1. **Rings and Fields**

1.1. **Introduction to Rings.** The operations of addition and multiplication in real numbers have direct parallels with operations which may be applied to pairs of integers, pairs of integers mod another positive integer, vectors in $\mathbb{R}^n$, matrices mapping $\mathbb{R}^n$ to $\mathbb{R}^m$, polynomials with real or integer coefficients, etc. The properties of the operations may be slightly different in each application, but there remains a subset of the properties of $+$ and $\cdot$, (addition and multiplication), which are common to all these examples. We will first define an abstract object called a *Ring* on which certain operations are possible which satisfy given properties. A ring will turn out to be a generalization of the real or complex numbers, and many other sets on which two operations are defined.

Definition: A *Ring* is a non-empty set, S on which two binary operations, from $S \times S$ to S,are defined, denoted by $+$ and $\cdot$, such that

$$\forall a, b \in S, \quad a + b \in S, \quad a \cdot b \in S, \tag{1}$$

and $\forall a, b \in S$ the following properties of $+$ and $\cdot$ hold:

(a) $a + b = b + a$. ($+$ is commutative.)
(b) $a + (b + c) = (a + b) + c$. ($+$ is associative.)
(c) $\exists z \in S, \quad a + z = z + a = a$. (There is an additive identity z.)
(d) $\forall a \in S, \ \exists b, \ a+b = b+a = z$. (There is an additive inverse denoted by $-a$.)
(e) $\forall a, b, c \in S, \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$. ($\cdot$ is associative.)
(f) $\forall a, b, c \in S, \ a \cdot (b + c) = a \cdot b + a \cdot c$. ($\cdot$ is distributive over $+$.)

Also, $\forall a, b, c \in S, \ (b + c) \cdot a = b \cdot a + c \cdot a$.

The ring, with the two operations, is denoted by $(S, +, \cdot)$. The conditions given in (1) are expressed by saying that S is *closed* under the operations $+$ and $\cdot$.

Definitions:

(a) If $\cdot$ is commutative $(S, +, \cdot)$ is a *commutative ring.*
(b) If $\forall a, b \in S$ we have $a \cdot b = z \quad \leftrightarrow \quad (a = z) \vee (b = z)$ then $(S, +, \cdot)$ has no divisors of zero. If $\exists a, b, \ \ a, b \neq z$ and $a \cdot b = z$ then a, b are called *divisors of zero.*
(c) If $\exists e \in S$ such that $\forall a \in S, \quad a \cdot e = e \cdot a = a$ then e is a *multiplicative identity*, or *unity.* If $\exists a, b \in S$ which satisfy $a \cdot b = e$, then a, b are called *units.*

1.2. **Examples of Rings.** Given a non-empty set S, with operations defined in it, we have an *Algebraic Structure.* We now discuss examples of algebraic structures which are Rings.

What is interesting is the properties of $+$, $\cdot$ which exist in arithmetic over $\mathbb{R}$ but are not required here. For example:

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\cdot$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

Figure 1. A ring of three elements

$+$	s	t	v	w	x	y
s	s	t	v	w	x	y
t	t	v	w	x	y	s
v	v	w	x	y	s	t
w	w	x	y	s	t	v
x	x	y	s	t	v	w
y	y	s	t	v	w	x

$\cdot$	s	t	v	w	x	y
s	s	s	s	s	s	s
t	s	t	v	w	x	y
v	s	v	x	s	v	x
w	s	w	s	w	s	w
x	s	x	v	s	x	v
y	s	y	x	w	v	t

Figure 2. A commutative ring of 6 elements

(i) It is not assumed that $\cdot$ is commutative.
(ii) There need not be a multiplicative identity, that is an element $e \in S$ such that $\forall a \in S \quad a \cdot e = a$.
(iii) There may not exist a multiplicative inverse for all $a \neq z$; that is there may be elements $a \neq z$ for which no b exists with $a \cdot b = e$, even if a multiplicative identity e exists.
(iv) No concept of ordering is necessary.

We now look at several examples of rings.

(1) $(\mathbb{R}, +, \cdot))$, where $\mathbb{R}$ is the set of real numbers. Similarly, $(\mathbb{Z}, +, \cdot)$, where $\mathbb{Z}$ is the set of integers; and $(\mathbb{Q}, +, \cdot)$, where Q is the set of rationals.
(2) A finite ring with $S = \{a, b, c\}$ whith $+, \cdot$ defined by the tables in 1. Here a plays the role of zero, b is the multiplicative identity, every element other than a has a multiplicative inverse, there are no divisors of zero, and $-b = c$. Multiplication is commutative.
(3) A finite ring with $S = \{s, t, v, w, x, y\}$. (See Figure 2.) Here s plays the role of zero, and t is the multiplicative identity. The only elements that have a multiplicative inverse are t, y, and there are divisors of zero. For example $w \cdot v = v \cdot x = q \cdot x = s$. Multiplication is commutatative.
(4) Let $(\mathbb{Z},\ +,\ \circ)$, where $\mathbb{Z}$ is the set of all integers, be an algebraic structure, with $+$ being the usual integer addition, and with $\circ$ being defined by

$$a \circ b \quad = \quad a + a \cdot b + b,$$

where $\cdot$ is the usual integer multipication. Is $(\mathbb{Z},\ +,\ \circ)$ a ring?

Since the addition operation is the usual operation on integers we can assume axioms (a), (b) hold. Axiom (c) holds with $z = 0$. Axiom (d) holds with -a as the additive inverse.

For axiom (e) note that

$$a \circ (b \circ c) = a \circ (b + b \cdot c + c)$$

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

This simplifies to $a + b + c + a \cdot b + a \cdot c + b \cdot c + a \cdot b \cdot c$. Also

$$(a \circ b) \circ c = (a + a \cdot b + b) \circ c$$

$$= a + a \cdot b + b + (a + a \cdot b + b) \circ c + c.$$

This also simplifies to $a + b + c + a \cdot b + a \cdot c + b \cdot c + a \cdot b \cdot c$. Hence axiom (e) holds. What about axiom (f)?

In each of the following examples, show that $(S, +, \cdot)$ is in fact a ring. Check to see if it is a commutative ring, whether there is a unity, and if there are any units.

(4) Arithmetic mod $m \in \mathbb{Z}$. The integers mod m are $\{0, 1, 2, \ldots, m-1\}$, and are denoted by $\mathbb{Z}_m$. If $a, b \in \mathbb{Z}_m$ then $a + b = c \ mod \ m$, and $a \cdot b = d \ mod \ m$.

Properties (a),(b),(e),(f), are properties carrying over from regular integer arithmetic. The additive identity is 0. The additive inverse of n where $0 < n \leq m - 1$ is $m - n$, since $(m - n) + n \equiv 0 \ \ mod \ \ m$. The additive inverse of 0 is 0.

Multiplication is commutative as in integer arithmetic.

There is a unity, namely 1. The question of the existence of units is a bit less obvious. If m is *prime*, then for any $a \in \mathbb{Z}_m$, $\exists b \in \mathbb{Z}_m$ with $a \cdot b = 1 \ \ mod \ \ m$. To see this, if a is an arbitrary integer in the range $1 \leq a \leq m-1$, and we form $a \cdot k$, for $k = 1, 2, \ldots, m-1$ we get $m-1$ integers mod m. If any two of these are equal, say $k \cdot a = j \cdot a$, with $j < k$, then $a \cdot (k - j) = 0$ mod m. This is impossible, since m has no factors, and so the $m-1$ values are distinct. Therefore there is one k such that $k \cdot a = 1$ mod m. Therefore *every* integer in the range $[1, m-1]$ is a unit. (Proof in class.)

If, however, m is composite then there exists divisors of zero, which are not units. But if a is relatively prime to m, then a is a unit. (Proof in class.)

For example, the addition and multiplication tables for $\mathbb{Z}_5$ are in Figure 3.

If we identify $\{s, t, v, w, x, y\}$ in Figure 2 with $\{0, 1, 2, 3, 4, 5\}$, then we get the table for $\mathbb{Z}_6$. Note that 5 has an inverse, namely itself, but 2,3,4 are divisors of zero.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

FIGURE 3. The ring of integers mod 5

In $\mathbb{Z}_8$ all odd integers are units and all even integers are divisors of zero.

(5) The set of $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.

Addition of these objects is just like working with ordered pairs (a, b). The $\sqrt{3}$ is just a symbol. Therefore requirements (a), (b), (c), (d) hold. But the multiplication properties need to be looked at.

$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$$

so that multiplication gives objects which are still in the set. The properties of multiplication are inherited from those of integer multiplication. Hence multiplication is commutative.

There is a unity, namely $1 + 0\sqrt{3}$. But are there units? Consider

$$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2}.$$

Then $a + b\sqrt{3}$ is a unit only if $\frac{a}{a^2-3b^2}$ and $\frac{b}{a^2-3b^2}$ are both integers. This leads to 6 units, namely $\pm 1, \pm 2 \pm 1\sqrt{3}$.

Are there any divisors of zero? That is, are there values of a, b, c, d such that $(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = 0$? If so, then it follows that

$$ac + 3bd = 0; \quad ad + bc = 0.$$

Therefore

$$acd = -3bd^2; \quad \therefore cad = -3bd^2; \quad \therefore c(-bc) = -3bd^2.$$

Therefore $c^2 = 3d^2$, provided $b \neq 0$. If $b = 0$ then it is easy to show that one of the multiplicands $= 0$. Now assume that c, d have no common factors. (We can cancel any common factor.) But $c^2 = 3d^2$ means that $3|c^2$, i.e. $3|c$, and so $3^2|c^2$. Therefore $3|d^2$ and $3|d$, which is not possible since we have removed all common factors of c, d. Therefore there are no divisors of zero.

(6) The set of $m \times n$ matrices $\mathbb{R}^n$ to $\mathbb{R}^m$.

Multiplication may not even be defined. It is necessary to have $n = m$ before we can multiply two such matrices.

The ring properties all hold for $m \times m$ matrices over the real numbers. The unity is the identity matrix. Units are the invertible matrices. Multiplication is not commutative.

(7) The set $\{a + bi \mid a, b \in \mathbb{R}, \;\; i^2 = -1\}$. These are the set of *complex numbers.*

The ring properties can be shown as in example (5). The unity is 1, and every non-zero complex number has an inverse. Multiplication is commutative.

(8) The set of 2×2 matrices given by

$$a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \; + \; b \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

where $a, b \in \mathbb{Z}_5$.

Write these objects as $aI + bJ$. Then note that $J^2 = -I$, that is J plays a role somewhat like i in example (4).

There is a unity, namely I. Since 5 is prime in $\mathbb{Z}_5$ every element of this set is a unit.(This kind of structure will be called a field.) It is easy to verify that multiplication of these elements is commutative. We can write the inverse of $aI + bJ$ formally as $(a^2 + b^2)^{-1}(aI - bJ)$ which is in the set since $(a^2 + b^2)^{-1}$ is in $\mathbb{Z}_5$.

(9) The set as in (5) but with $a, b \in \mathbb{Z}_5$.

(10) $S = P(U)$, the set of subsets of a set U. Define $+$ as $\cup$ and $\cdot$ as $\cap$.

(11) The set of 2×2 integer matrices with determinant +1 or -1.

1.3. **Properties of Rings.** Some properties of arithmetic in rings, following from the axioms, are now developed.

(a) If $a + b = a + c$ then $b = c$. If $b + a = c + a$ then $b = c$. (Cancellation Laws.)

If $a + b = a + c$ then we can add $-a$ to both sides of the equation to get $b = c$.

(b) The zero element is unique.

If z_1 and z_2 are both additive identities, then from the definition

$$z_1 + z_2 = z_1; \quad z_1 + z_2 = z_2,$$

the first because z_2 is an additive identity, and the second because z_1 is an additive identity. Hence $z_1 = z_2$.

(c) The additive inverse of a, namely $-a$ is unique.

If b and c are additive inverses of a then $a + b = 0 = a + c$, by definition. Hence by the cancellation law, $b = c$.

(d) If b is the additive inverse of a then $-b = a$.

Since $a + (-a) = 0 = b + (-b)$, where $b = -a$, then cancelling $(-a)$ and b gives $a = -b$.

(e) $(-a) \cdot (-b) = a \cdot b$.

(f) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(g) If a unity exists it is unique.

If u_1 and u_2 are both unity, then

$$u_1 = u_1 \cdot u_2 = u_2$$

the first equality holding because u_2 is a unity, and the second because u_1 is a unity.

(h) If a unity exists and x is a unit, then the multiplicative inverse of x is unique.

Let a, b both be multiplicative inverses of x. Then $xa = xb = 1$. Premultilpying by a gives $axa = axb$ and so, since $ax = 1$, $a = b$.

1.4. **Integral Domains and Fields.** *Definitions:*

(i) A commutative ring with a unity, in which there are no divisors of zero is called an *Integral Domain*.

(ii) If $(S, +, \cdot)$ is an integral domain and every non-zero element is a unit (i.e. has an inverse), then $(S, +, \cdot)$ is called a *Field*. (*Note: If* $(S, +, \cdot)$ *is a field then it is an integral domain.)*

The simplest common example of a field is the set of real numbers, $\mathbb{R}$. The integers fail to be a field because the only units are +1 and -1. But the integers themselves form an integral domain, since the product of two integers is zero if and only if at least one of the integers is zero.

Which of the examples in section 1.2 are integral domains or fields?

Examples:

(12) The set of even integers is an integral domain, but not a field.

(13) The set $\mathbb{R}^+ \times \mathbb{R}^+$ with $+, \cdot$ defined by

$$(a, b) + (c, d) \; = \; (a + c, b + d); \quad (a, b) \cdot (c, d) \; = \; (ac - bd, ad + bc).$$

1.5. **Subrings and Ring Isomorphisms.** *Definition*: Two rings, $(S_1, +, .)$ and $(S_2, +, .)$ are *isomorphic* if there is a one-to-one and onto mapping $f : S_1 \to S_2$ such that

$$\forall a, b \in S_1, \quad f(a + b) = f(a) + f(b); \quad f(a \cdot b) = f(a) \cdot f(b).$$

We write $S_1 \cong S_2$.

For example, the ring with elements a, b, c in example (2) of section 1.2 is isomorphic to $\mathbb{Z}_3$, and the ring in example (3) of section 1.2 is isomorphic to $\mathbb{Z}_6$.

$+$	s	v	x
s	s	v	x
v	v	x	s
x	x	s	v

$\cdot$	s	v	x
s	s	s	s
v	s	x	v
x	s	v	x

Figure 4. Subring of the ring in Figure 2, isomorphic to $\mathbb{Z}_3$.

$+$	s	w
s	s	w
w	w	s

$\cdot$	s	w
s	s	s
w	s	w

Figure 5. Subring of the ring in Figure 2, isomorphic to $\mathbb{Z}_2$.

In Figure 2, there is a subset $\{s, v, x\}$ which forms a ring on its own. This is a *subring* of the original ring. It is isomorphic to $\mathbb{Z}_3$, and shown in Figure 4. The original ring is isomorphic to $\mathbb{Z}_6$, and so we might wonder if there is a subring which is isomorphic to $\mathbb{Z}_2$. There is, in fact, namely the ring based on the elements $\{s, w\}$, given in Figure 5.

(14) Let S_1 be the above ring of 3 elements, and let S_2 be the ring with 2 elements. Now define a ring S over $S_1 \times S_2$ as follows.
  (a) Addition, denoted by $\oplus$ is defined by
$$\forall (a,b),(c,d) \in S_1 \times S_2, \quad (a,b) \oplus (c,d) = (a+b, c+d).$$
  (b) Multiplication, denoted by $\otimes$ is defined by
$$\forall (a,b),(c,d) \in S_1 \times S_2, \quad (a,b) \otimes (c,d) = (a \cdot b, c \cdot d).$$
  Show that $(S, \oplus, \otimes)$ is a ring. Is it isomorphic to $\mathbb{Z}_6$?

(15) If S_1, S_2 are two rings, with $S_1 \cong S_2$, under the isomorphism $f : S_1 \to S_2$, then:
  (i) $f(z_{S_1}) = z_{S_2}$ where z_{S_1}, z_{S_2} are the zero elements in S_1, S_2.
  (ii) If a unity, e_{S_1}, exists in S_1 then there is a unity, e_{S_2} in S_2, and $f(1_{S_1}) = 1_{S_2}$.
  (iii) If S_1, S_2 each have a unity, and is $a \in S_1$ is a unit, then $f(a)$ is a unit in S_2, and $f(a^{-1}) = f(a)^{-1}$.

(16) Let $(S, +, \cdot)$ be a finite ring, with n elements, $a_0, a_1, a_2, \ldots, a_{n-1}$, where a_0 is the zero. If an element a satisfies $a^2 = a$, then a is said to be *idempotent*. If for some positive integer k, $a^k = a_0$, then a is said to be *nilpotent*. Show that
  (i) If $a \neq a_0$ and a is idempotent then a cannot be nilpotent.
  (ii) If $a \neq a_0$ and a is nilpotent, then a is a divisor of zero.
  (iii) In an integral domain, the only nilpotent element is the zero element, and the only idempotent element is the unity.

Definition: Let $(S, +, \cdot)$ be a ring, and let $T \subseteq S$ be a subset of S. Then $(T, +, \cdot)$ is a *subring* of $(S, +, \cdot)$ if

(i) $\forall a, b \in T, \;\; a + b \in T, \;\; a \cdot b \in T$ and
(ii) $\forall a \in T, \;\; -a \in T$.

A second characterisation of a subring of a given ring is

$$\forall a, b \in T, \;\; a - b \in T, \;\; a \cdot b \in T.$$

We have to prove that these two characterisations are equivalent. Suppose that $T \subseteq S$ and that the elements of T satisfy the conditions of the definition of a subring. Then $\forall a, b \in T$ we know that $-b \in T$, and so $a + (-b) \in T$, which states that $a - b \in T$. Hence the definition implies the second characterisation.

Now, suppose that the elements of T satisfying the second condition. Then $\forall a, b \in T, \;\; a - b \in T$. Hence if a is in T, then $a - a \in T$ and so $z \in T$. Hence $z - a = -a \in T$, hence $-a \in T$. Also, for any $b \in T$, $-b \in T$, and so $a - (-b = a + b \in T$. Therefore T satisfies the requirements of a subring.

1.6. **Exercises.**

(1) Let $(S, +, \cdot)$ be a ring with unity. For any integer $n \geq 0$, define na where $a \in S$, to be $a + a + \ldots + a$, a added to itself n times. $0a$ is interpreted as z. Define $(-n)a$ to be $n(-a)$ for $n \geq 0$. Let m, n be non-negative integers. Prove:
   (a) $(n + m)a = ma + na$.
   (b) $n(ab) = (na)b = a(nb)$.
   (c) $m(na) = (mn)a$.

(2) The *characteristic* of a ring $(S, +, \cdot)$ is the smallest positive integer n such that $n \cdot e = z$ where e is the multiplicative identity, and z is the additive identity.
   (a) If S is finite prove that the the characteristic is finite.
   (b) If $a \in S$ is an element of a finite ring with characteristic n then $na = z$.
   (c) Give an example of a finite ring with characteristic n in which there is an element a with $ma = z$ for some $m < n$. (Hint: look at the examples we have done.)

(3) Let $\mathbb{Z}_m$ be the ring of integers mod m. What is its characteristic? Show that every element of $\mathbb{Z}_m$ is *either* a unit, *or* a divisor of zero.

(4) If $(S, +, \cdot)$ is a finite integral domain, prove that the characteristic is a prime number. (*Hint*: see exercise (2).)

(5) Let the operations $\oplus$ and $\otimes$ be defined on $\mathbb{Z}$, the set of integers, by

$$a \oplus b = a + b + a \cdot b; \quad a \otimes b = a + b + 1,$$

where $+$ and $\cdot$ are the usual operations on $\mathbb{Z}$. Is $(\mathbb{Z}, \oplus, \otimes)$ a ring under these operations?

(6) Is the set of all odd integers an integral domain?

(7) Let S be the set of all rational numbers $\frac{p}{q}$, where p is an integer, and q is of the form 2^a, where $a \geq 0$ is integer. Is S a ring? Is it an integral domain? Is it a field?

(8) Which elements in the ring $(\mathbb{Z}_{12}, +, \cdot)$ are units? Prove your claim. If this set is U, is U a subring of $\mathbb{Z}_{12}$?

(9) If $(S, +, \cdot)$ is a ring, and if a is a nilpotent element, prove that $1 + a$ and $1 - a$ are units.

(10) Is $\{0, 2, 4, 6, 8\}$ a subring of $\mathbb{Z}_{10}$? If so, construct the addition and multiplication tables.