4. Ring Theory

4.1 Definitions & Examples

The objects that we have studied so far, namely groups, were sets on which an operation that satisfied certain rules was defined. However, many of the sets that we deal with have two natural operations. For example, we can both add and multiply integers or real numbers. A ring likewise has two operations, and these operations must satisfy some of the rules satisfied by addition & multiplication of numbers. However, this does not mean that all rings behave exactly like the integers or real numbers - while $\mathbb{Z}$ & $\mathbb{R}$ are both examples of rings, a wide range of other examples fall into the category of rings. Thus, while $\mathbb{Z}$ & $\mathbb{R}$ give us some intuition & insight into

the structure of general rings, we must be aware that there is much more to ring theory than just these particular examples. The same was true in our study of groups — while abelian or cyclic groups might be the "easiest" examples that provide us with concrete examples & some motivation, many groups are nonabelian, and can be extremely complicated to understand, e.g., consider the symmetric group S_n, the alternating group A_n, or the "monster" m.

Definition

A nonempty set R is a ring if there are two operations on R, that we denote by $+$ and $\cdot$, such that the following requirements are satisfied:

a. R is an abelian group under $+$. Specifically,

i. if $a, b \in R$ then $a+b \in R$. Closure under $+$

ii. $a+b = b+a \quad \forall a, b \in R$ Commutativity of $+$

Associativity → iii. $(a+b)+c = a+(b+c) \quad \forall a, b, c \in R$

Existence of an identity → iv. $\exists$ element $0 \in R$ s.t. $a+0 = a \quad \forall a \in R$

Existence of inverses → v. $\forall a \in R$, there exists an element $-a \in R$ such that $a+(-a) = 0$.

b. $\cdot$ satisfies:

Closure under $\cdot$ → i. if $a, b \in R$ then $a \cdot b \in R$

Associativity → ii. $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in R$

Note: Multiplication need not be commutative!

c. $+$ and $\cdot$ are interrelated by the following

distributive laws:

i. $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$

ii. $(b+c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R.$

Remarks

- We do not require that R is a group under $\cdot$.

There are many reasons for this. For example, one of the prime examples of a ring is the set of integers $\mathbb{Z}$ under the usual operations of addition & multiplication. Note that $\mathbb{Z}$ is not a group under multiplication, since 0 has no multiplicative inverse. On the other hand, even if we consider $\mathbb{Z} \setminus \{0\} = \{n \in \mathbb{Z} : n \neq 0\}$ under multiplication, it is still not a group, since no integers other than 1 & -1 have multiplicative inverses in $\mathbb{Z}$.

Notation

Although the operations $+$ and $\cdot$ on R could conceivably have very little to do with "addition" or "multiplication" in the ordinary sense, we will refer to $+$ as addition and to $\cdot$ as multiplication.

Further, for simplicity of notation, we usually write a product with respect to $\cdot$ as

$$ab \quad \text{instead of} \quad a \cdot b$$

Note: Addition is commutative by definition in any ring! But multiplication need not be.

Commutative Rings

Note that we do not require that the operation of multiplication in a ring be commutative. We do require that addition be commutative, but multiplication need not be.

If a ring R satisfies

$$ab = ba \quad \forall a, b \in R$$

then we say that it is a commutative ring

Rings with identity

Further, we do not require that there be an identity element for multiplication. If there is an identity for multiplication, then we denote it by the symbol 1. That is, an element $1 \in R$ is an identity for multiplication, or a multiplicative identity, if

A multiplicative identity must be two-sided: Both $1a$ and $a1$ must equal a for every $a \in R$

$$1a = a1 \quad \forall a \in R.$$

If such a multiplicative identity element 1 exists and if $1 \neq 0$, then we say that R is a ring with identity or a ring with unit.

Remark

Many authors require that a ring contain a multiplicative identity. That is, according to some authors, R can't be called a ring unless there exists a multiplicative identity $1 \neq 0$ in R. We will not require this of our rings.

Examples/Exercises

a. The set $\mathbb{Z}$ of integers, the set $\mathbb{Q}$ of rational numbers, & the set $\mathbb{R}$ of real numbers are commutative rings with identity under the usual operations of addition & multiplication. Although

we will not make too much use of complex numbers initially, it is likewise true that the set $\mathbb{C}$ of complex numbers is a commutative ring with identity under the ordinary definitions of addition & multiplication of complex numbers.

b. Given $n > 1$, let

$$M_n = \{A : A \text{ is an } n \times n \text{ matrix with real entries}\}$$

Then M_n is a noncommutative ring with identity. The complex version of M_n, where we allow matrices to have complex entries, is likewise a noncommutative ring with unit.

c. Let Example: Abusing notation, $f(x) = \sin x$ and $g(x) = e^x$ are elements of $C(\mathbb{R})$.

$$C(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} : f \text{ is continuous}\},$$

Let $C(\mathbb{R})$ be the set of all continuous functions that map real numbers to real numbers. As usual, define the sum of two functions f, g to be the function $f+g$ whose rule is

$$(f+g)(x) = f(x) + g(x), \text{ for } x \in \mathbb{R},$$

and the product fg is the function whose rule is

$$(fg)(x) = f(x)\,g(x), \text{ for } x \in \mathbb{R}.$$

Then $C(\mathbb{R})$ is a commutative ring with identity. The multiplicative identity is a function. We denote this function by the symbol 1, but must note that this symbol is now playing two roles at once: the function 1 is the mapping whose rule is:

$$1(x) = 1 \quad \forall x \in \mathbb{R}$$

This 1 denotes a function

This 1 denotes the number 1

Technically, we should really use two different symbols to denote two different objects. For example, it would be more precise to define a function $\mathbb{1} : \mathbb{R} \to \mathbb{R}$ whose rule is

$$\mathbb{1}(x) = 1 \quad \forall x \in \mathbb{R}$$

($\mathbb{1}$: the function whose rule is $\mathbb{1}(x) = 1$; 1: the number 1)

$\mathbb{1}$ is an attempt to write a boldface 1 on the board

the function $\mathbb{1}$ whose rule is $\mathbb{1}(x) = 1 \ \forall x \in \mathbb{R}$.

Then the function $\mathbb{1}$ is the multiplicative identity of $C(\mathbb{R})$. The number 1 does not belong to $C(\mathbb{R})$. However, we typically abuse notation and write the symbol "1" to mean either the function $\mathbb{1}$ or the number 1, letting the reader figure out which is meant from the context in which they appear.

d. Let $C_0(\mathbb{R})$ denote the subset of $C(\mathbb{R})$ consisting of those functions that "vanish at ∞":

$$C_0(\mathbb{R}) = \{f \in C(\mathbb{R}) : \lim_{x\to\infty} f(x) = 0 = \lim_{x\to-\infty} f(x)\}.$$

For example, $\sin x \notin C_0(\mathbb{R})$ [note an abuse of notation – we should really say that the function f whose rule is $f(x) = \sin x$ $\forall x \in \mathbb{R}$ does not belong to $C_0(\mathbb{R})$, i.e., $f \notin C_0(\mathbb{R})$. When we wrote $f(x)$ we mean the value of f at x, which is a number, not a function.]

A similar abuse of notation here – we really mean "the function f whose rule is $f(x) = e^x$ belongs to $C_0(\mathbb{R})$."

→ Likewise, $e^x \notin C_0(\mathbb{R})$, even though $\lim_{x\to-\infty} e^x = 0$. Show that the following functions do belong to $C_0(\mathbb{R})$:

- $e^{-(x^2)} \in C_0(\mathbb{R})$
- $e^{-|x|} \in C_0(\mathbb{R})$

- if we define $f(x) = \begin{cases} \frac{\sin x}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases}$

then $f \in C_0(\mathbb{R})$.

Now show that $C_0(\mathbb{R})$ is a commutative ring without identity.

NOTE: Do not just say that there is no multiplicative identity because the function $\mathbb{1}(x) = 1$ does not belong to $C_0(\mathbb{R})$. How do you know that some other function can't be a multiplicative identity for $C_0(\mathbb{R})$? You should proceed by contradiction: Suppose that there did exist a function $g \in C_0(\mathbb{R})$ that satisfied

$$gf = f \quad \text{for all } f \in C_0(\mathbb{R}). \quad (*)$$

Show that this leads to a contradiction. Be sure that your argument is valid; in particular, make

→ Specifically, show that the assumption (*) implies that $g(x) = x$ for every x.

sure that you don't divide by zero.

Integral Domains

Because a ring need not contain multiplicative inverses, for a general ring we need not have cancellation laws for multiplication. In particular, $ab = 0$ will not in general imply that either $a = 0$ or $b = 0$.

An integral domain will be a commutative ring where ab=0 does imply that either a=0 or b=0

Example

Consider $\mathbb{Z}_6$ under the operations of addition and multiplication mod 6. Show that this is a commutative ring with identity. However, $\mathbb{Z}_6$ is not an integral domain, because there are nonzero elements whose product is zero,

$$2 \cdot 3 = 0 \quad (\text{in } \mathbb{Z}_6).$$

Another example in the ring $M_2 = \{\text{all } 2\times 2 \text{ matrices}\}$.
If $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, then $A^2 = AA = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$

On the other hand, even though a ring does not have multiplicative inverses, it can still be an integral domain!

Example

The set $\mathbb{Z}$ of integers is a commutative ring with identity. The only elements that have multiplicative inverses are 1 & -1. Even so, there are no nonzero numbers $a, b \in \mathbb{Z}$ whose product is zero. (Why?) Therefore $\mathbb{Z}$ is an integral domain.

Definition

An element $a \neq 0$ in a ring R is a zero divisor if there exists a $b \neq 0$ in R such that $ab = 0$.

Definition

An integral domain is a commutative ring that has no zero divisors. That is, a commutative ring is an integral domain if:

ab = 0 IMPLIES a = 0 or b = 0.

Example: $\mathbb{Z}$ is an integral domain.

Cancellation in Integral Domains

Suppose R is an integral domain, and

$$ab = ac \quad \text{where} \quad a \neq 0.$$

Then $ab - ac = 0$, so by the distributive law,

$$a(b-c) = 0.$$

But R is an integral domain & $a \neq 0$, so

R implies that

$$b - c = 0 \quad \text{or} \quad b = c.$$

Thus, we can cancel in an integral domain, as long as $a \neq 0$.

Contrapositive form

The definition of an integral domain is that it is a commutative ring that satisfies:

If ab = 0, then either a = 0 or b = 0 (or both).

We can write this condition in an equivalent contrapositive form:

If a and b are BOTH nonzero, then ab is nonzero.

In either formulation, in order to be called an integral domain, the condition must hold for ALL a and b in the ring, not just some a and b.

Exercise

Show that the rings $C(\mathbb{R})$ and $C_0(\mathbb{R})$ are not integral domains, i.e., there exist functions $f \neq 0$, $g \neq 0$ such that $fg = 0$.

Note: The zero element of $C(\mathbb{R})$ or $C_0(\mathbb{R})$ is the zero function. We denote this function by 0, but must again emphasize that the symbol "0" is playing double-duty: On the one hand it denotes the function 0 whose rule is $0(x) = 0 \ \forall x \in \mathbb{R}$, but the second "0" in this rule denotes the number zero.

To say that $f \neq 0$ means that f is not the zero function. That means that $f(x)$ & $0(x)$ are not equal for all x, which means that $f(x) \neq 0$ for at least one x. It does not mean that $f(x) \neq 0$ for all x!

Exercise/Example

Recall the noncommutative ring M_n of all $n \times n$ matrices.

Show that $M_n(\mathbb{R})$ has zero divisors. In particular, show that there exists a nonzero matrix $A \in M_n(\mathbb{R})$ such that $A^2 = O$.

For $n = 2$ we can take $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

Note that O here again is playing a dual role - in the equation $A^2 = O$, it denotes the $n \times n$ zero matrix, all of whose entries are zero.

The zero element can never have a multiplicative inverse, since $0a = 0 \neq 1$ for every $a \in R$.

Division Rings

A ring that does have multiplicative inverses (except for the zero element) is called a division ring.

Definition

Let R be a ring with identity. Then R is a division ring if for each $a \neq 0$ in R there exists an element $a^{-1} \in R$ such that

$$aa^{-1} = 1 = a^{-1}a.$$

Examples: $\mathbb{Z}$ and $M_n(\mathbb{R})$ are not division rings, because there are nonzero elements that do not have multiplicative inverses.

Noncommutative division rings are quite complicated. The "simplest" example of a noncommutative division ring is the ring of quaternions. In some sense, the quaternions are a generalization of the complex numbers. In the complex numbers there are units 1 and i which satisfy $i^2 = -1$. In the quaternions, there are units

units $1, i, j, k$ which satisfy

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j.$$

However, unlike the complex numbers, multiplication of quaternions is <u>not commutative</u>. For details, see the discussion on pages 131-133 of Herstein's text.

We will mostly be interested in division rings that are commutative. These rings are called <u>fields</u>.

Field

A field is a commutative ring with identity such that every nonzero element has a multiplicative inverse.

Definition

A commutative ring R with identity is a <u>field</u> if for each $a \neq 0$ in R there exists $a^{-1} \in R$ such that

$$a a^{-1} = 1$$

(and therefore $a^{-1}a = 1$ since R is commutative).

Exercise

$\mathbb{Z}$ is not a field, but $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

Exercise

Show that if $n > 1$ is composite (meaning that n is not prime) then $\mathbb{Z}_n$ is not an integral domain, and show this implies that $\mathbb{Z}_n$ is not a field.

Show that if p is prime, then $\mathbb{Z}_p$ is a field.

Example: In $\mathbb{Z}_7$, $3 \cdot 5 = 1$ (in $\mathbb{Z}_7$).

A field like $\mathbb{Z}_p$ that has finitely many elements is called a <u>finite field</u>. Finite fields play important roles in many areas, including computer science. The fields $\mathbb{Z}_p$ are <u>not</u> the only finite fields.

<u>Exercise</u>

Let R be a commutative ring with identity. Prove that the following two statements are equivalent.

a. R is a field.

b. $R^* = R \setminus \{0\}$ is a group under multiplication.

In particular, if R is a field then:

R is a commutative group under addition,

and $R^* = R \setminus \{0\}$ is a commutative group under multiplication.

Notation

Many authors define a unit in a ring to be an element that has a multiplicative inverse. For these authors, $a \in R$ is a unit if there exists $a^{-1} \in R$ such that $aa^{-1} = 1 = a^{-1}a$. Herstein does not use this notation, and instead reserves the word "unit" for the multiplicative identity element 1. Be aware of this terminology when looking at other texts. For example, in many texts, the real number 2 would be a unit in the ring $\mathbb{R}$ because it has a multiplicative inverse $\frac{1}{2} \in \mathbb{R}$. However, 2 is not a unit in $\mathbb{Z}$ because it has no multiplicative inverse in $\mathbb{Z}$.

Exercise

Let M_n be the ring of all $n \times n$ matrices with real entries. Show that a matrix $A \in M_n$ is a unit (has a multiplicative inverse) if & only if it is an invertible matrix.

The subset $GL_n(\mathbb{R})$ consisting of all the invertible $n \times n$ matrices is called the general linear group of $n \times n$ matrices. Show that $GL_n(\mathbb{R})$ is a group under multiplication of matrices, but it is not closed under addition of matrices. Hence $GL_n(\mathbb{R})$ is not a ring.

Exercise

Find all of the ~~units~~ elements that have inverses in $\mathbb{Z}_{12}$.

Example: $4 \cdot 3 = 0$ in $\mathbb{Z}_{12}$ so 3 and 4 cannot have multiplicative inverses (why not?)

Exercise

Given $n > 1$, show that $m \in \mathbb{Z}_n$ is ~~a unit~~ has a multiplicative inverse if and only if $(m, n) = 1$.

Show that if p is prime then $\mathbb{Z}_p$ is a field.

Subrings

Definition

If R is a ring, then a subset $S \subseteq R$ is called a subring of R if it is itself a ring, using the same operations $a+b$ and ab that are defined for R.

Exercise

Let R be a ring, and suppose that $S \subseteq R$ is nonempty.

Prove that S is a subring if and only if the following conditions hold:

Closure Rules

a. if $a, b \in S$ then $a+b \in S$ and $a-b \in S$

b. if $a, b \in S$ then $ab \in S$.

For example, $\mathbb{Z}$ and $\mathbb{Q}$ are subrings of $\mathbb{R}$.

Exercise

Let S be a subset of $\mathbb{Q}$ containing all of the rational numbers $r = \frac{m}{n}$ such that when written in lowest terms we have that n is odd.

Example: $\frac{2}{5} \in S$ but $\frac{3}{4} \notin S$.

Show that S is a subring of $\mathbb{Q}$, and that S is an integral domain but $\underline{\text{not}}$ a field.

integral domain: So $ab = 0 \Rightarrow a = 0$ or $b = 0$

field: requires each nonzero element has a multiplicative inverse.

Exercise

Let $i = \sqrt{-1}$. The Gaussian integers are

$$\mathbb{Z}[i] = \{ m + ni : m, n \in \mathbb{Z} \}.$$

Show that $\mathbb{Z}[i]$ is a subring of the complex numbers $\mathbb{C}$.

Show that it is closed under addition, subtraction, and multiplication.

Exercise

Show that every subring of a field is an integral domain

Remark

In some noncommutative rings with identity, to prove the existence of a multiplicative inverse, you only have to prove the existence of a one-sided inverse.

For example, consider the ring M_n of all $n \times n$ matrices. It is proved in a course on linear algebra that if $A \in M_n$, then TFAE: (among many other equivalences!)

a. $\exists B \in M_n$ s.t. $AB = I$

One-sided inverses are two-sided inverses in M_n!

b. $\exists B \in M_n$ s.t. $BA = I$

Note $AB \neq BA$ in general!

c. $\exists B \in M_n$ s.t. $\boxed{AB = I = BA}$

This is the def. of an invertible matrix

However, this is not true for all rings!

Example: What happens for infinite sequences?

Let

$$X = \{ x = (x_1, x_2, x_3, \ldots) : x_k \in \mathbb{R} \ \forall k \in \mathbb{N} \}$$

That is, X contains all infinite sequences of real numbers.

Example: The sequence $x = (1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots)$ is one element of X

Now let

$$S = \{A : X \to X \ : \ A \text{ is a linear function}\}$$

The operations are addition and composition

Then S is a noncommutative ring with identity.

Consider $L \in S$ defined by

$$L(x_1, x_2, \ldots) = (x_2, x_3, \ldots) \qquad (\text{"left-shift"})$$

Example: $L(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots) = (\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots)$

and $R \in S$ defined by

$$R(x_1, x_2, \ldots) = (0, x_1, x_2, \ldots) \qquad (\text{"right-shift"})$$

Example: $R(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots) = (0, 1, \frac{1}{2}, \frac{1}{3}, \ldots)$

Show that

$$LR = I \quad (\text{identity})$$

Try $RL(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots)$

Thus L has a right-inverse, & R has a left-inverse.

However, show that

$$RL \neq I$$

Hence R & L do not have two-sided inverses.