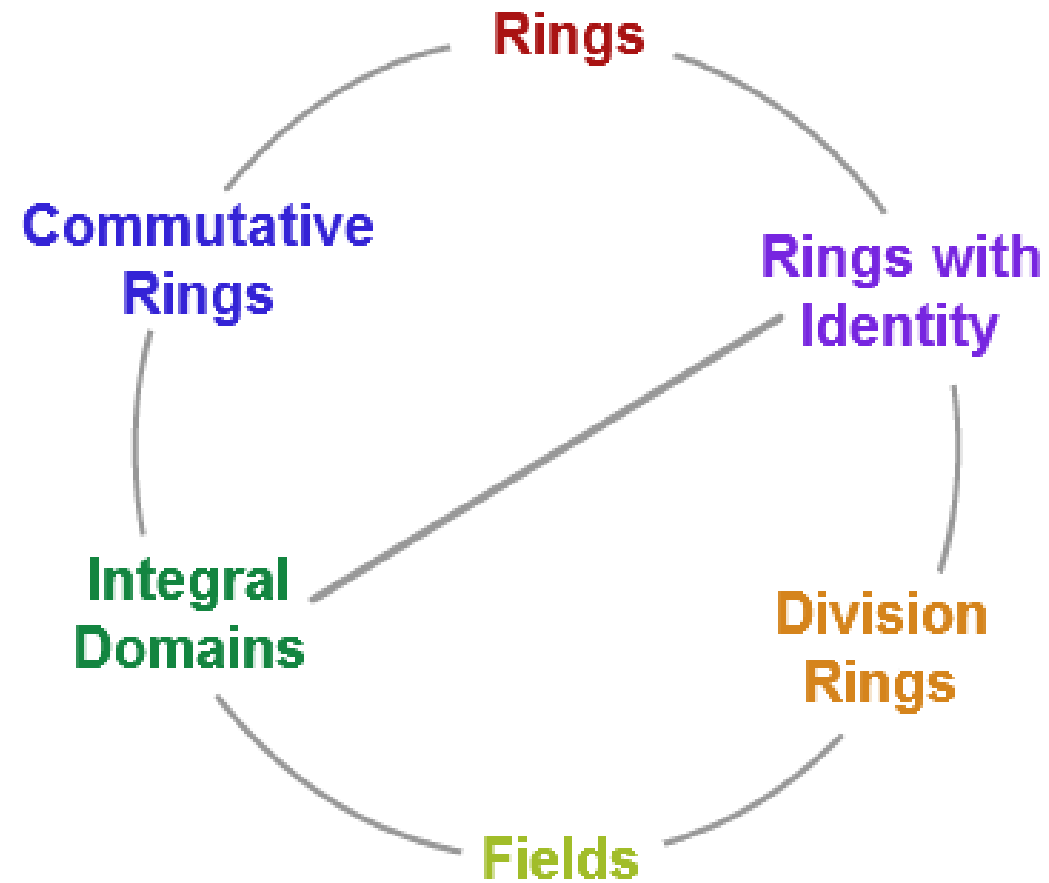
A ring  $R$  with identity is called a **division ring** (可除環) (skew-field (斜体)) if every nonzero element of  $R$  is a **unit**.

### Definition 9.9

A commutative division ring  $R$  is called a **field** (体).

## 9.1 Rings (環) & Fields (体)

The relationship among rings, integral domains, division rings, and fields is shown in the following Figure



## 9.1 Rings (環) & Fields (体)

### Example 9.3

Because multiplication of numbers is commutative, it follows that  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ , and  $(\mathbb{C}, +, \cdot)$  are commutative rings.

### Example 9.4

Consider  $2\mathbb{Z}$ , the ring of even integers. In  $2\mathbb{Z}$ , there does not exist any element  $e$  such that  $ex = x = xe$  for all  $x \in 2\mathbb{Z}$ . Hence,  $2\mathbb{Z}$ , is a ring without identity.

## 9.1 Rings (環) & Fields (体)

### **Example 9.5**

The ring of even integers  $2\mathbb{Z}$  is a commutative ring, without identity, and without zero divisors.  
Thus,  $2\mathbb{Z}$  is not an integral domain.

### **Example 9.6**

The ring of integers  $\mathbb{Z}$  is an **integral domain**.

## 9.1 Rings (環) & Fields (体)

**Example 9.6** Let  $R$  denote the set of all functions  $f: \mathbb{R} \rightarrow \mathbb{R}$ . Define  $+, \cdot$  on  $R$  by for all  $f, g \in R$  and for all  $a \in R$ ,

$$(f + g)(a) = f(a) + g(a),$$

$$(f \cdot g)(a) = f(a)g(a).$$

- From the definition of  $+$  and  $\cdot$ , it follows that  $+$  and  $\cdot$  are binary operations on  $R$ . Let  $f, g, h \in R$ . Then for all  $a \in R$ , we have by using the associativity of  $\mathbb{R}$  that

$$\begin{aligned} ((f + g) + h)(a) &= (f + g)(a) + h(a) \\ &= (f(a) + g(a)) + h(a) \\ &= f(a) + (g(a) + h(a)) \\ &= f(a) + (g + h)(a) \\ &= (f + (g + h))(a) \end{aligned}$$

Thus,  $(f + g) + h = f + (g + h)$ . This shows that  $+$  is associative.

In a similar way, we can show that the other properties of a ring hold for  $R$  by using the fact that they hold for  $\mathbb{R}$ . **Thus,  $(R, +, \cdot)$  is a ring.**

- We note that the function  $i_0: \mathbb{R} \rightarrow \mathbb{R}$ , where  $i_0(a) = 0$  for all  $a \in R$ , is the additive identity of  $R$  and the element  $i_1 \in R$ , where  $i_1(a) = 1$  for all  $a \in R$ , is the identity of  $R$ . Also, for all  $f, g \in R$  and for all  $a \in R$ ,  $(f \cdot g)(a) = f(a)g(a) = g(a)f(a) = (g \cdot f)(a)$ .

Thus, for all  $f, g \in R$ ,  $f \cdot g = g \cdot f$ . **Consequently,  $(R, +, \cdot)$  is a commutative ring with identity.**

## 9.1 Rings (環) & Fields (体)

### Example 9.7

Consider  $\mathbb{Z}$ , the ring of integers. Let  $a \in \mathbb{Z}$  be such that  $a \neq 0$ ,  $a \neq 1$ , and  $a \neq -1$ .

Now  $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$ . That is, the multiplicative inverse of  $a$  is  $\frac{1}{a}$ .

However,  $\frac{1}{a} \notin \mathbb{Z}$ . (For example, the multiplicative inverse of 2 is  $\frac{1}{2} \notin \mathbb{Z}$ .)

It follows that  $\mathbb{Z}$  is not a field. Note that in  $\mathbb{Z}$ , the only invertible elements are 1 and  $-1$ .

## 9.1 Rings (環) & Fields (体)

### Definition 9.10

A ring  $R$  is called a **finite ring** if  $R$  has only a **finite number of elements**; otherwise  $R$  is called an **infinite ring**.



## 9.1 Rings (環) & Fields (体)

### \*Theorem 9.2

A finite commutative ring  $R$  with more than one element and without zero divisors is a field.

Proof: Page 136 of Ref. Textbook

### \*Corollary 9.1

Every finite integral domain is a field.

### \*Corollary 9.2

Let  $n$  be a positive integer. Then  $\mathbb{Z}_n$  is a field if and only if  $n$  is prime.

Notice: \* mark is optional material. It will not be included in the final examination.

## 9.1 Rings (環) & Fields (体)

### Definition 9.11

Let  $(R, +, \cdot)$  be a ring. Let  $S$  be a subset of  $R$ . Then  $(S, +, \cdot)$  is called a **subring** of  $(R, +, \cdot)$  if

- (i)  $(S, +)$  is a **subgroup** of  $(R, +)$  and
- (ii) for all  $x, y \in S, x \cdot y \in S$ .

**Remark** When  $S$  and  $R$  are **fields**,  $S$  is called a **subfield** of  $R$ .

### Theorem 9.3

Let  $S$  be a ring. A **nonempty subset**  $S$  of  $R$  is a **subring** of  $R$  if and only if  $x - y \in S$  and  $xy \in S$  for all  $x, y \in S$ .

#### Proof

- First suppose that  $S$  is a subring of  $R$ . Then  $S$  is a ring. Hence, for all  $x, y \in R, x - y, xy \in S$ .
- Conversely, suppose  $x - y \in S$  and  $xy \in S$  for all  $x, y \in S$ . Because  $x - y \in S$  for all  $x, y \in S$ ,  $(S, +)$  is a subgroup of  $(R, +)$  by Theorem 4.2. By the hypothesis,  $xy \in S$  for all  $x, y \in S$ . Hence,  $S$  is a subring of  $R$ .

## 9.1 Rings (環) & Fields (体)

### Example 9.8

Let  $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$ , where  $m$  is an integer greater than 1. That is,  $m\mathbb{Z}$  is the set of integer multiples of  $m$ .

We claim that  $m\mathbb{Z}$  is a subring of  $\mathbb{Z}$ .

For if  $ma, mb \in m\mathbb{Z}$ , then

$$ma - mb = m(a - b) \in m\mathbb{Z}$$

and so  $m\mathbb{Z}$  is closed under subtraction. Similarly,

$$(ma)(mb) = m(mab) \in m\mathbb{Z}$$

and so  $m\mathbb{Z}$  is closed under multiplication.

## 9.1 Rings (環) & Fields (体)

### \*Theorem 9.4

Let  $F$  be a field. A nonempty subset  $U$  of  $F$  is a subfield of  $F$  if and only if

- (i)  $U$  contains more than one element,
- (ii)  $x - y, xy \in U$  for all  $x, y \in U$ , and
- (iii)  $x^{-1} \in U$  for all  $x \in U, x \neq 0$ .

## **9.2 Ideals (イデアル) & Quotient Rings (剰余環, 商環)**

## 9.2 Ideals (イデアル) & Quotient Rings (剰余環)

In this section, we introduce the notions of **ideals** and **quotient rings**. These concepts are analogous to **normal subgroups** and **quotient groups**.

### Definition 9.12

Let  $R$  be a ring. Let  $I$  be a **nonempty subset** of  $R$ .

- (i)  $I$  is called a **left ideal** of  $R$  if for all  $a, b \in I$  and for all  $r \in R$ ,  $a - b \in I$ ,  $ra \in I$ .
- (ii)  $I$  is called a **right ideal** of  $R$  if for all  $a, b \in I$  and for all  $r \in R$ ,  $a - b \in I$ ,  $ar \in I$ .
- (iii)  $I$  is called a **(two-sided) ideal** of  $R$  if  $I$  is **both a left and a right ideal** of  $R$ .

From the definition of a left (right) ideal, it follows that if  $I$  is a left (right) ideal of  $R$ , then  $I$  is a subring of  $R$ . Also, if  $R$  is a commutative ring, then every left ideal is also a right ideal and every right ideal is a left ideal.

Thus, for commutative rings every left or right ideal is an ideal.

## 9.2 Ideals (イデアル) & Quotient Rings (剰余環)

### Example 9.9

Let  $R$  be a ring. The subsets  $\{0\}$  and  $R$  of  $R$  are (left, right) ideals. These ideals are called **trivial ideals** (自明なイデアル). All other (left, right) ideals are called **nontrivial**.

An ideal  $I$  of a ring  $R$  is called a **proper ideal** (真のイデアル) if  $I \neq R$ .

### Example 9.10

We see that  $n\mathbb{Z}$  is an ideal in the ring  $\mathbb{Z}$  since we know it is a subring, and  $s(nm) = (nm)s = n(ms) \in n\mathbb{Z}$  for all  $s \in \mathbb{Z}$ .

## 9.2 Ideals (イデアル) & Quotient Rings (剰余環)

### Example 9.11

If  $a$  is any element in a commutative ring  $R$  with identity, then the set

$$\langle a \rangle = \{ar : r \in R\}$$

is an **ideal** in  $R$ . Certainly,  $\langle a \rangle$  is nonempty since both  $0 = a0$  and  $a = a1$  are in  $\langle a \rangle$ . The sum of two elements  $r, r'$  in  $\langle a \rangle$  is again in  $\langle a \rangle$  since  $ar + ar' = a(r + r')$ . The inverse of  $ar$  is  $-ar = a(-r) \in \langle a \rangle$ . Finally, if we multiply an element  $ar \in \langle a \rangle$  by an arbitrary element  $s \in R$ , we have  $s(ar) = a(sr)$ . Therefore,  $\langle a \rangle$  satisfies the definition of an ideal.

If  $R$  is a commutative ring with identity, then an ideal of the form  $\langle a \rangle = \{ar : r \in R\}$  is called a **principal ideal** (主イデアル).

### Theorem 9.5

Every ideal in the ring of integers  $\mathbb{Z}$  is a **principal ideal**.



## 9.2 Ideals (イデアル) & Quotient Rings (剰余環)

**Example 9.12** Find all ideals of  $\mathbb{Z}$ .

**Solution:**

We know that the subrings of  $\mathbb{Z}$  are the subsets  $n\mathbb{Z}, n = 0, 1, 2, \dots$ .

Let us now show that these subrings are precisely the ideals of  $\mathbb{Z}$ .

If  $I$  is an ideal of  $\mathbb{Z}$ , then  $I$  is a subring of  $\mathbb{Z}$ , so  $I = n\mathbb{Z}$  for some nonnegative integer  $n$ .

Now, let  $I = n\mathbb{Z}$  ( $n$  is a nonnegative integer). Then  $I$  is a subring. If  $r \in \mathbb{Z}$ , then  $rI = r(n\mathbb{Z}) = n(r\mathbb{Z}) \subseteq n\mathbb{Z} = I$ . Similarly,  $Ir \subseteq I$ . Hence,  $I$  is an ideal of  $\mathbb{Z}$ .

## 9.2 Ideals (イデアル) & Quotient Rings (剰余環)

### Definition 9.5

If  $R$  is a ring and  $I$  is an ideal of  $R$ , then the ring  $(R/I, +, \cdot)$  is called the **quotient ring** of  $R$  by  $I$ .

### Remark

The quotient ring  $R/I$  can also be realized by observing the  $(I, +)$  is a normal subgroup of  $(R, +)$  because the latter group is commutative.

Hence, if  $R/I$  denotes the set of all cosets  $x + I = \{x + a \mid a \in I\}$  for all  $x \in R$ , then  $(R/I, +)$  is a commutative group, where

$$(x + I) + (y + I) = (x + y) + I$$

for all  $x + I, y + I \in R/I$ . Now define multiplication on  $R/I$  by  $(x + I) \cdot (y + I) = xy + I$  for all  $x + I, y + I \in R/I$ . Then  $(R/I, +, \cdot)$  forms a **ring**.

# Review for Lecture 9

- Rings
- Integral domain (整域)
- Fields
- Subring & Subfield
- Ideal
- Quotient Rings

# Assignment

Please Check <https://github.com/uoaworks/Applied-Algebra>

## References

- [1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018
- [2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007
- [3] (おすすめ) 松本 眞, 代数系への入門, <http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/daisu-nyumon2014.pdf>
- [4] Wikipedia
- [5] Materials from internet.