Ring Theory Notes

Jason Sass

July 6, 2023

Rings

A ring is an algebraic structure upon which two binary operations (addition and multiplication) are defined.

Definition 1. Ring

Let R be a set.

Define binary operation $+ : R \times R \to R$ by $a + b \in R$ for all $a, b \in R$. (**addition**)

Define binary operation $\cdot : R \times R \to R$ by $a \cdot b \in R$ for all $a, b \in R$. (**multiplication**)

A **ring** $(R, +, \cdot)$ is a set R with two binary operations $+$ and $\times$ defined on R such that the following axioms hold:

A1. Addition is associative.
$(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

A2. Addition is commutative.
$a + b = b + a$ for all $a, b \in R$.

A3. There is a right additive identity.
$(\exists 0 \in R)(\forall a \in R)(a + 0 = a)$.

A4. Each element has a right additive inverse.
$(\forall a \in R)(\exists b \in R)(a + b = 0)$.

M. Multiplication is associative.
$(ab)c = a(bc)$ for all $a, b, c \in R$.

D. Multiplication is distributive over addition.
Left Distributive $a(b + c) = ab + ac$ for all $a, b, c \in R$.
Right Distributive $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Proposition 2. ***alternate definition of a ring***

Let R be a set with two binary operations $+$ and $\cdot$ defined on R.
Then $(R, +, \cdot)$ is a ring iff
1. $(R, +)$ is an abelian group.
2. Multiplication is associative.
3. Multiplication is distributive over addition.

Let $(R, +, \cdot)$ be a ring.

Then R has a right additive identity $0 \in R$, so R is a non-empty set.

Since multiplication is a binary operation on R, then R is closed under multiplication.

Since $(R, +)$ is an abelian group and R is closed under multiplication and multiplication is associative and multiplication is distributive over addition, then R satisfies the following axioms:

A1. $a + b \in R$ for all $a, b \in R$.
A2. $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
A3. $a + b = b + a$ for all $a, b \in R$.
A4. $(\exists 0 \in R)(\forall a \in R)(0 + a = a + 0 = a)$.
A5. $(\forall a \in R)(\exists b \in R)(a + b = b + a = 0)$.
M1. $ab \in R$ for all $a, b \in R$.
M2. $(ab)c = a(bc)$ for all $a, b, c \in R$.
D1. $a(b + c) = ab + ac$ for all $a, b, c \in R$.
D2. $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Proposition 3. *The additive identity of a ring is unique.*

Definition 4. zero of a ring
The identity for ring addition is called the **zero of the ring**.

Therefore, the zero of a ring is unique.
The zero of a ring R is denoted 0_R or 0.
Since $0 \in R$ for any ring R, then any ring has at least one element.

Proposition 5. *The additive inverse of each element of a ring is unique.*

The additive inverse of an element a in a ring R is denoted $-a$.
Therefore, each element of a ring has a unique additive inverse.
$(\forall a \in R)(\exists!(-a) \in R)(a + (-a) = 0)$.

Definition 6. commutative ring
A ring is **commutative** iff its multiplication is commutative.

Let $(R, +, \cdot)$ be a ring.
Then R is commutative iff $(\forall a, b \in R)(ab = ba)$.

Example 7. commutative ring of integers
$(\mathbb{Z}, +, \cdot)$ is a commutative ring.
additive identity = 0
additive inverse of a is $-a$
multiplicative identity = 1

Example 8. commutative ring of integers modulo n
Let $n \in \mathbb{Z}^+$.
$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\} = \langle [1] \rangle = \{a[1] : a \in \mathbb{Z}\} = \{[a] : a \in \mathbb{Z}\}$.
$(\mathbb{Z}_n, +, \cdot)$ is a commutative ring.
additive identity = [0]
additive inverse of $[a]$ is $[-a] = [n - a]$
multiplicative identity = [1]

Example 9. Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b, \in \mathbb{Z}\}$.
Then $\mathbb{Z}[\sqrt{2}]$ is a commutative ring.

Example 10. Let R, S be rings.
Define addition by $(a, b) + (c, d) = (a + c, b + d)$ and multiplication by $(a, b)(c, d) = (ac, bd)$.
Then $R \times S$ is a ring.

Definition 11. ring with unity
Let $(R, +, \cdot)$ be a ring with zero $0 \in R$.
Then R is a **ring with unity** iff
1. $(\exists 1 \in R)(1 \neq 0)$.
2. $(\forall a \in R)(1a = a1 = a)$.

Let $(R, +, \cdot)$ be a ring with unity $1 \in R$.
The element $1 \in R$ is a **multiplicative identity**, so $(\forall a \in R)(1a = a1 = a)$.
The identity for ring multiplication is called the **unity of the ring**.

Proposition 12. *The multiplicative identity of a ring with unity is unique.*

Let $(R, +, \cdot)$ be a ring with unity.
Then the unity of R is unique.
The unity of R is denoted 1_R or 1.

Example 13. zero ring
The **zero ring** is $\{0\}$.
$\{0\}$ is a commutative ring with unity.
Additive identity = multiplicative identity, so $0 = 1$ in the zero ring.

Proposition 14. *Let $(R, +, \cdot)$ be a ring.*
Then for all $a, b, c \in R$
1. if $a = b$, then $a + c = b + c$.
2. if $a = b$, then $ac = bc$.

Theorem 15. ***basic properties of a ring***
Let $(R, +, \cdot)$ be a ring.
Then for all $a, b, c \in R$
1. if $c + a = c + b$ then $a = b$ and if $a + c = b + c$ then $a = b$.
(left and right additive cancellation laws)
2. $a0 = 0a = 0$.
3. $-(-a) = a$.
4. $-(a + b) = (-a) + (-b)$.
5. $a(-b) = (-a)b = -(ab)$.
6. $(-a)(-b) = ab$.
7. If R has a unity, then $(-1)a = -a$.

Definition 16. subtraction
Let $(R, +, \cdot)$ be a ring.
Define binary operation **subtraction**, $R \times R \to R$ by $a - b = a + (-b)$ for all $a, b \in R$.
Then $a - b$ is the **difference** between a and b.

Let a, b be elements of a ring R.
Then $a - b = a + (-b) \in R$, by closure of R under addition.
Therefore, a ring is closed under subtraction: $(\forall a, b \in R)(a - b \in R)$.

Proposition 17. ***addition and subtraction are inverse operations***
Let R be a ring.
Then $(\forall a, b \in R)(\exists! x \in R)(a + x = b)$.

Therefore, $a + x = b$ means $x = b - a$.
Addition and subtraction are inverse operations.
Therefore $a - b = c$ iff $a = b + c$.
Therefore c is the element such that $b + c = a$.

Proposition 18. ***properties of subtraction in a ring***
Let $(R, +, \cdot)$ be a ring.
For all $a, b, c \in R$
1. $-a = 0 - a$.
2. Multiplication is distributive over subtraction.
$a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.
3. $a = b$ iff $a - b = 0$.
4. $-a - b = -(a + b)$.
5. $a - (b - c) = (a - b) + c$.

Definition 19. unit
Let R be a ring with unity $1 \neq 0$.
An element $a \in R$ is a **unit** iff $(\exists b \in R)(ab = ba = 1)$.

Therefore an element of a ring is a unit iff it has a multiplicative inverse.
In the zero ring $\{0\}$, the unity $1 = 0$, so we don't allow units to be defined in the zero ring.
Therefore, any consideration of multiplicative inverses excludes the zero ring.

Proposition 20. *The multiplicative inverse of each unit of a ring is unique.*

Let a be a unit of a ring R with unity $1 \neq 0$.
The multiplicative inverse of a is denoted by a^{-1} and $aa^{-1} = a^{-1}a = 1$.

Proposition 21. *The zero element of a ring is not a unit.*

Therefore the zero element of a ring does not have a multiplicative inverse.
Hence, 0^{-1} does not exist.
Let R be a ring.
Let $a \in R$.
Then either $a = 0$ or $a \neq 0$.
If $a = 0$, then a is not a unit.
Hence, if a is a unit, then $a \neq 0$.
Therefore any unit of a ring must be nonzero.

Proposition 22. *In any ring the additive inverse of the additive identity element equals itself.*

Let R be a ring with zero 0.
Then $-0 = 0$, so $0 + 0 = 0$.

Let R be a ring and $a \in R$.
If $a = 0$, then $-a = -0 = 0$.
Therefore, if $a = 0$, then $-a = 0$ for all $a \in R$.

Proposition 23. *In any nonzero ring the multiplicative inverse of the multiplicative identity element equals itself.*

Therefore, in any nonzero ring $1^{-1} = 1$, so $1 \cdot 1 = 1$.

Proposition 24. *In any ring $-x = 0$ iff $x = 0$.*

Theorem 25. *The set of all units of a ring is a multiplicative group.*

Let S be the set of all units of a ring $(R, +, \cdot)$.
Then

$$\begin{aligned} S &= \{a \in R : a \text{ is a unit}\} \\ &= \{a \in R : (\exists b \in R)(ab = ba = 1)\}. \end{aligned}$$

$(S, \cdot)$ is a multiplicative group called the **group of units of** R.
The multiplicative identity of S is $1 \in R$.
The multiplicative inverse of $a \in S$ is $a^{-1} \in S$.
Therefore, a^{-1} is a unit and $aa^{-1} = a^{-1}a = 1$.
Since $a^{-1}a = aa^{-1} = 1$, then a is a multiplicative inverse of a^{-1}.
Therefore, a and a^{-1} are multiplicative inverses of each other.

Definition 26. division ring(skew field)
Let $(R, +, \cdot)$ be a ring with unity $1 \neq 0$.
Then $(R, +, \cdot)$ is a **division ring** iff every nonzero element of R is a unit.

Example 27. $(\mathbb{Z}, +, \cdot)$ is not a division ring.

Since $1 = 0$ in the zero ring, then the zero ring is not a division ring.
Since $1 \neq 0$ in a division ring, then any division ring must contain at least two elements.

Let $(R, +, \cdot)$ be a division ring.
Let $R^* = \{a \in R : a \neq 0\}$.
Let S be the set of all units of R.
We prove $S = R^*$.
Let $a \in R^*$.
Then $a \in R$ and $a \neq 0$.
Since every nonzero element of R is a unit, then a is a unit.
Hence, $a \in S$.
Therefore, $R^* \subset S$.
Let $b \in S$.
Then $b \in R$ and b is a unit. Since any unit of a ring is nonzero, then $b \neq 0$. Thus, $b \in R$ and $b \neq 0$, so $b \in R - \{0\}$. Hence, $b \in R^*$. Therefore, $S \subset R^*$.
Since $S \subset R^*$ and $R^* \subset S$, then $S = R^*$.

Since the set of all units of R is a multiplicative group and $S = R^*$, then $(R^*, \cdot)$ is the group of units of R.

Therefore, $(R^*, \cdot)$ is the group of units of a division ring R.

The multiplicative identity of R^* is $1 \in R$.

Let $a \in R^*$. Then $a \in R$ and $a \neq 0$ and a is a unit.

The multiplicative inverse of a is $a^{-1} \in R^*$. Therefore, $a^{-1} \neq 0$ and $aa^{-1} = a^{-1}a = 1$. Since $a^{-1} \in R^*$, then a^{-1} is a unit.

Definition 28. division

Let $(R, +, \cdot)$ be a division ring.

Let $R^* = \{r \in R : r \neq 0\}$.

Let $a, b \in R$ with $b \neq 0$.

Define operation **division**, $R \times R^* \to R$ by $\frac{a}{b} = a \cdot b^{-1}$.

Then $\frac{a}{b}$ is the **quotient** of a and b.

Let $(R, +, \cdot)$ be a division ring.

Let $a, b \in R$ with $b \neq 0$.

Since $b \neq 0$, then its multiplicative inverse b^{-1} exists in R and $\frac{a}{b} = a \cdot b^{-1} \in R$, by closure of R under multiplication.

Therefore, a division ring is closed under division: $(\forall a, b \in R, b \neq 0)(\frac{a}{b} \in R)$.

Since zero does not have a multiplicative inverse in any ring, then zero does not have a multiplicative inverse in R.

Therefore, division by zero is undefined.

Since $(R^*, \cdot)$ is the group of units of R, let $a, b \in R^*$. Then b is a unit, so $b^{-1} \in R^*$. Hence, $b^{-1} \neq 0$.

Since R^* is closed under multiplication and $a \in R^*$ and $b^{-1} \in R^*$, then $ab^{-1} = \frac{a}{b} \in R^*$. Therefore, R^* is closed under division.

Therefore, the set of all nonzero elements of a division ring, the multiplicative group of units, is closed under division: $(\forall a, b \in R^*)(\frac{a}{b} \in R^*)$.

Multiplication and division are inverse operations.

Thus $\frac{a}{b} = c$ iff $a = bc$.

Therefore c is the element such that $bc = a$.

Proposition 29. ***properties of a division ring***

Let $(R, +, \cdot)$ be a division ring. Then for all $a, b, c \in R$

1. *if $a \neq 0$, then $a^{-1} = \frac{1}{a}$.*
2. *if $a \neq 0$, then $(a^{-1})^{-1} = a$.*
3. *$\frac{a}{b} = 1$ iff $a = b$ and $b \neq 0$.*
4. *if $a \neq 0$ and $b \neq 0$, then $(\frac{a}{b})^{-1} = \frac{b}{a}$.*
5. *if $c \neq 0$, then $\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$.*
6. *if $c \neq 0$, then $\frac{a}{c} - \frac{b}{c} = \frac{a-b}{c}$.*

Definition 30. Let $(R, +, \cdot)$ be a ring.

Let $x \in R$.

Define $nx = (n-1)x + x$ for all $n \in \mathbb{N}$.

Since $1x = (1-1)x + x = 0x + x = 0 + x = x$, then $1x = x$.

Example 31. characteristic of $\mathbb{Z}$ is zero.
Since $0k = 0$ for all $k \in \mathbb{Z}$, then there is no positive integer n such that $nk = 0$ for all $k \in \mathbb{Z}$. Therefore, the characteristic of $\mathbb{Z}$ is zero.

Subrings

Definition 32. Subring
A **subring** of a ring R is a subset of R which is a ring under the same $+$ and $\times$ as R and shares the same multiplicative identity.
Let $(R, +, \cdot)$ be a ring.
Then S is a subring of R iff
1. $S \subset R$.
2. $(S, +, *)$ is a ring.
3. S has the same multiplicative identity as R.
if e is multiplicative identity of R, then e is multiplicative identity of S.

$(S, +, *) < (R, +, *)$ means S is a subring of R

Let $(R, +, *)$ be an arbitrary ring with additive identity $0 \in R$.
Since $R \subset R$ and $(R, +, *)$ is a ring, then $R < R$.
Therefore every ring is a subring of itself.

Since $0 \in R$ and $\{0\}$ is the trivial ring, then $\{0\} < R$.
Therefore the zero ring is a subring of every ring.

Theorem 33. *Let $(R, +, *)$ be a ring.*
Let $S \subset R$.
Then S is a subring of R iff
1. $S \neq \emptyset$.
2. Closed under subtraction: $(\forall a, b \in S)(a - b \in S)$.
3. Closed under multiplication: $(\forall a, b \in S)(ab \in S)$.
4. S has the same multiplicative identity as R.

Example 34. $\mathbb{Z}$ has no subrings other than itself.
$\mathbb{Z}_n$ has no subrings other than itself.

Integral Domains

Definition 35. zero divisor of a commutative ring
Let R be a commutative ring.
Let $a \in R^*$.
Then a is a **zero divisor** iff $(\exists b \in R^*)(ab = 0)$.

Suppose $a \in R^*$.
If $(\exists b \in R^*)(ab = 0)$, then a is a zero divisor.
If $\neg(\exists b \in R^*)(ab = 0)$, then a is not a zero divisor.
Therefore, if $(\forall b \in R^*)(ab \neq 0)$, then a is not a zero divisor.

Since there are no nonzero elements in the zero ring, then there are no zero divisors in the zero ring. Therefore, only nonzero rings may have zero divisors.

Example 36. In $(\mathbb{Z}_{10}, +, *)$, [2] is a divisor of [0] because $[5] \neq [0]$ and $[2][5] = [0]$. Also, [5] is a divisor of [0] because $[2] \neq [0]$ and $[5][2] = [0]$.

Proposition 37. *A zero divisor cannot be a unit and a unit cannot be a zero divisor.*

Definition 38. integral domain
An **integral domain** is a commutative ring with nonzero unity that has no zero divisors.

Let $(R, +, \cdot)$ be a commutative ring with unity $1 \neq 0$.
Define predicate $p(a) : a$ is a zero divisor of R.
Then $p(a) : a \in R^* \wedge (\exists b \in R^*)(ab = 0)$.
The statement 'there is a zero divisor in R' translates into $(\exists a \in R^*)(\exists b \in R^*)(ab = 0)$.
The statement 'there are no zero divisors in R' means 'there does not exist a zero divisor in R'.
The statement there does not exist a zero divisor in R translates into $\neg(\exists a \in R)(p(a))$.
Observe that

$$\begin{aligned}
\neg(\exists a \in R)(p(a)) &\Leftrightarrow \neg(\exists a \in R)(a \in R^*) \wedge (\exists b \in R^*)(ab = 0)) \\
&\Leftrightarrow \neg(\exists a \in R^*)(\exists b \in R^*)(ab = 0) \\
&\Leftrightarrow (\forall a \in R^*)(\forall b \in R^*)(ab \neq 0) \\
&\Leftrightarrow a \in R^* \wedge b \in R^* \rightarrow ab \neq 0 \\
&\Leftrightarrow a \neq 0 \wedge b \neq 0 \rightarrow ab \neq 0 \\
&\Leftrightarrow ab = 0 \rightarrow a = 0 \vee b = 0.
\end{aligned}$$

Therefore, there are no zero divisors in R is equivalent to
1. $(\forall a, b \in R^*)(ab \neq 0)$.
2. $(\forall a, b \in R)$ if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.
3. $(\forall a, b \in R)$ if $ab = 0$, then either $a = 0$ or $b = 0$.

Therefore, an integral domain $(R, +, \cdot)$ is a commutative ring with unity $1 \neq 0$ such that any of the following are true:
1. $(\forall a, b \in R^*)(ab \neq 0)$ (The product of any two nonzero elements of R is nonzero).
2. $a \neq 0 \wedge b \neq 0 \rightarrow ab \neq 0$ for all $a, b \in R$.
3. $ab = 0 \rightarrow a = 0 \vee b = 0$ for all $a, b \in R$.

Let $(R, +, \cdot)$ be an integral domain.
Since $1 \neq 0$, then R contains at least two elements.
Therefore, an integral domain has at least two elements.
Hence, the zero ring cannot be an integral domain.

Let $a, b \in R$.
If $a = 0$, then $ab = 0b = 0$.
If $b = 0$, then $ab = a0 = 0$.
Therefore, $a = 0$ or $b = 0$ implies $ab = 0$.
Since $ab = 0$ implies either $a = 0$ or $b = 0$ and $a = 0$ or $b = 0$ implies $ab = 0$, then $ab = 0$ iff either $a = 0$ or $b = 0$ for all $a, b \in R$.
Therefore, in any integral domain $ab = 0$ iff $a = 0$ or $b = 0$.
Hence, in any integral domain $ab \neq 0$ iff $a \neq 0$ and $b \neq 0$.

Example 39. $(\mathbb{Z}, +, \cdot)$ is an integral domain.

Proposition 40. $(\mathbb{Z}_p, +, \cdot)$ ***is an integral domain.***
Let p be prime and $[a], [b] \in (\mathbb{Z}_p, +, \cdot)$.
If $[a][b] = 0$, then $[a] = 0$ or $[b] = 0$.

Generally, $(\mathbb{Z}_n, +, \cdot)$ is not an integral domain.
However, if p is prime, then $(\mathbb{Z}_p, +, \cdot)$ is an integral domain.

Theorem 41. ***multiplicative cancellation laws hold in an integral domain***
Let $(D, +, \cdot)$ be a commutative ring with nonzero unity.
Then D is an integral domain iff for all $a, b, c \in D$, if $ca = cb$ and $c \neq 0$, then $a = b$.

Ideals

Definition 42. ideal of a ring
An **ideal in a ring** R is an additive subgroup $I \subset R$ such that $RI \subset I$ and $IR \subset I$.
Let $(R, +, *)$ be a ring.
Let $(I, +) < (R, +)$.
Then I is an ideal iff $(\forall x \in I)(Rx \subset I \wedge xR \subset I)$.

Let $x \in I$.
$Rx = \{rx : r \in R\}$ (**left ideal**)
$xR = \{xr : r \in R\}$ (**right ideal**)
Therefore, all multiples of $x \in R$ lie in I.

Since $(R, +)$ is an abelian group and $I \subset R$, then I is abelian.
Hence, $(I, +)$ is an abelian subgroup of $(R, +)$.

Let I be an ideal of a ring R.
Then $I \subset R$ and
1. $(\forall a, b \in I)(a + b \in I)$. (closed under addition)
2. $(\forall a \in I)(\forall r \in R)(ra \in I)$. (closed under multiplication by any element of R)

Examples:
$(2\mathbb{Z}, +, *)$ is an ideal of $\mathbb{Z}$.

Proposition 43. *Let R be a ring.*
The zero ring and R itself are ideals in R.

R and the zero ring $\{0\}$ are **trivial ideals**.

Definition 44. principal ideal of a ring
Let R be a commutative ring.
Let $a \in R$.
Then the ideal $(a) = \{ra : r \in R\}$ is called the **principal ideal generated by a in R.**

Since R is commutative, then $ra = ar$, so $(a) = \{ra : r \in R\} = \{ar : r \in R\}$.

Theorem 45. *Every ideal in the ring $\mathbb{Z}$ is a principal ideal.*

Let I be an ideal of $\mathbb{Z}$. Then there exists $n \in \mathbb{Z}$ such that $I = (n) = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$. Thus, the only ideals in $\mathbb{Z}$ are multiples of n for every $n \in \mathbb{Z}$.

Quotient Rings

Definition 46. congruence modulo relation of an ideal
Let I be an ideal of a ring R.
Let $a, b \in R$.
Then a **is congruent to** b **modulo** I , denoted $a \equiv b \pmod{I}$, iff $a - b \in I$.
Observe that congruence modulo I is a binary relation on R.

Proposition 47. *Let I be an ideal in a ring R. Then congruence modulo I is an equivalence relation on R.*

Let $a \in R$. The equivalence class containing a is

$$\begin{aligned} [a] &= \{r \in R : r \equiv a \pmod{I}\} \\ &= \{r \in R : r - a \in I\} \\ &= \{r \in R : i = r - a \in I, i \in I\} \\ &= \{a + i \in R : i \in I\} \\ &= \{a + i : i \in I\} \\ &= a + I. \end{aligned}$$

$a + I$ is the left coset of I with representative $a \in R$.

Proposition 48. *Let I be an ideal in a ring R. Let $a, b \in R$. Then $a - b \in I$ iff $a + I = b + I$.*

Therefore, $a \equiv b \pmod{I}$ iff $a - b \in I$ iff $a + I = b + I$.

Definition 49. Quotient Ring
Let I be an ideal in a ring R.
Let $\frac{R}{I}$ be the collection of all cosets of I in R.
Then $\frac{R}{I} = \{a + I : a \in R\}$.
Define coset addition by : $(a + I) + (b + I) = (a + b) + I$ for all $a, b \in R$.
Define coset multiplication by : $(a + I)(b + I) = ab + I$ for all $a, b \in R$.
The set $\frac{R}{I}$ is a ring under coset addition and coset multiplication.
$I = 0 + I$ is additive identity, where 0 is additive identity of R
$e + I$ is multiplicative identity, where e is multiplicative identity of R
$(\frac{R}{I}, +, *)$ is the **quotient ring of R modulo I**.
Each $a + I$ is called a **coset modulo I**.

Ring Homomorphisms

Definition 50. ring homomorphism
Let R be a ring with unity 1 and let R' be a ring with unity $1'$.
A function $\phi : R \to R'$ is a **ring homomorphism** iff
1. Preserves addition: $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$.
2. Preserves multiplication: $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.
3. Preserves unity: $\phi(1) = 1'$.

Definition 51. kernel of a ring homomorphism
Let R be a ring with zero 0 and let R' be a ring with zero $0'$.
Let $\phi : R \to R'$ be a ring homomorphism.
The **kernel of** ϕ, denoted $\ker(\phi)$, is the set $\{r \in R : \phi(r) = 0'\}$.

Example 52. Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $\phi(a) = [a]_n$ for all $a \in \mathbb{Z}$.
Let $a, b \in \mathbb{Z}$.
Then

$$\begin{aligned} \phi(a + b) &= [a + b]_n \\ &= [a] + [b] \\ &= \phi(a) + \phi(b) \end{aligned}$$

and

$$\begin{aligned} \phi(ab) &= [ab]_n \\ &= [a][b] \\ &= \phi(a)\phi(b). \end{aligned}$$

Observe that 1 is the unity of $\mathbb{Z}$ and $[1]_n$ is the unity of $\mathbb{Z}_n$ and $\phi(1) = [1]_n$.

Therefore, ϕ is a ring homomorphism.

$$\begin{aligned}\ker(\phi) &= \{a \in \mathbb{Z} : \phi(a) = [0]_n\} \\ &= \{nk : k \in \mathbb{Z}\} \\ &= n\mathbb{Z}.\end{aligned}$$

Example 53. Let $C_{[a,b]}$ be the ring of continuous real valued functions defined on the closed interval $[a, b]$.

Then $C_{[a,b]} = \{f : [a, b] \to \mathbb{R} | f \text{ is continuous }\}$.

Let $\alpha \in [a, b]$ be fixed.

Let $\phi : C_{[a,b]} \to \mathbb{R}$ be defined by $\phi_\alpha(f) = f(\alpha)$.

Let $f, g \in C_{[a,b]}$.

Then

$$\begin{aligned}\phi_\alpha(f + g) &= (f + g)(\alpha) \\ &= f(\alpha) + g(\alpha) \\ &= \phi_\alpha(f) + \phi_\alpha(g)\end{aligned}$$

and

$$\begin{aligned}\phi_\alpha(fg) &= (fg)(\alpha) \\ &= f(\alpha)g(\alpha) \\ &= \phi_\alpha(f)\phi_\alpha(g).\end{aligned}$$

The function $f : [a, b] \to \mathbb{R}$ defined by $f(x) = 1$ for all $x \in [a, b]$ is the unity element of $C_{[a,b]}$ and 1 is the unity element of $\mathbb{R}$. Observe that $\phi_\alpha(f) = f(\alpha) = 1$.

Therefore, ϕ is a ring homomorphism.

$$\begin{aligned}\ker(\phi) &= \{f \in C_{[a,b]} : \phi_\alpha(f) = 0\} \\ &= \{f \in C_{[a,b]} : f(\alpha) = 0\}.\end{aligned}$$

Thus, the kernel of ϕ is the collection of all continuous real valued functions defined on $[a, b]$ that have x intercept at $x = \alpha$.

Proposition 54. *Let R be a ring with zero 0 and let R' be a ring with zero $0'$.*

Let $\phi : R \to R'$ be a ring homomorphism. Then the following are true:

1. $\phi(0) = 0'$.

2. If R is a commutative ring, then $\phi(R)$ is a commutative ring.

3. If R is a field and $\phi(R) \neq \{0'\}$, then $\phi(R)$ is a field.

Theorem 55. *Let $\phi : R \to R'$ be a ring homomorphism.*

Then $\ker(\phi)$ is an ideal in R.

Theorem 56. *Let I be an ideal of a ring R. Let $\eta : R \to \frac{R}{I}$ be defined by $\eta(a) = a + I$ for all $a \in R$. Then η is a ring homomorphism of R onto $\frac{R}{I}$ with kernel I. We call η the **natural homomorphism** from R onto $\frac{R}{I}$.*

Definition 57. ring isomorphism
A **ring isomorphism** is a bijective ring homomorphism.

Theorem 58. *Fundamental Homomorphism Theorem*
Let $\phi : R \mapsto R'$ be a ring homomorphism with kernel K. Then there exists a unique ring isomorphism $\phi' : \frac{R}{K} \to \phi(R)$ defined by $\phi'(rK) = \phi(r)$ for all $r \in R$ such that $\phi' \circ \eta = \phi$, where $\eta : R \to \frac{R}{K}$ is the natural homomorphism.

Ring Facts

finite fields $\subset$ fields $\subset$ Euclidean domains $\subset$ principal ideal domains $\subset$ unique factorization domains $\subset$ integral domains $\subset$ commutative rings

Definition 59. integral ideal
Let $S \subseteq \mathbb{Z}$ be nonempty. Then S is an **integral ideal** iff
1. S is closed under addition and subtraction.
2. if $n \in S$ and $r \in \mathbb{Z}$, then $rn \in S$.

$\langle m \rangle = \{km : k \in \mathbb{Z}\}$ = all multiples of integer m is an integral ideal.

Number Rings

Multiples of integer n $(n\mathbb{Z}, +, *)$

Let $n \in \mathbb{Z}^+$.
$(n\mathbb{Z}, +, *)$ is an ideal of $\mathbb{Z}$.
additive identity = 0
additive inverse of nk is $-nk$ for some $k \in \mathbb{Z}$

Proposition 60. *Let $n \in \mathbb{Z}^+$. Then $(n\mathbb{Z}, +, *)$ has a multiplicative identity iff $n = 1$.*

Therefore, if $n > 1$, then $n\mathbb{Z}$ has no multiplicative identity.

Proposition 61. *Let $n \in \mathbb{Z}^+$. Then $n\mathbb{Z}$ is an integral domain iff $n = 1$.*

Therefore, if $n > 1$, then $n\mathbb{Z}$ is not an integral domain.

Subring Relationships of number rings

$(n\mathbb{Z}, +, *) < (\mathbb{Z}, +, *) < (\mathbb{Q}, +, *) < (\mathbb{R}, +, *) < (\mathbb{C}, +, *)$
$(\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$
$(\mathbb{Q}^+, \cdot) < (\mathbb{R}^+, \cdot) < (\mathbb{R}^*, \cdot)$

Function Rings

Let $F = \{f : \mathbb{R} \mapsto \mathbb{R} | f \text{ is a function}\}$.

The sum of functions, denoted $f + g$, is defined by function addition where $(f + g)(x) = f(x) + g(x)$ for all $x \in \mathbb{R}$.

The product of functions, denoted fg, is defined by function multiplication where $(fg)(x) = f(x)g(x)$ for all $x \in \mathbb{R}$.

$(F, +)$ = abelian group

Additive identity is the zero function $f(x) = 0$ for all $x \in \mathbb{R}$.

Additive inverse of $f(x)$ is $-f(x) = (-f)(x)$ for all $x \in \mathbb{R}$.

$(F, +, *)$ = commutative ring

Direct product of Rings

Theorem 62. *Let $(R, +, *)$ be a ring with unity e. Let $n \in \mathbb{Z}^+, n \geq 2$. Then $(R^n, +, *)$ is a ring with unity $(e, e, ..., e)$.*

Therefore, the direct product of n copies of a ring is a ring.

Theorem 63. *Let $(R, +, *)$ be a commutative ring. Then $(R^n, +, *)$ is a commutative ring.*

Therefore, the direct product of n copies of a commutative ring is a commutative ring.

Matrix Rings

Let R be a ring.

Let $n \in \mathbb{Z}^+$.

Let $M_n(R)$ = $n \times n$ matrices with entries in R.

Then $(M_n(R), +, *)$ is a ring with unity I = identity matrix.

If $n \geq 2$, then $M_n(R)$ is a non-commutative ring.

Rings:

1. $M_n(\mathbb{Z})$ = square matrices of integers
2. $M_n(\mathbb{Q})$ = square matrices of rationals
3. $M_n(\mathbb{R})$ = square matrices of real numbers
4. $M_n(\mathbb{C})$ = square matrices of complex numbers