Ring Theory

Jason Sass

June 22, 2023

Rings

Proposition 1. ***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.

Proof. We prove if $(R, +)$ is an abelian group and multiplication is associative and multiplication is distributive over addition, then $(R, +, \cdot)$ is a ring.

Suppose $(R, +)$ is an abelian group and multiplication is associative and multiplication is distributive over addition.

Since $(R, +)$ is an abelian group, then addition is associative and commutative.

Hence, $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$ and $a + b = b + a$ for all $a, b \in R$.

Since $(R, +)$ is a group, then there is an additive identity in R.

Therefore, there exists $0 \in R$ such that $0 + a = a + 0 = a$ for all $a \in R$.

Hence, there exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$.

Therefore, 0 is a right additive identity in R.

Since $(R, +)$ is a group, then each element has an additive inverse.

Thus, for each $a \in R$ there exists $b \in R$ such that $a + b = b + a = 0$.

Hence, for each $a \in R$ there exists $b \in R$ such that $a + b = 0$.

Therefore, each element of R has a right additive inverse in R.

Since multiplication is associative, then $(ab)c = a(bc)$ for all $a, b, c \in R$.

Since multiplication is distributive over addition, then $a(b+c) = ab+ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Therefore, $(R, +, \cdot)$ is a ring.

Conversely, we prove if $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group and multiplication is associative and multiplication is distributive over addition.

Suppose $(R, +, \cdot)$ is a ring.

Since R is a ring, then $(ab)c = a(bc)$ for all $a, b, c \in R$, so multiplication is associative.

Since R is a ring, then $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ for all $a, b, c \in R$.

Hence, multiplication is left and right distributive over addition, so multiplication is distributive over addition.

We prove $(R, +)$ is an abelian group.

Since R is a ring, then addition is a binary operation defined on R.

Therefore, $(R, +)$ is a binary algebraic structure.

Since R is a ring, then addition is associative and there is a right additive identity and each element of R has a right additive inverse in R.

Therefore, $(R, +)$ is an associative binary algebraic structure with a right additive identity such that every element has a right additive inverse.

Any associative binary structure with a right identity such that each element has a right inverse is a group.

Therefore, $(R, +)$ is a group.

Since R is a ring, then addition is commutative.

Therefore, $(R, +)$ is an abelian group. $\square$

Proposition 2. *The additive identity of a ring is unique.*

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

We must prove there is an additive identity in R and the additive identity is unique.

Existence:

Since R is a ring, then there exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$.

Let $a \in R$.

Then $a + 0 = a$.

Since addition is commutative in R, then $0 + a = a$.

Hence, $a + 0 = a = 0 + a$, so 0 is an additive identity of R.

Therefore, at least one additive identity element exists in R.

Uniqueness:

Since R is a ring, then addition is a binary operation defined over R.

Therefore, $(R, +)$ is a binary structure.

Since 0 is an additive identity of R, then $(R, +)$ is a binary structure with identity.

If a binary structure has an identity element, then the identity element is unique.

Therefore, 0 is unique. $\square$

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

Existence:

Let $a \in R$.

Since there is a right additive identity in R, then there exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$.

In particular, $a + 0 = a$ and $0 + 0 = 0$.

Since $a \in R$ and each element has a right additive inverse, then there exists $b \in R$ such that $a + b = 0$.

We prove $0 + a = a$.

Observe that

$$\begin{aligned} a+b &= 0 \\ &= 0+0 \\ &= 0+(a+b) \\ &= (0+a)+b. \end{aligned}$$

Thus, $a+b=(0+a)+b$.

Since addition is a binary operation on R, then $(R,+)$ is a binary algebraic structure.

Since R is a ring, then addition is associative and there is a right additive identity in R and each element in R has a right additive inverse in R.

Therefore, $(R,+)$ is an associative binary structure with a right identity such that each element of R has a right inverse.

Hence, the right cancellation law holds.

Thus, $a=0+a$, so $a+0=a=0+a$.

Therefore, 0 is an additive identity in R.

Uniqueness:

Since $(R,+)$ is a binary structure with identity, then the identity is unique.

Therefore, 0 is unique. □

Proposition 3. *The additive inverse of each element of a ring is unique.*

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

Let $a \in R$.

We must prove a has an additive inverse and the additive inverse of a is unique.

Existence:

Let $0 \in R$ be the additive identity of R.

Since each element of R has a right additive inverse and $a \in R$, then there exists $b \in R$ such that $a+b=0$.

Since addition is commutative in R, then $b+a=0$.

Hence, $a+b=0=b+a$, so b is an additive inverse of a.

Therefore, at least one additive inverse of a exists in R.

Uniqueness:

Since $(R,+,\cdot)$ is a ring, then $+$ is a binary operation on R and addition is associative and there is an additive identity in R.

Therefore, $(R,+)$ is an associative binary structure with identity.

Hence, the inverse of each invertible element is unique.

Since b is an additive inverse of a, then a is invertible, so the inverse of a is unique.

Therefore, b is unique. □

Proposition 4. *The multiplicative identity of a ring with unity is unique.*

Proof. Let $(R, +, \cdot)$ be a ring with unity $1 \in R$.

Since $(R, +, \cdot)$ is a ring, then multiplication is a binary operation on R, so $(R, \cdot)$ is a binary structure.

Since $1 \in R$ is unity, then $1a = a1 = a$ for all $a \in R$, so there exists $1 \in R$ such that $1a = a1 = a$ for all $a \in R$.

Hence, 1 is a multiplicative identity in R.

Thus, $(R, \cdot)$ is a binary structure with identity.

If a binary structure has an identity, then the identity is unique.

Therefore, 1 is unique. □

Proposition 5. *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 $ac = bc$.

Proof. We prove 1.

Suppose $a = b$.

By reflexivity of equality, $a + c = a + c$.

Since $a = b$, then by substitution we have $a + c = b + c$, as desired. □

Proof. We prove 2.

Suppose $a = b$.

By reflexivity of equality, $ac = ac$.

Since $a = b$, then by substitution we have $ac = bc$, as desired. □

Theorem 6. ***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 $(-1)a = -a$.

Proof. We prove 1.

Let $a, b, c \in R$.

Suppose $c + a = c + b$.

Then

$$\begin{aligned} a &= 0 + a \\ &= ((-c) + c) + a \\ &= -c + (c + a) \\ &= -c + (c + b) \\ &= ((-c) + c) + b \\ &= 0 + b \\ &= b. \end{aligned}$$

Therefore, $a = b$, as desired.

Suppose $a + c = b + c$.

Then

$$\begin{aligned} a &= a + 0 \\ &= a + (c + (-c)) \\ &= (a + c) + (-c) \\ &= (b + c) + (-c) \\ &= b + (c + (-c)) \\ &= b + 0 \\ &= b. \end{aligned}$$

Therefore, $a = b$, as desired. ☐

Proof. We prove 2.

Let $a \in R$.

Observe that

$$\begin{aligned} a0 + 0 &= a0 \\ &= a(0 + 0) \\ &= a0 + a0. \end{aligned}$$

Therefore, $a0 + 0 = a0 + a0$, so by the left cancellation law for addition, $0 = a0$.

Observe that

$$\begin{aligned} 0a + 0 &= 0a \\ &= (0 + 0)a \\ &= 0a + 0a. \end{aligned}$$

Therefore, $0a + 0 = 0a + 0a$, so by the left cancellation law for addition, $0 = 0a$.

Hence, $a0 = 0 = 0a$. ☐

Proof. We prove 3.

Let $a \in R$.

Then $-a \in R$, so $a + (-a) = -a + a = 0$.
Hence, $-a + a = a + (-a) = 0$, so a is the additive inverse of $-a$.
Therefore, $-(-a) = a$. $\square$

Proof. We prove 4.
Let $a, b \in R$.
Then $-a, -b \in R$.
Observe that

$$\begin{aligned}(a+b)+(-(a+b)) &= 0 \\ &= 0+0 \\ &= (-a+a)+(b+(-b)) \\ &= -a+(a+b)+(-b) \\ &= (a+b)+((-a)+(-b)).\end{aligned}$$

Therefore, $(a+b)+(-(a+b)) = (a+b)+((-a)+(-b))$, so by the left cancellation law for addition, $-(a+b) = (-a)+(-b)$. $\square$

Proof. We prove 5.
Let $a, b \in R$.
Observe that

$$\begin{aligned}ab + a(-b) &= a(b+(-b)) \\ &= a0 \\ &= 0 \\ &= ab + (-(ab)).\end{aligned}$$

Therefore, $ab+a(-b) = ab+(-(ab))$, so by the left cancellation law for addition, $a(-b) = -(ab)$.
Observe that

$$\begin{aligned}ab + (-a)b &= (a+(-a))b \\ &= 0b \\ &= 0 \\ &= ab + (-(ab)).\end{aligned}$$

Therefore, $ab+(-a)b = ab+(-(ab))$, so by the left cancellation law for addition, $(-a)b = -(ab)$.
Hence, $a(-b) = -(ab) = (-a)b$. $\square$

Proof. We prove 6.
Let $a, b \in R$.
Observe that

$$\begin{aligned}(-a)(-b) &= -(a(-b)) \\ &= -(-(ab)) \\ &= ab.\end{aligned}$$

□

Proof. We prove 7.

Suppose R has a unity.

Then R has a multiplicative identity, so let 1 be the multiplicative identity of R.

Then $1a = a1 = a$ for all $a \in R$.

Let $a \in R$.

Then $1a = a$.

Since $(R, +)$ is an additive group, then $(-1)a = -(1a)$, by the laws of exponents for an additive group.

Observe that $(-1)a = -(1a) = -a$. □

Proposition 7. ***addition and subtraction are inverse operations***

Let R be a ring.

Then $(\forall a, b \in R)(\exists! x \in R)(a + x = b)$.

Proof. Let $a, b \in R$.

We prove a solution to the equation $a + x = b$ is unique.

Existence:

Since R is closed under subtraction, then $b - a \in R$.

Let $x = b - a$.

Then

$$\begin{aligned} a + x &= a + (b - a) \\ &= a + (-a + b) \\ &= (a + (-a)) + b \\ &= 0 + b \\ &= b. \end{aligned}$$

Hence, $a + x = b$.

Therefore, at least one solution exists.

Uniqueness:

Suppose $x_1, x_2 \in R$ are solutions to $a + x = b$.

Then $a + x_1 = b$ and $a + x_2 = b$.

Thus $a + x_1 = a + x_2$.

By the left additive cancellation law for rings, we obtain $x_1 = x_2$.

Therefore, at most one solution exists.

Since at least one solution exists and at most one solution exists, then exactly one solution exists.

Therefore, a solution to $a + x = b$ is unique. □

Proposition 8. ***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. $a - (b-c) = (a-b) + c$.

Proof. We prove 1.
Let $a \in R$.
Since $a \in R$, then $-a \in R$.
Therefore, $-a = 0 + (-a) = 0 - a$, as desired. ☐

Proof. We prove 2.
Let $a, b, c \in R$.
Then

$$\begin{aligned} a(b-c) &= a(b+(-c)) \\ &= ab + a(-c) \\ &= ab + (-(ac)) \\ &= ab - ac \end{aligned}$$

and

$$\begin{aligned} (b-c)a &= (b+(-c))a \\ &= ba + (-c)a \\ &= ba + (-(ca)) \\ &= ba - ca \end{aligned}$$

We prove 3.
Let $a, b \in R$.
Suppose $a = b$.
Then $a - b = a + (-b) = b + (-b) = 0$. Therefore, $a - b = 0$.
Conversely, suppose $a - b = 0$.
Then

$$\begin{aligned} a + (-a) &= 0 \\ &= a - b \\ &= a + (-b). \end{aligned}$$

Hence, $a + (-a) = a + (-b)$. By the left additive cancellation law, we have $-a = -b$. Thus,

$$\begin{aligned} a &= -(-a) \\ &= -(-b) \\ &= b. \end{aligned}$$

Therefore, $a = b$.

We prove 4.

Let $a, b \in R$.

Observe that

$$\begin{aligned} -(a+b) &= (-1)(a+b) \\ &= (-1)a + (-1)b \\ &= -a - b. \end{aligned}$$

We prove 5.

Observe that

$$\begin{aligned} a-(b-c) &= a+(-(b-c)) \\ &= a+(-(b+(-c))) \\ &= a+(-b-(-c)) \\ &= a+((-b)+c) \\ &= (a+(-b))+c \\ &= (a-b)+c. \end{aligned}$$

□

Proposition 9. *The multiplicative inverse of each unit of a ring is unique.*

Proof. Let $(R, +, \cdot)$ be a ring with multiplicative identity $1 \neq 0$.

Suppose a is a unit of R.

We must prove a has a multiplicative inverse and the multiplicative inverse of a is unique.

Existence:

Since a is a unit, then there exists $b \in R$ such that $ab = ba = 1$. Hence, b is a multiplicative inverse of a. Therefore, at least one multiplicative inverse of a exists in R.

Uniqueness:

Since $(R, +, \cdot)$ is a ring with unity, then $\cdot$ is a binary operation on R and multiplication is associative and there is a multiplicative identity in R. Therefore, $(R, \cdot)$ is an associative binary structure with identity. Hence, the inverse of each invertible element is unique.

Since b is a multiplicative inverse of a, then a is invertible. Thus, the inverse of a is unique. Therefore, b is unique. □

Proposition 10. *The zero element of a ring is not a unit.*

Proof. Let 0 be the zero of a ring $(R, +, \cdot)$ with unity $1 \neq 0$. To prove 0 is not a unit, suppose 0 is a unit. Then there exists $b \in R$ such that $0b = 1$. Since $0a = 0$ for all $a \in R$, then in particular, $0b = 0$. Thus, $1 = 0b = 0$, so $1 = 0$. Therefore, we have $1 \neq 0$ and $1 = 0$, a contradiction. Hence, 0 is not a unit. □

Proposition 11. *In any ring the additive inverse of the additive identity element equals itself.*

Proof. Let R be a ring. Let 0 be the additive identity of R.

We must prove $-0 = 0$.

Since 0 is the additive identity of R and $0 \in R$, then $0 + 0 = 0$. Hence, 0 is the additive inverse of 0. Therefore, $-0 = 0$. $\square$

Proposition 12. *In any nonzero ring the multiplicative inverse of the multiplicative identity element equals itself.*

Proof. Let R be a nonzero ring. Let 1 be the multiplicative identity of R.

We must prove $1^{-1} = 1$.

Since 1 is the multiplicative identity of R and $1 \in R$, then $1 \cdot 1 = 1$. Hence, 1 is the multiplicative inverse of 1. Therefore, $1^{-1} = 1$. $\square$

Proposition 13. *In any ring $-x = 0$ iff $x = 0$.*

Proof. Let R be a ring. Let $x \in R$.

We must prove $-x = 0$ iff $x = 0$.

We prove if $-x = 0$, then $x = 0$.

Suppose $-x = 0$. Then

$$\begin{aligned} x &= x + 0 \\ &= x + (-x) \\ &= 0. \end{aligned}$$

Therefore, $x = 0$.

Conversely, we prove if $x = 0$, then $-x = 0$.

Suppose $x = 0$. Then $-x = -0 = 0$. Therefore, $-x = 0$. $\square$

Theorem 14. *The set of all units of a ring is a multiplicative group.*

Proof. Let $(R, +, \cdot)$ be a ring with unity $1 \neq 0$. Let S be the set of all units of R.

Then $S = \{x \in R : x \text{ is a unit }\}$, so $S \subset R$.

We prove S is closed under $\cdot$ of R.

Let $a, b \in S$. Then $a \in R$ and $b \in R$ and a and b are units. Hence, there exist elements $a^{-1} \in R$ and $b^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$ and $bb^{-1} = b^{-1}b = 1$. Since R is closed under multiplication, then $ab \in R$ and $b^{-1}a^{-1} \in R$. Observe that

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= a1a^{-1} \\ &= aa^{-1} \\ &= 1 \\ &= b^{-1}b \\ &= b^{-1}1b \\ &= b^{-1}(a^{-1}a)b \\ &= (b^{-1}a^{-1})(ab). \end{aligned}$$

Since $b^{-1}a^{-1} \in R$ and $(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)$, then ab is a unit. Since $ab \in R$ and ab is a unit, then $ab \in S$. Therefore, S is closed under multiplication in R. Since multiplication is a binary operation on R and $a, b \in R$, then ab is unique. Hence, multiplication is a binary operation on S.

Associativity of multiplication holds in S since $S \subset R$.

We prove 1 is a multiplicative identity of S under $\cdot$ of R.

Let $a \in S$. Since $S \subset R$, then $a \in R$. Since 1 is the multiplicative identity of R, then $1a = a1 = a$. Hence, $1a = a1 = a$ for all $a \in S$.

Since $1 \in R$ and $1 \cdot 1 = 1$, then 1 is a unit, so $1 \in S$. Therefore, there exists $1 \in S$ such that $1a = a1 = a$ for all $a \in S$.

Hence, 1 is an identity for $\cdot$ in S.

We prove each element of S has a multiplicative inverse in S.

Let $a \in S$. To prove a has a multiplicative inverse in S, we must prove there exists $b \in S$ such that $ab = ba = 1$.

Since $a \in S$, then a is a unit. Hence, there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. Since $a \in S$ and $S \subset R$, then $a \in R$. Thus, $a \in R$ and $a^{-1}a = aa^{-1} = 1$, so a^{-1} is a unit. Since $a^{-1} \in R$ and a^{-1} is a unit, then $a^{-1} \in S$.

Let $b = a^{-1}$. Then $b \in S$ and $ab = ba = 1$. Hence, a has a multiplicative inverse in S. Thus, every element of S has a multiplicative inverse in S.

Therefore, $(S, \cdot)$ is a multiplicative group. $\square$

Division Rings

Proposition 15. ***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 $\frac{a}{c} - \frac{b}{c} = \frac{a-b}{c}$.*

Proof. We prove 1.

Suppose $a \neq 0$.

Then the multiplicative inverse a^{-1} exists in R.

Observe that $a^{-1} = 1 \cdot a^{-1} = \frac{1}{a}$.

We prove 2.

Suppose $a \neq 0$.

Since R is a division ring, then every nonzero element of R is a unit. Hence, a is a unit, so a has a multiplicative inverse in R. Thus, there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. Hence, $a^{-1}a = aa^{-1} = 1$. Thus, a is a multiplicative inverse of a^{-1}, so a^{-1} is a unit. Since the multiplicative inverse of each unit of a ring is unique, then the multiplicative inverse of a^{-1} is unique. Therefore, $(a^{-1})^{-1} = a$.

We prove 3.

Suppose $a = b$ and $b \neq 0$. Then $\frac{a}{b} = ab^{-1} = bb^{-1} = 1$. Therefore, $\frac{a}{b} = 1$.

Conversely, suppose $\frac{a}{b} = 1$.

Then $1 = \frac{a}{b} = ab^{-1}$, so $b \neq 0$. Observe that

$$\begin{aligned} a &= a \cdot 1 \\ &= a(b^{-1}b) \\ &= (ab^{-1})b \\ &= \frac{a}{b} \cdot b \\ &= 1 \cdot b \\ &= b. \end{aligned}$$

Therefore, $a = b$.

We prove 4.

Suppose $a \neq 0$ and $b \neq 0$.

Then

$$\begin{aligned} 1 &= aa^{-1} \\ &= a \cdot 1 \cdot a^{-1} \\ &= a(b^{-1}b)a^{-1} \\ &= (ab^{-1})(ba^{-1}) \\ &= \frac{a}{b} \cdot \frac{b}{a}. \end{aligned}$$

and

$$\begin{aligned} 1 &= bb^{-1} \\ &= b \cdot 1 \cdot b^{-1} \\ &= b(a^{-1}a)b^{-1} \\ &= (ba^{-1})(ab^{-1}) \\ &= \frac{b}{a} \cdot \frac{a}{b}. \end{aligned}$$

Hence, $\frac{a}{b} \cdot \frac{b}{a} = 1 = \frac{b}{a} \cdot \frac{a}{b}$, so $\frac{b}{a}$ is the multiplicative inverse of $\frac{a}{b}$. Therefore, $(\frac{a}{b})^{-1} = \frac{b}{a}$.

We prove 5.

Suppose $c \neq 0$.

Then

$$\begin{aligned} \frac{a}{c} + \frac{b}{c} &= ac^{-1} + bc^{-1} \\ &= (a+b)c^{-1} \\ &= \frac{a+b}{c}. \end{aligned}$$

Therefore, $\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$.

We prove 6.

Suppose $c \neq 0$.

Then

$$\begin{aligned}\frac{a}{c} - \frac{b}{c} &= ac^{-1} - bc^{-1} \\ &= (a-b)c^{-1} \\ &= \frac{a-b}{c}.\end{aligned}$$

Therefore, $\frac{a}{c} - \frac{b}{c} = \frac{a-b}{c}$. $\square$

Subrings

Theorem 16. *Let $(R, +, *)$ be a ring.*

Let $S \subset R$.

Then S is a subring of R iff

1. $S \neq \emptyset$.

2. $(\forall a, b \in S)(a - b \in S)$.

3. $(\forall a, b \in S)(ab \in S)$.

4. S has the same multiplicative identity as R.

Proof. Suppose S is a subring of R. Then S is a subset of R and $(S, +, *)$ is a ring under the induced operations of addition and multiplication in R and S has the same multiplicative identity as R. Since S is a ring, then S must contain the zero element of R. Hence, $S \neq \emptyset$.

Let $a, b \in S$. Since S is an additive group, then $-b \in S$. Since S is a group, then S is closed under addition. Hence, $a + (-b) \in S$, so $a - b \in S$.

Since S is a ring, then multiplication is a binary operation on S. Hence, S is closed under multiplication, so $ab \in S$.

Conversely, suppose all of the criteria are satisfied by S. By assumption, $S \neq \emptyset$ and for every $a, b \in S, a - b \in S$. Hence, by the subgroup test, $(S, +)$ is a subgroup of $(R, +)$. Since addition is commutative in R and S is closed under addition, then addition is commutative when restricted to S. Thus, S is abelian, so $(S, +)$ is an abelian group.

By assumption, for every $a, b \in S$, $ab \in S$. Therefore, S is closed under multiplication. Let $a, b \in S$. Then $ab \in S$. Since $a, b \in S$ and $S \subset R$, then $a, b \in R$. Since multiplication is a binary operation on R, then ab is unique. Thus, multiplication is a binary operation on S, since $ab \in S$ and ab is unique.

Since multiplication is associative in R and S is closed under multiplication, then multiplication is associative when restricted to S. Since multiplication is left and right distributive over addition in R and S is closed under multiplication and addition, then multiplication is left and right distributive over addition when restricted to S.

Therefore, $(S, +, *)$ is a ring.

Since S is a subset of R, and S is a ring under the induced operations of addition and multiplication of R, and S has the same multiplicative identity as R, then S is a subring of R. $\square$

Integral Domains

Proposition 17. *A unit of a ring cannot be a zero divisor.*

Proof. Let R be a ring.
Let a be a unit of R.
Then R is a ring with unity and a has a multiplicative inverse.
Let e be the unity element of R.
Let b be the multiplicative inverse of a.
Then $b \in R$ and $ab = ba = e$.

We must prove a cannot be a zero divisor.
Suppose for the sake of contradiction that a is a zero divisor of R.
Then R is a commutative ring and there exists $c \in R$ such that $c \neq 0$ and $ac = 0$.
Observe that

$$\begin{aligned}(b+c)a &= a(b+c)\\ &= ab+ac\\ &= e+0\\ &= e.\end{aligned}$$

Thus, $a(b+c) = (b+c)a = e$, so $b+c$ is a multiplicative inverse of a.
The multiplicative inverse of each unit in a ring is unique.
Hence, $b + c = b = b + 0$.
By additive cancellation for rings, $c = 0$.
Thus, we have $c \neq 0$ and $c = 0$, a contradiction.
Therefore, a cannot be a zero divisor. $\square$

Proposition 18. *A zero divisor of a ring cannot be a unit.*

Proof. Let R be a ring.
Let a be a zero divisor of R.
Then R is a commutative ring and $a \neq 0$ and there exists $b \in R$ such that $b \neq 0$ and $ab = 0$.

We must prove a cannot be a unit.
Suppose for the sake of contradiction that a is a unit.
Then R is a ring with unity and a has a multiplicative inverse.
Let e be the unity of R and let c be the multiplicative inverse of a.
Then $c \in R$ and $ac = ca = e$.

Observe that

$$
\begin{aligned}
(b+c)a &= a(b+c)\\
&= ab+ac\\
&= 0+e\\
&= e.
\end{aligned}
$$

Thus, $a(b+c) = (b+c)a = e$, so $b+c$ is a multiplicative inverse of a.
The multiplicative inverse of each unit in a ring is unique.
Hence, $b+c = c$.
Thus, $c+b = c+0$, so by additive cancellation for rings, $b = 0$.
Hence, $b = 0$ and $b \neq 0$, a contradiction.
Therefore, a cannot have a multiplicative inverse. □

Proposition 19. $(\mathbb{Z}_p, +, \cdot)$ ***is an integral domain.***
Let p be prime and $[a], [b] \in (\mathbb{Z}_p, +, \cdot)$.
If $[a][b] = 0$, then $[a] = 0$ or $[b] = 0$.

Proof. Suppose $[a][b] = [0]$.
Then $[ab] = [0]$ so $ab \equiv 0 \pmod{p}$.
Thus, $p|ab - 0$, so $p|ab$.
Since p is prime and $p|ab$ then we know by Euclid's lemma either $p|a$ or $p|b$ (or both).
We consider these cases separately.
Case 1: Suppose $p|a$.
Then $p|a-0$ so $a \equiv 0 \pmod{p}$.
Therefore, $[a] = [0]$.
Case 1: Suppose $p|b$.
Then $p|b-0$ so $b \equiv 0 \pmod{p}$.
Therefore, $[b] = [0]$.
Hence, either $[a] = [0]$ or $[b] = [0]$. □

Theorem 20. ***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 $a = b$.

Proof. We prove if D is an integral domain, then for all $a, b, c \in D$, if $ca = cb$ and $c \neq 0$, then $a = b$.
Suppose D is an integral domain.
Let $a, b, c \in D$ such that $ca = cb$ and $c \neq 0$.
Then

$$
\begin{aligned}
0 &= ca + (-ca)\\
&= ca - ca\\
&= ca - cb\\
&= c(a-b).
\end{aligned}
$$

Since $c(a-b)=0$ and D is an integral domain, then either $c=0$ or $a-b=0$.
Since $c \neq 0$, then $a-b=0$.
Therefore, $a=b$. □

Proof. Conversely, we prove if $ca=cb$ and $c \neq 0$, then $a=b$ for all $a,b,c \in D$, then D is an integral domain.

Suppose $ca=cb$ and $c \neq 0$ implies $a=b$ for every $a,b,c \in D$.

To prove D is an integral domain, we need only prove D has no divisors of zero since D is a commutative ring with nonzero unity.

To prove D has no zero divisors, we prove the product of two nonzero elements of D is nonzero.

Let x and y be arbitrary nonzero elements of D.
Then $x \in D$ and $y \in D$ and $x \neq 0$ and $y \neq 0$.
To prove $xy \neq 0$, suppose $xy=0$.
Since D is a ring, then $x0 = 0 = xy$.
Therefore, $x0 = xy$.
Since $x0 = xy$ and $x \neq 0$, then by hypothesis, $0 = y$.
Therefore, $y = 0$.
Hence, we have $y \neq 0$ and $y = 0$, a contradiction.
Therefore, $xy \neq 0$, as desired. □

Ideals

Proposition 21. *Let R be a ring.*
The zero ring and R itself are ideals in R.

Proof. We prove the zero ring $\{0\}$ is an ideal of R.
Observe that $\{0\}$ is an abelian subgroup of $(R,+)$.
Let $I = \{0\}$.
We prove $Rx \subset I$ and $xR \subset I$ for all $x \in I$. Let $x = 0$.

Let $a \in Rx$. Then $a = rx = r0 = 0$ for some $r \in R$. Thus, $a \in I$. Hence, $a \in Rx$ implies $a \in I$, so $Rx \subset I$.

Let $b \in xR$. Then $b = xr = 0r = 0$ for some $r \in R$. Thus, $b \in I$. Hence, $b \in xR$ implies $b \in I$, so $xR \subset I$.

Since $(I,+)$ is an additive subgroup of $(R,+)$ and $Rx \subset I$ and $xR \subset I$, then I is an ideal of R. Hence, the zero subring of R is an ideal of R.

We prove R is an ideal of R.
By definition of subring, $(R,+)$ is an abelian subgroup of $(R,+)$.
Let $I = R$.
We prove $Rx \subset I$ and $xR \subset I$ for all $x \in I$.
Let $x \in I$. Then $x \in R$.

Let $a \in Rx$. Then $a = rx$ for some $r \in R$. Since R is a ring, then R is closed under multiplication. Since$r, x \in R$, then this implies $a \in R$. Since $R = I$, then $a \in I$. Hence, $a \in Rx$ implies $a \in I$, so $Rx \subset I$.

Let $b \in xR$. Then $b = xr$ for some $r \in R$. Since R is a ring, then R is closed under multiplication. Since $r, x \in R$, then this implies $b \in R$. Since $R = I$, then $b \in I$. Hence, $b \in xR$ implies $b \in I$, so $xR \subset I$.

Thus, $RI \subset I$ and $IR \subset I$.

Since $(I, +)$ is an abelian subgroup of $(R, +)$ and $RI \subset I$ and $IR \subset I$, then I is an ideal in R. □

Theorem 22. *Let R be a commutative ring. Let $a \in R$. The set $(a) = \{ra : r \in R\}$ is an ideal of R.*

Proof. Let $I = \{ra : r \in R\}$. We prove $(I, +)$ is a subgroup of $(R, +)$.

Let $b \in I$. Then $b = ra$ for some $r \in R$. Since R is a ring, then R is closed under multiplication. Thus, $b \in R$, since $a \in R$ and $r \in R$. Hence, $b \in I$ implies $b \in R$, so $I \subset R$.

Let e be the multiplicative identity of R. Since $e \in R$ and $ea = a$, then $a \in I$, so I is not empty.

Let $x, y \in I$. Then $x = ra$ and $y = r'a$ for some $r, r' \in R$. Thus, $x - y = ra - r'a = (r - r')a$. Since $r - r'$ is an element of R, then $x - y \in I$.

Therefore, $(I, +)$ is a subgroup of $(R, +)$.

We prove $RI \subset I$ and $IR \subset I$. Let $x \in I$. Then $x = ra$ for some $r \in R$.

Let $x' \in Rx$. Then $x' = r'x$ for some $r' \in R$. Thus, $x' = r'(ra) = (r'r)a$. Since $r'r \in R$, then $x' \in I$. Hence, $x' \in Rx$ implies $x' \in I$, so $Rx \subset I$.

Let $y' \in xR$. Then $y' = xs'$ for some $s' \in R$. Thus, $y' = (ra)s' = s'(ra) = (s'r)a$. Since $r, s' \in R$, then $y' \in I$. Hence, $y' \in xR$ implies $y' \in I$, so $xR \subset I$.

Thus, we have $RI \subset I$ and $IR \subset I$.

Since $(I, +) < (R, +)$ and $RI \subset I$ and $IR \subset I$, then I is an ideal of R.

Therefore, (a) is an ideal of R.

The ideal (a) is called the **principal ideal generated by** a **in** R. □

Theorem 23. *Every ideal in the ring $\mathbb{Z}$ is a principal ideal.*

Proof. Let I be an arbitrary ideal of $\mathbb{Z}$.

Since I is an ideal of $\mathbb{Z}$, then $I \subset \mathbb{Z}$ and $(I, +)$ is a subgroup of $(\mathbb{Z}, +)$ and $\mathbb{Z}I \subset I$ and $I\mathbb{Z} \subset I$.

Either I is the zero ring or I is not the zero ring.

We consider these cases separately.

Case 1: Suppose I is the zero ring.

Observe that $(0) = \{k0 : k \in \mathbb{Z}\} = \{0\} = I$. Hence, I is the principal ideal generated by zero.

Case 2: Suppose I is not the zero ring.

Then $(I, +)$ is a group other than the trivial group. Therefore, I contains some nonzero element.

Thus, there exists $k \in I$ such that $k \neq 0$. By definition of ideal, for every $x \in \mathbb{Z}, xk \in I$. Thus, for $x = -1$, $-k \in I$. Hence, both k and $-k$ are in I. Since $I \subset \mathbb{Z}$, then $k \in \mathbb{Z}$ and $-k \in \mathbb{Z}$. Since $k \neq 0$, then either k is positive or $-k$ is positive, by trichotomy of $\mathbb{Z}$. Therefore, I contains some positive integer.

Let M be the set of all positive elements of I. Then $M = \{m \in I : m > 0\}$, so $M \subset I$. Since $M \subset I$ and $I \subset \mathbb{Z}$, then $M \subset \mathbb{Z}$. Since $M \subset \mathbb{Z}$ and every element of M is positive, then $M \subset \mathbb{Z}^+$. By the well ordering principle of $\mathbb{Z}^+$, M contains a least element. Thus, there exists $n \in M$ such that n is the least element of M. Hence, $n \in I$ and $n > 0$.

Let a be an arbitrary element of I. Since $a \in I$ and $I \subset \mathbb{Z}$, then $a \in \mathbb{Z}$. We divide a by n. By the division algorithm, there exist unique integers q, r such that $a = nq + r$ and $0 \leq r < n$. Thus, $r = a - nq = a + (-nq)$. Since $n \in I$, then by definition of ideal, for every $x \in \mathbb{Z}, nx \in I$. In particular, if we let $x = -q$, then we have $-nq \in I$. Since I is an additive group, then I is closed under addition. Thus, $r \in I$, since $a \in I$ and $-nq \in I$.

Either $r > 0$ or $r = 0$.

Suppose $r > 0$. Then $r \in M$, since $r \in I$ and $r > 0$. Since n is the least element of M, then $n \leq r$, so $r \geq n$. Thus, we have $r < n$ and $r \geq n$, a contradiction. Therefore, r cannot be greater than zero, so $r = 0$. Hence, $a = nq$. Thus, $a \in (n)$, by definition of principal ideal. Consequently, $a \in I$ implies $a \in (n)$. Therefore, $I \subset (n)$.

Conversely, let b be an arbitrary element of (n). Then $b = sn$ for some integer s. Since $n \in I$, then by definition of ideal, $sn \in I$. Hence, $b \in I$. Thus, $b \in (n)$ implies $b \in I$, so $(n) \subset I$.

Therefore, $I \subset (n)$ and $(n) \subset I$, so $I = (n)$. Consequently, I is the principal ideal generated by n. $\square$

Quotient Rings

Proposition 24. *Let I be an ideal in a ring R. Then congruence modulo I is an equivalence relation on R.*

Proof. We prove the relation congruence modulo I is reflexive, symmetric, and transitive.

Let $a \in R$. Then $a - a = 0$. Since I is an ideal, then $(I, +)$ is a subgroup of $(R, +)$. Hence, the additive identity of R is in I, so $0 \in I$. Thus, $a - a \in I$, so aRa is true. Therefore, congruence modulo I is reflexive.

Let $a, b \in R$ such that $a \equiv b \pmod{I}$. Then $a - b \in I$. Let 1 be the multiplicative identity of R. Since R is a ring, then $(R, +)$ is a group, so $-1 \in R$. By definition of ideal, for every $x \in R, x(a - b) \in I$. Hence, in particular, if we let $x = -1$, then $(-1)(a - b) = -a + b = b - a \in I$. Thus, $b \cong a \pmod{I}$. Therefore, $a \equiv b \pmod{I}$ implies $b \cong a \pmod{I}$, so congruence modulo I is symmetric.

Let $a, b, c \in R$ such that $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$. Then $a - b \in I$ and $b - c \in I$. Since I is an additive group, then I is closed under addition. Hence, $(a - b) + (b - c) = a - c \in I$. Thus, $a \cong c \pmod{I}$. Therefore, $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$ imply $a \cong c \pmod{I}$, so congruence modulo I is transitive.

Since congruence modulo I is reflexive, symmetric, and transitive, then congruence modulo I is an equivalence relation on R. $\square$

Theorem 25. *Let I be an ideal in a ring R. The set $\frac{R}{I}$ is an abelian group under coset addition.*

Proof. Let $\frac{R}{I}$ to be the collection of all cosets of I in R. Then $\frac{R}{I} = \{a + I : a \in R\}$.

We prove coset addition is well defined.

Let $a+I, b+I, c+I, d+I$ be arbitrary elements of $\frac{R}{I}$ such that $(a+I, b+I) = (c+I, d+I)$. Then $a+I = c+I$ and $b+I = d+I$ and $a, b, c, d \in R$.

We prove $(a+I)+(b+I) = (c+I)+(d+I)$.

Since $a+I = c+I$, then $a \equiv c \pmod I$, so $a-c \in I$. Since $b+I = d+I$, then $b \equiv d \pmod I$, so $b-d \in I$. Since $(I, +)$ is an additive group, then I is closed under addition. Thus, $(a-c)+(b-d) = (a+b)-(c+d) \in I$. Hence, $a+b \equiv c+d \pmod I$, so $(a+b)+I = (c+d)+I$. Therefore, $(a+I)+(b+I) = (c+I)+(d+I)$, by definition of coset addition. Thus, coset addition is well defined, so coset addition is a binary operation on $\frac{R}{I}$.

Let $a+I, b+I$ be arbitrary elements of $\frac{R}{I}$. Then $a, b \in R$ and

$$\begin{aligned}
(a+I)+(b+I) &= (a+b)+I \\
&= (b+a)+I \\
&= (b+I)+(a+I).
\end{aligned}$$

Therefore, coset addition is commutative.

Let $a+I, b+I, c+I$ be arbitrary elements of $\frac{R}{I}$. Then $a, b, c \in R$ and

$$\begin{aligned}
[(a+I)+(b+I)]+(c+I) &= [(a+b)+I]+(c+I) \\
&= [(a+b)+c]+I \\
&= [a+(b+c)]+I \\
&= (a+I)+[(b+c)+I] \\
&= (a+I)+[(b+I)+(c+I)].
\end{aligned}$$

Therefore, coset addition is associative.

Let $a+I$ be an arbitrary element of $\frac{R}{I}$. Then $a \in R$ and

$$\begin{aligned}
(a+I)+I &= (a+I)+(0+I) \\
&= (a+0)+I \\
&= a+I \\
&= (0+a)+I \\
&= (0+I)+(a+I) \\
&= I+(a+I).
\end{aligned}$$

Hence, $I = 0+I$ is an additive identity of $\frac{R}{I}$.

Observe that

$$\begin{aligned}
(a+I)+(-a+I) &= [a+(-a)]+I \\
&= 0+I \\
&= (-a+a)+I \\
&= (-a+I)+(a+I).
\end{aligned}$$

Thus, the additive inverse of $a + I$ is $-a + I$.

Hence, $\frac{R}{I}$ is an abelian group under coset addition. $\square$

Theorem 26. *Let I be an ideal in a ring R. The set $\frac{R}{I}$ is a ring under coset addition and coset multiplication.*

Proof. Let $\frac{R}{I}$ to be the collection of all cosets of I in R. Then $\frac{R}{I} = \{a + I : a \in R\}$.

We proved $\frac{R}{I}$ is an abelian group under coset addition.

We now prove coset multiplication is well defined.

Let $a+I, b+I, c+I, d+I$ be arbitrary elements of $\frac{R}{I}$ such that $(a+I, b+I) = (c + I, d + I)$. Then $a + I = c + I$ and $b + I = d + I$ and $a, b, c, d \in R$.

We prove $(a + I)(b + I) = (c + I)(d + I)$.

Since $a + I = c + I$, then $a \equiv c \pmod{I}$, so $a - c \in I$. Since $b + I = d + I$, then $b \equiv d \pmod{I}$, so $b - d \in I$. Since $(I, +)$ is an additive group, then I is closed under addition. We multiply by b to obtain $(a - c)b = ab - cb$. Since $a - c \in I$ and $b \in R$, then $ab - cb \in I$, by definition of ideal. We multiply by c to obtain $c(b - d) = cb - cd$. Since $b - d \in I$ and $c \in R$, then $cb - cd \in I$, by definition of ideal. Since I is closed under addition, we obtain $(ab - cb) + (cb - cd) = ab - cd \in I$. Hence, $ab \equiv cd \pmod{I}$, so $ab + I = cd + I$. Therefore, $(a + I)(b + I) = (c + I)(d + I)$, by definition of coset multiplication. Thus, coset multiplication is well defined, so coset multiplication is a binary operation on $\frac{R}{I}$.

Let $a + I, b + I, c + I$ be arbitrary elements of $\frac{R}{I}$. Then $a, b, c \in R$ and

$$\begin{aligned}
[(a + I)(b + I)](c + I) &= (ab + I)(c + I) \\
&= (ab)c + I \\
&= a(bc) + I \\
&= (a + I)(bc + I) \\
&= (a + I)[(b + I)(c + I)].
\end{aligned}$$

Therefore, coset multiplication is associative.

Let e be the multiplicative identity of R. Let $a + I$ be an arbitrary element of $\frac{R}{I}$. Then $a \in R$ and

$$\begin{aligned}
(a + I)(e + I) &= ae + I \\
&= a + I \\
&= ea + I \\
&= (e + I)(a + I).
\end{aligned}$$

Hence, $e + I$ is multiplicative identity of $\frac{R}{I}$.

Let $a+I, b+I, c+I$ be arbitrary elements of $\frac{R}{I}$. Then $a, b, c \in R$ and

$$\begin{aligned}
(a+I)[(b+I)+(c+I)] &= (a+I)[(b+c)+I] \\
&= a(b+c)+I \\
&= (ab+ac)+I \\
&= (ab+I)+(ac+I) \\
&= (a+I)(b+I)+(a+I)(c+I).
\end{aligned}$$

Therefore, coset multiplication is left distributive over coset addition.

Observe that

$$\begin{aligned}
[(a+I)+(b+I)](c+I) &= [(a+b)+I](c+I) \\
&= (a+b)c+I \\
&= (ac+bc)+I \\
&= (ac+I)+(bc+I) \\
&= (a+I)(c+I)+(b+I)(c+I).
\end{aligned}$$

Therefore, coset multiplication is right distributive over coset addition.

Hence, $\frac{R}{I}$ is a ring. $\square$

Ring Homomorphisms

Proposition 27. *Let $\phi : R \mapsto R'$ be a ring homomorphism. Then the following are true:*

1. $\phi(0) = 0'$, where 0 is additive identity of R and $0'$ is additive identity of R'.

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.

Proof. We prove 1. Let $a \in R$. Then

$$\begin{aligned}
\phi(a)+0' &= \phi(a) \\
&= \phi(a+0) \\
&= \phi(a)+\phi(0).
\end{aligned}$$

By cancellation in R, we have $0' = \phi(0)$.

We prove 2. Suppose R is a commutative ring. Then for every $a, b \in R, ab = ba$.

Since ϕ is a ring homomorphism, then ϕ is a function and $\phi(a+b) = \phi(a) + \phi(b)$ for every $a, b \in R$. Since R and R' are rings, then $(R, +)$ and $(R', +)$ are abelian groups. Hence, ϕ is a group homomorphism, so ϕ preserves subgroups of R. Thus, if $S < R$, then $\phi(S) < R'$. In particular, $R < R$, so $\phi(R) < R'$. Therefore, $\phi(R)$ is an additive subgroup of R'. Since R' is an abelian additive group, then every additive subgroup of R' is abelian. In particular, $\phi(R)$ is abelian, so $\phi(R)$ is an additive abelian group.

Let $a', b' \in \phi(R)$. Then there exist $a, b \in R$ such that $\phi(a) = a'$ and $\phi(b) = b'$, by definition of $\phi(R)$. By closure of R' under multiplication, $a'b' \in R'$. Let $c = ab$. By closure of R under multiplication, $ab \in R$, so $c \in R$. Observe that

$$\begin{aligned} \phi(c) &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= a'b'. \end{aligned}$$

Thus, there exists $c \in R$ such that $\phi(c) = a'b' \in R'$. Hence, $a'b' \in \phi(R)$, so $\phi(R)$ is closed under multiplication.

Since $a'b' \in R'$ and multiplication is well defined in R', then $a'b'$ is unique. Therefore, multiplication is a binary operation on $\phi(R)$.

Observe that

$$\begin{aligned} a'b' &= \phi(a)\phi(b) \\ &= \phi(ab) \\ &= \phi(ba) \\ &= \phi(b)\phi(a) \\ &= b'a'. \end{aligned}$$

Hence, multiplication is commutative in $\phi(R)$.

Associativity of multiplication in R' holds in $\phi(R)$ since $\phi(R)$ is a subset of R' and $\phi(R)$ is closed under multiplication.

Distributivity of multiplication over addition (left and right) in R' holds in $\phi(R)$ since $\phi(R)$ is a subset of R' and $\phi(R)$ is closed under addition and multiplication.

Since ϕ is a ring homomorphism, then $\phi(1) = 1'$, where 1 is unity of R and $1'$ is unity of R'. Thus, there exists $1 \in R$ such that $\phi(1) = 1'$, so $1' \in \phi(R)$.

Therefore, $\phi(R)$ is a commutative ring.

We prove 3.

Suppose R is a field and $\phi(R) \neq \{0'\}$. Since R is a field, then R is a commutative division ring, so R is a commutative ring. Therefore, $\phi(R)$ is a commutative ring.

Since $\phi(R)$ is a ring and $\phi(R) \neq \{0'\}$, then there exists a nonzero element in $\phi(R)$.

Let $a' \in R'$ and $a' \neq 0'$. Then there exists $a \in R$ such that $\phi(a) = a'$, by definition of $\phi(R)$.

Suppose $a = 0$. Then $a' = \phi(a) = \phi(0) = 0'$, so $a' = 0'$. Thus, we have $a' \neq 0'$ and $a' = 0'$, a contradiction. Therefore, $a \neq 0$.

Since R is a field, then every nonzero element of R is a unit of R. Hence, in particular, a is a unit of R. Therefore, there exists $a^{-1} \in R$ such that $aa^{-1} = 1$, where 1 is unity of R. Let $b' = \phi(a^{-1})$. Then $b' \in R'$. Since $a^{-1} \in R$ and $\phi(a^{-1}) \in R'$, then $b' \in \phi(R)$, by definition of $\phi(R)$.

Let $1'$ be the unity of R'. Observe that

$$\begin{aligned} 1' &= \phi(1) \\ &= \phi(aa^{-1}) \\ &= \phi(a)\phi(a^{-1}) \\ &= a'b' \\ &= b'a'. \end{aligned}$$

Hence, there exists $b' \in \phi(R)$ such that $a'b' = b'a' = 1'$. Therefore, a' is a unit of R'. Thus, every nonzero element of R' is a unit of R', so R' is a field. □

Theorem 28. *Let $\phi : R \mapsto R'$ be a ring homomorphism. Then $\ker(\phi)$ is an ideal in R.*

Proof. Let $0'$ be the additive identity of R'. Let $I = \ker(\phi) = \{r \in R : \phi(r) = 0'\}$.

Since ϕ is a ring homomorphism, then $\phi : R \mapsto R'$ is a function and for all $a, b \in R, \phi(a + b) = \phi(a) + \phi(b)$. Since R and R' are rings, then $(R, +)$ and $(R', +)$ are additive groups. Therefore, ϕ is a group homomorphism. Hence, the kernel of ϕ is a subgroup of $(R, +)$.

Let $x \in I$. Then $x \in R$ and $\phi(x) = 0'$.

Let $x' \in Rx$. Then $x' = rx$ for some $r \in R$. Since R is a ring, then R is closed under multiplication. Thus, $x' \in R$, since $r, x \in R$. Observe that

$$\begin{aligned} \phi(x') &= \phi(rx) \\ &= \phi(r)\phi(x) \\ &= \phi(r)0' \\ &= 0'. \end{aligned}$$

Hence, $x' \in I$, by definition of I. Thus, $x' \in Rx$ implies $x' \in I$, so $Rx \subset I$.

Let $y' \in xR$. Then $y' = xs$ for some $s \in R$. Since R is a ring, then R is closed under multiplication. Thus, $y' \in R$, since $s, x \in R$. Observe that

$$\begin{aligned} \phi(y') &= \phi(xs) \\ &= \phi(x)\phi(s) \\ &= 0'\phi(r) \\ &= 0'. \end{aligned}$$

Hence, $y' \in I$, by definition of I. Thus, $y' \in xR$ implies $y' \in I$, so $xR \subset I$.

Since x is arbitrary, then $RI \subset I$ and $IR \subset I$.

Since $(I, +)$ is a subgroup of $(R, +)$ and $RI \subset I$ and $IR \subset I$, then I is an ideal of R, by definition of ideal.

Therefore, $\ker(\phi)$ is an ideal of R. □

Theorem 29. *Let I be an ideal of a ring R. Let $\eta : R \mapsto \frac{R}{I}$ 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 $\frac{R}{I}$.*

Proof. Since R is a ring, then $(R, +)$ is an abelian group. Since I is an ideal of R, then $(I, +)$ is a subgroup of $(R, +)$. Every subgroup of an abelian group is normal. Since R is abelian, then I is normal in R. Thus, η is the natural group homomorphism from R onto $\frac{R}{I}$. Hence, η is a function and $\eta(a+b) = \eta(a)+\eta(b)$ for every $a, b \in R$ and $\ker(\eta) = I$ and η is surjective.

To prove η is a ring homomorphism, we need only prove multiplication and multiplicative identity are preserved.

Let $a, b \in R$. Then

$$\begin{aligned} \eta(ab) &= (ab) + I \\ &= (a + I)(b + I) \\ &= \eta(a)\eta(b). \end{aligned}$$

Observe that $\eta(e) = e + I$, which is multiplicative identity of $\frac{R}{I}$.

Therefore, η is a ring homomorphism. □

Theorem 30. ***Fundamental Homomorphism Theorem***

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

Proof. By assumption, ϕ is a ring homomorphism. If ϕ is a ring homomorphism, then the kernel of ϕ is an ideal of R. Therefore, K is an ideal of R. Hence, the quotient ring $\frac{R}{K}$ exists and there exists a natural homomorphism from R onto $\frac{R}{K}$. Let $\eta : R \mapsto \frac{R}{K}$ be the natural ring homomorphism defined by $\eta(a) = a + K$ for all $a \in R$.

Since R and R' are rings, then R and R' are additive abelian groups. Since ϕ is a ring homomorphism, then ϕ is a group homomorphism with kernel K. Therefore, by the fundamental group homomorphism theorem, there exists a group isomorphism $\phi' : \frac{R}{K} \mapsto \phi(R)$ defined by $\phi'(r + K) = \phi(r)$ for all $r \in R$ such that $\phi' \circ \eta = \phi$.

Let $x, y \in \frac{R}{K}$. Then there exist $a, b \in R$ such that $x = a + K$ and $y = b + K$. Since ϕ' is a group isomorphism, then ϕ' is a bijective function and $\phi'(x + y) = \phi'(x) + \phi'(y)$. Observe that

$$\begin{aligned} \phi'(xy) &= \phi'[(a + K)(b + K)] \\ &= \phi'[(ab) + K] \\ &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= \phi'(a + K)\phi'(b + K) \\ &= \phi'(x)\phi'(y). \end{aligned}$$

Let e be the unity of R and e' be the unity of R'. Then $\phi'(e + K) = \phi(e) = e'$.

Therefore, ϕ' is a ring homomorphism and $\phi' \circ \eta = \phi$. □

Ring Isomorphisms

Theorem 31. ***First Isomorphism Theorem***

Let H and K be subgroups of a group G such that $K \lhd G$.

Let $HK = \{hk : h \in H \wedge k \in K\}$.

Then HK is a subgroup of G such that $K \lhd HK$ and $\frac{H}{H \cap K} \cong \frac{HK}{K}$.

Solution. We must prove:

1. $HK < G$.
2. $K \lhd HK$.
3. $\frac{H}{H \cap K} \cong \frac{HK}{K}$.

$\square$

Proof. We first prove $HK < G$.

Let $x \in HK$. Then there exists $h \in H$ and $k \in K$ such that $x = hk$. Since $H < G$, then $H \subset G$. Since $h \in H$ and $H \subset G$, then $h \in G$. Since $K < G$, then $K \subset G$. Since $k \in K$ and $K \subset G$, then $k \in G$. Since G is a group, then G is closed under its binary operation. Thus, since $h, k \in G$, then $hk = x \in G$. Therefore, $x \in HK$ implies $x \in G$, so $HK \subset G$.

We apply a subgroup test.

Let e be the identity of G. Since $H < G$, then $e \in H$. Since $K < G$, then $e \in K$. Since $e = ee$, then $e \in HK$, by definition of HK. Therefore, $HK \neq \emptyset$.

Let $a, b \in HK$. Then there exist $h_1 \in H$ and $k_1 \in K$ such that $a = h_1k_1$ and there exist $h_2 \in H$ and $k_2 \in K$ such that $b = h_2k_2$, by definition of HK. Since $a, b \in HK$ and $HK \subset G$, then $a, b \in G$. Thus, $ab^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1k_1k_2^{-1}h_2^{-1}$. Let $k = k_1k_2^{-1}$. Since K is a group, then $k \in K$ and $ab^{-1} = h_1kh_2^{-1}$.

Since $h_2 \in H$ and $H \subset G$, then $h_2 \in G$. Since $K \lhd G$, then for every $g \in G, h \in K, ghg^{-1} \in K$. Thus, in particular, if we let $g = h_2$ and $h = k$, then $h_2kh_2^{-1} \in K$. Let $k_3 = h_2kh_2^{-1}$. Then $k_3 \in K$ and $kh_2^{-1} = h_2^{-1}k_3$, so $ab^{-1} = h_1(h_2^{-1}k_3) = (h_1h_2^{-1})k_3$. Since H is a group, then H is closed under its binary operation. Therefore, since $h_1 \in H$ and $h_2^{-1} \in H$, then $h_1h_2^{-1} \in H$. Since $h_1h_2^{-1} \in H$ and $k_3 \in K$, then $ab^{-1} \in HK$, by definition of HK.

Therefore, HK is a subgroup of G.

We prove K is normal in HK. We first prove K is a subgroup of HK and then prove for every $g \in HK$ and $k \in K$, $gkg^{-1} \in K$.

Let $x \in K$. Then $x = ex$. Since $e \in H$ and $x \in K$, then $x \in HK$, by definition of HK. Thus, $x \in K$ implies $x \in HK$, so $K \subset HK$.

Since $K < G$, then $e \in K$, so $K \neq \emptyset$.

Let $a, b \in K$. Since K is a group, then $b^{-1} \in K$. Since K is closed under its binary operation, then $ab^{-1} \in K$.

Thus, K is a subgroup of HK.

Let $g \in HK$ and $k' \in K$. Then $g = hk$ for some $h \in H$ and $k \in K$. Observe that $gk'g^{-1} = (hk)k'(hk)^{-1} = hkk'k^{-1}h^{-1}$. Let $k'' = kk'k^{-1}$. Then $gk'g^{-1} = hk''h^{-1}$. Since $K \lhd G$, then $hk''h^{-1} \in K$, so $gk'g^{-1} \in K$. Therefore, K is a normal subgroup of HK.

Since K is normal in HK, then the quotient group $\frac{HK}{K}$ exists.

Let $\frac{HK}{K}$ be the set of all cosets of K in HK. Then $\frac{HK}{K} = \{hK : h \in H\}$.

Define binary relation $\phi : H \mapsto \frac{HK}{K}$ by $\phi(h) = hK$ for all $h \in H$.

We prove ϕ is well defined. Let $h_1, h_2 \in H$ such that $h_1 = h_2$. Then $h_1K = h_2K$. Thus, $\phi(h_1) = h_1K = h_2K = \phi(h_2)$. Hence, $h_1 = h_2$ implies $\phi(h_1) = \phi(h_2)$, so ϕ is well defined. Therefore, ϕ is a function.

Let $a, b \in H$. Then $\phi(ab) = (ab)K = (aK)(bK) = \phi(a)\phi(b)$. Thus, ϕ is a homomorphism.

We prove $\ker(\phi) = H \cap K$. Let $x \in \ker(\phi)$. Then $x \in H$ since $\ker(\phi) \subset H$ and $\phi(x) = K$, by definition of kernel of ϕ. Thus, $K = \phi(x) = xK$. Since $xK = K$, then $x \in K$. Since $x \in H$ and $x \in K$, then $x \in H \cap K$. Hence, $x \in \ker(\phi)$ implies $x \in H \cap K$, so $\ker(\phi) \subset H \cap K$.

Let $y \in H \cap K$. Then $y \in H$ and $y \in K$. Since $y \in H$ and $H \subset G$, then $y \in G$. Since $y \in K$, then $yK = K$. Thus, $\phi(y) = yK = K$. Since $y \in H$ and $\phi(y) = K$, then $y \in \ker(\phi)$. Hence, $y \in H \cap K$ implies $y \in \ker(\phi)$, so $H \cap K \subset \ker(\phi)$.

Since $\ker(\phi) \subset H \cap K$ and $H \cap K \subset \ker(\phi)$, then $\ker(\phi) = H \cap K$.

We prove $\phi(H) = \frac{HK}{K}$. Observe that $\phi(H) = \{\phi(h) \in \frac{HK}{K} : h \in H\}$.

Let $x \in \phi(H)$. Then there exists $h \in H$ such that $x = \phi(h)$ and $x \in \frac{HK}{K}$. Thus, $x = \phi(h) = hK$. Since there exists $h \in H$ such that $x = hK$, then $x \in \frac{HK}{K}$, by definition of $\frac{HK}{K}$. Hence, $x \in \phi(H)$ implies $x \in \frac{HK}{K}$, so $\phi(H) \subset \frac{HK}{K}$.

Let $y \in \frac{HK}{K}$. Then there exists $h \in H$ such that $y = hK$. Thus, $\phi(h) = hK = y$. Hence, there exists $h \in H$ such that $y = \phi(h)$, so $y \in \phi(H)$, by definition of $\phi(H)$. Therefore, $y \in \frac{HK}{K}$ implies $y \in \phi(H)$, so $\frac{HK}{K} \subset \phi(H)$.

Since $\phi(H) \subset \frac{HK}{K}$ and $\frac{HK}{K} \subset \phi(H)$, then $\phi(H) = \frac{HK}{K}$.

Hence, $\phi : H \mapsto \frac{HK}{K}$ is a homomorphism with kernel $H \cap K$ and $\phi(H) = \frac{HK}{K}$. Thus, by the fundamental homomorphism theorem, $\frac{H}{H \cap K} \cong \frac{HK}{K}$. □

Direct product of Rings

Theorem 32. *Let $(R, +, *)$ be a ring with unity e. Let $n \in \mathbb{Z}^+, n \geq 2$. Then $(R^n, +, *)$ is a ring with unity $(e, e, ..., e)$.*

Proof. Observe that $R^n = R \times R \times ... \times R = \{(a_1, a_2, ..., a_n) : a_i \in R\}$. Since $(R, +, *)$ is a ring, then $(R, +)$ is an abelian group. Observe that $(R^n, +)$ is the direct sum of the group $(R, +)$ with itself n times. The direct sum of abelian groups is an abelian group. Hence, $(R^n, +)$ is an abelian group.

We prove component wise multiplication is a binary operation over R^n. Let $a, b \in R^n$. Then for each $i \in \{1, 2, ..., n\}$ there exist $a_i, b_i \in R$ such that $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$. Observe that

$$\begin{aligned} ab &= (a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) \\ &= (a_1b_1, a_2b_2, ..., a_nb_n). \end{aligned}$$

Since R is a ring, then R is closed under multiplication, so $a_ib_i \in R$ for each i. Therefore, $ab \in R^n$, so R^n is closed under componentwise multiplication.

We prove componentwise multiplication is well defined. Let (a, b) and (c, d) be arbitrary elements of $R^n \times R^n$ such that $(a, b) = (c, d)$. Then $a, b, c, d \in R^n$ and $a = c$ and $b = d$. Hence, for each $i = 1, 2, ..., n$ there exist $a_i, b_i, c_i, d_i \in R$ such that $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$ and $c = (c_1, c_2, ..., c_n)$ and $d = (d_1, d_2, ..., d_n)$ and $a_i = c_i$ and $b_i = d_i$ for each i. Thus,

$$\begin{aligned}
ab &= (a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) \\
&= (a_1 b_1, a_2 b_2, ..., a_n b_n) \\
&= (c_1 b_1, c_2 b_2, ..., c_n b_n) \\
&= (c_1 d_1, c_2 d_2, ..., c_n d_n) \\
&= (c_1, c_2, ..., c_n)(d_1, d_2, ..., d_n) \\
&= cd.
\end{aligned}$$

Hence, $ab = cd$, so componentwise multiplication is well defined over R^n. Therefore, componentwise multiplication is a binary operation on R^n.

We prove componentwise multiplication is associative. Let $a, b, c \in R^n$. Then for each $i = 1, 2, ..., n$ there exist $a_i, b_i, c_i \in R$ such that $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$ and $c = (c_1, c_2, ..., c_n)$. Observe that

$$\begin{aligned}
(ab)c &= [(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n)](c_1, c_2, ..., c_n) \\
&= (a_1 b_1, a_2 b_2, ..., a_n b_n)(c_1, c_2) \\
&= ((a_1 b_1)c_1, (a_2 b_2)c_2, ..., (a_n b_n)c_n) \\
&= (a_1(b_1 c_1), a_2(b_2 c_2), ..., a_n(b_n c_n)) \\
&= (a_1, a_2, ..., a_n)(b_1 c_1, b_2 c_2, ..., b_n c_n) \\
&= (a_1, a_2, ..., a_n)[(b_1, b_2, ..., b_n)(c_1, c_2, ..., c_n)] \\
&= a(bc).
\end{aligned}$$

Therefore, componentwise multiplication is associative.

Observe that

$$\begin{aligned}
(a_1, a_2, ..., a_n)(e, e, ..., e) &= (a_1 e, a_2 e, ..., a_n e) \\
&= (a_1, a_2, ..., a_n) \\
&= (e a_1, e a_2, ..., e a_n) \\
&= (e, e, ...e)(a_1, a_2, ..., a_n).
\end{aligned}$$

Therefore, $(e, e, ..., e)$ is a multiplicative identity in R^n, so a multiplicative identity exists in R^n.

Observe that

$$\begin{aligned}
a(b+c) &= (a_1, a_2, ..., a_n)[(b_1, b_2, ..., b_n) + (c_1, c_2, ..., c_n)] \\
&= (a_1, a_2, ..., a_n)(b_1 + c_1, b_2 + c_2, ..., b_n + c_n) \\
&= (a_1(b_1 + c_1), a_2(b_2 + c_2), ..., a_n(b_n + c_n)) \\
&= (a_1 b_1 + a_1 c_1, a_2 b_2 + a_2 c_2, ..., a_n b_n + a_n c_n) \\
&= (a_1 b_1, a_2 b_2, ..., a_n b_n) + (a_1 c_1, a_2 c_2, ..., a_n c_n) \\
&= (a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) + (a_1, a_2, ..., a_n)(c_1, c_2, ..., c_n) \\
&= ab + ac
\end{aligned}$$

and

$$\begin{aligned}
(a+b)c &= [(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n)](c_1, c_2, ..., c_n) \\
&= (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)(c_1, c_2, ..., c_n) \\
&= ((a_1 + b_1)c_1, (a_2 + b_2)c_2, ..., (a_n + b_n)c_n) \\
&= (a_1 c_1 + b_1 c_1, a_2 c_2 + b_2 c_2, ..., a_n c_n + b_n c_n) \\
&= (a_1 c_1, a_2 c_2, ..., a_n c_n) + (b_1 c_1, b_2 c_2, ..., b_n c_n) \\
&= (a_1, a_2, ..., a_n)(c_1, c_2, ..., c_n) + (b_1, b_2, ..., b_n)(c_1, c_2, ..., c_n) \\
&= ac + bc
\end{aligned}$$

Therefore, the left and right distributive laws hold in R^n.

Hence, $(R^n, +, *)$ is a ring with unity $(e, e, ..., e)$. □

Theorem 33. *Let $(R, +, *)$ be a commutative ring. Then $(R^n, +, *)$ is a commutative ring.*

Proof. Let $n \in \mathbb{Z}^+, n \geq 2$. Let R^n be the direct product of n copies of the ring R. The direct product of n copies of a ring is a ring. Therefore, $(R^n, +, *)$ is a ring.

Let $a, b \in R^n$. Then for each $i \in \{1, 2, ..., n\}$ there exist $a_i, b_i \in R^n$ such that $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$. Observe that

$$\begin{aligned}
ab &= (a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) \\
&= (a_1 b_1, a_2 b_2, ..., a_n b_n) \\
&= (b_1 a_1, b_2 a_2, ..., b_n a_n) \\
&= (b_1, b_2, ..., b_n)(a_1, a_2, ..., a_n) \\
&= ba.
\end{aligned}$$

Therefore, component wise multiplication in R^n is commutative. Hence, $(R^n, +, *)$ is a commutative ring. □