Modern Algebra I

Lecture 15

Jung-Chen Liu

liujc@math.ntnu.edu.tw

2009, Fall

Chapter III: Rings

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations,

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "*$+$*"*

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",*

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$,

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.
- If $(R, +, \cdot)$ is a ring and

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.
- If $(R, +, \cdot)$ is a ring and $\exists 1_R \in R$ such that $\forall a \in R$, $1_R a = a 1_R = a$,

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.
- If $(R, +, \cdot)$ is a ring and $\exists 1_R \in R$ such that $\forall a \in R$, $1_R a = a 1_R = a$, then R is said to be a **ring with identity**.

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.
- If $(R, +, \cdot)$ is a ring and $\exists 1_R \in R$ such that $\forall a \in R$, $1_R a = a 1_R = a$, then R is said to be a **ring with identity**.

Theorem (1.2)

Let R be a ring. Then

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,
- $(na)b = a(nb) = n(ab), \forall n \in \mathbb{Z}$ and $\forall a, b \in R$,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,
- $(na)b = a(nb) = n(ab), \forall n \in \mathbb{Z}$ and $\forall a, b \in R$,
- $(\sum_{i=1}^{n} a_i)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j, \forall a_i, b_j \in R$.

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor
  if $\exists b \in R \setminus \{0\}$ such that $ab = 0$

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ *such that* $ab = 0$,

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor and b is a right zero divisor.

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor and b is a right zero divisor.
- a is called a **zero divisor**

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor and b is a right zero divisor.
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor and b is a right zero divisor.
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor and b is a right zero divisor.
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R,

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor and b is a right zero divisor.
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$,

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor and b is a right zero divisor.
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$, $ab = ac$ or $ba = ca$

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
  In other words, if $a, b \in R \setminus \{0\}$ such that $ab = 0$, then a is a left zero divisor and b is a right zero divisor.
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$, $ab = ac$ or $ba = ca \implies b = c$.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible
  if $\exists b \in R$ such that $ba = 1_R$

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible
  if $\exists b \in R$ such that $ba = 1_R$
  The element b is called a left inverse of a.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible)
  if $\exists b \in R$ such that $ba = 1_R$
  The element b is called a left inverse of a.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left inverse of a.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit**

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible,

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

$$a_L^{-1} = a_L^{-1}1_R = a_L^{-1}(aa_R^{-1}) = (a_L^{-1}a)a_R^{-1} = 1_R a_R^{-1} = a_R^{-1}.$$

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

(ii) The set of units in a ring R with identity,

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

(ii) The set of units in a ring R with identity, denoted by $U(R)$,

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

(ii) The set of units in a ring R with identity, denoted by $U(R)$, is a group under multiplication.

Definition (1.5)

Let R be a ring.

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,
  - every nonzero element of R is a unit.

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,
  - every nonzero element of R is a unit.
- R is called a **field**

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,
  - every nonzero element of R is a unit.
- R is called a **field** if it is a commutative division ring.

Definition (1.5)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,
  - every nonzero element of R is a unit.
- R is called a **field** if it is a commutative division ring.

Remark. A field is a commutative ring with an identity $1_R \neq 0$ such that every nonzero element is a unit.

Remark

- A ring R with identity is a division ring

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit,

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit, then R has no zero divisors.

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit, then R has no zero divisors. More precisely,

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit, then R has no zero divisors. More precisely, suppose $a \in R \setminus \{0\}$.

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit, then R has no zero divisors. More precisely, suppose $a \in R \setminus \{0\}$. Then $a^{-1} \in R$.

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit, then R has no zero divisors. More precisely, suppose $a \in R \setminus \{0\}$. Then $a^{-1} \in R$. If $ab = 0$ for some $b \in R$,

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit, then R has no zero divisors. More precisely, suppose $a \in R \setminus \{0\}$. Then $a^{-1} \in R$. If $ab = 0$ for some $b \in R$, then
$a^{-1}ab = a^{-1}0 \Rightarrow b = 0$;

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit, then R has no zero divisors. More precisely, suppose $a \in R \setminus \{0\}$. Then $a^{-1} \in R$. If $ab = 0$ for some $b \in R$, then $a^{-1}ab = a^{-1}0 \Rightarrow b = 0$; if $ba = 0$ for some $b \in R$,

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

This is because if every nonzero element of R is a unit, then R has no zero divisors. More precisely, suppose $a \in R \setminus \{0\}$. Then $a^{-1} \in R$. If $ab = 0$ for some $b \in R$, then $a^{-1}ab = a^{-1}0 \Rightarrow b = 0$; if $ba = 0$ for some $b \in R$, then $baa^{-1} = 0a^{-1} \Rightarrow b = 0$.

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Example. For $n \in \mathbb{N}$,

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Example. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a commutative ring with identity $\overline{1}$

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Example. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a commutative ring with identity $\overline{1}$ and $U(\mathbb{Z}_n) = \{\overline{i} \in \mathbb{Z}_n \mid gcd(i, n) = 1\}$.

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Example. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a commutative ring with identity $\overline{1}$ and $U(\mathbb{Z}_n) = \{\overline{i} \in \mathbb{Z}_n \mid gcd(i, n) = 1\}$. This is because

$$gcd(i, n) = 1$$

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Example. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a commutative ring with identity $\overline{1}$ and $U(\mathbb{Z}_n) = \{\overline{i} \in \mathbb{Z}_n \mid gcd(i, n) = 1\}$. This is because

$$gcd(i, n) = 1 \iff \exists s, t \in \mathbb{Z} \text{ such that } si + tn = 1$$

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Example. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a commutative ring with identity $\overline{1}$ and $U(\mathbb{Z}_n) = \{\overline{i} \in \mathbb{Z}_n \mid gcd(i,n) = 1\}$. This is because

$$\begin{aligned} gcd(i,n) = 1 &\iff \exists s,t \in \mathbb{Z} \text{ such that } si + tn = 1 \\ &\iff \exists \overline{s} \in \mathbb{Z}_n \text{ such that } \overline{s}\overline{i} = \overline{1} \text{ in } \mathbb{Z}_n. \end{aligned}$$

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Example. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a commutative ring with identity $\overline{1}$ and $U(\mathbb{Z}_n) = \{\overline{i} \in \mathbb{Z}_n \mid gcd(i,n) = 1\}$. This is because

$$\begin{aligned} gcd(i,n) = 1 &\iff \exists s,t \in \mathbb{Z} \text{ such that } si + tn = 1 \\ &\iff \exists \overline{s} \in \mathbb{Z}_n \text{ such that } \overline{s}\overline{i} = \overline{1} \text{ in } \mathbb{Z}_n. \end{aligned}$$

Hence $\mathbb{Z}_n$ is a field

Remark

- A ring R with identity is a division ring if and only if the nonzero elements of R form a group under multiplication.
- Every field is an integral domain.

Example. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a commutative ring with identity $\overline{1}$ and $U(\mathbb{Z}_n) = \{\overline{i} \in \mathbb{Z}_n \mid gcd(i,n) = 1\}$. This is because

$$\begin{aligned} gcd(i,n) = 1 &\iff \exists s,t \in \mathbb{Z} \text{ such that } si + tn = 1 \\ &\iff \exists \overline{s} \in \mathbb{Z}_n \text{ such that } \overline{s}\overline{i} = \overline{1} \text{ in } \mathbb{Z}_n. \end{aligned}$$

Hence $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring.

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates,

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$.

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$.

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,
- some g_i are repeated.

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,
- some g_i are repeated.

With this notation,

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,
- some g_i are repeated.

With this notation,

- the addition in $R(G)$ is given by

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,
- some g_i are repeated.

With this notation,

- the addition in $R(G)$ is given by

$$\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i$$

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,
- some g_i are repeated.

With this notation,

- the addition in $R(G)$ is given by

$$\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i}) g_i$$

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,
- some g_i are repeated.

With this notation,

- The multiplication in $R(G)$ is given by

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,
- some g_i are repeated.

With this notation,

- The multiplication in $R(G)$ is given by

$$\left(\sum_{i=1}^{n} r_{g_i} g_i \right) \cdot \left(\sum_{j=1}^{m} s_{h_j} h_j \right)$$

Group Rings

Example. Let G be a (multiplicative) group and let R be a ring. Consider the additive abelian group $R(G) = \sum_{g \in G} R$.
Note that every element $x = (r_g)_{g \in G}$ of $R(G)$ has only finitely many nonzero coordinates, say $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$. Denote x by the formal sum $r_{g_1} g_1 + r_{g_2} g_2 + \cdots + r_{g_n} g_n$ or $\sum_{i=1}^{n} r_{g_i} g_i$. We also allow the possibility that

- some of the r_{g_i} are zero,
- some g_i are repeated.

With this notation,

- The multiplication in $R(G)$ is given by

$$\left(\sum_{i=1}^{n} r_{g_i} g_i \right) \cdot \left(\sum_{j=1}^{m} s_{h_j} h_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_{g_i} s_{h_j})(g_i h_j)$$

Group Rings

- The addition in $R(G)$ is given by

$$\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i}) g_i$$

- The multiplication in $R(G)$ is given by

$$\left(\sum_{i=1}^{n} r_{g_i} g_i \right) \cdot \left(\sum_{j=1}^{m} s_{h_j} h_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_{g_i} s_{h_j})(g_i h_j)$$

Group Rings

- The addition in $R(G)$ is given by

$$\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i}) g_i$$

- The multiplication in $R(G)$ is given by

$$\left(\sum_{i=1}^{n} r_{g_i} g_i \right) \cdot \left(\sum_{j=1}^{m} s_{h_j} h_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_{g_i} s_{h_j})(g_i h_j)$$

With these operations, $R(G)$ is a ring and is called

Group Rings

- The addition in $R(G)$ is given by

$$\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i}) g_i$$

- The multiplication in $R(G)$ is given by

$$\left(\sum_{i=1}^{n} r_{g_i} g_i \right) \cdot \left(\sum_{j=1}^{m} s_{h_j} h_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_{g_i} s_{h_j})(g_i h_j)$$

With these operations, $R(G)$ is a ring and is called the **group ring of G over R**.

Group Rings

- The addition in $R(G)$ is given by

$$\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i}) g_i$$

- The multiplication in $R(G)$ is given by

$$\left(\sum_{i=1}^{n} r_{g_i} g_i \right) \cdot \left(\sum_{j=1}^{m} s_{h_j} h_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_{g_i} s_{h_j})(g_i h_j)$$

With these operations, $R(G)$ is a ring and is called the **group ring of G over R**.

- $R(G)$ is commutative if and only if both R and G are commutative.

Group Rings

- The addition in $R(G)$ is given by

$$\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i}) g_i$$

- The multiplication in $R(G)$ is given by

$$\left(\sum_{i=1}^{n} r_{g_i} g_i \right) \cdot \left(\sum_{j=1}^{m} s_{h_j} h_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_{g_i} s_{h_j})(g_i h_j)$$

With these operations, $R(G)$ is a ring and is called the **group ring of G over R**.

- If R has an identity 1_R and if e is the identity of G,

Group Rings

- The addition in $R(G)$ is given by

$$\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i}) g_i$$

- The multiplication in $R(G)$ is given by

$$\left(\sum_{i=1}^{n} r_{g_i} g_i \right) \cdot \left(\sum_{j=1}^{m} s_{h_j} h_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_{g_i} s_{h_j})(g_i h_j)$$

With these operations, $R(G)$ is a ring and is called the **group ring of G over R**.

- If R has an identity 1_R and if e is the identity of G, then $1_R e$ is the identity of the ring $R(G)$.

Example

Let $(A, +)$ be an abelian group

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$.

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for $a, b \in A$,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for $a, b \in A$,

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

by the definition of $f + g$

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for $a, b \in A$,

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

because f and g are group homomorphisms

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for $a, b \in A$,

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

because A is an abelian group

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for $a, b \in A$,

$$\begin{aligned} (f+g)(a+b) &= f(a+b)+g(a+b) \\ &= \big(f(a)+f(b)\big)+\big(g(a)+g(b)\big) \\ &= \big(f(a)+g(a)\big)+\big(f(b)+g(b)\big) \\ &= (f+g)(a)+(f+g)(b). \end{aligned}$$

by the definition of $f+g$

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for $a, b \in A$,

$$\begin{aligned} (f+g)(a+b) &= f(a+b)+g(a+b) \\ &= \big(f(a)+f(b)\big)+\big(g(a)+g(b)\big) \\ &= \big(f(a)+g(a)\big)+\big(f(b)+g(b)\big) \\ &= (f+g)(a)+(f+g)(b). \end{aligned}$$

Thus $f+g \in \mathrm{End}A$

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for $a, b \in A$,

$$\begin{aligned} (f+g)(a+b) &= f(a+b)+g(a+b) \\ &= \big(f(a)+f(b)\big)+\big(g(a)+g(b)\big) \\ &= \big(f(a)+g(a)\big)+\big(f(b)+g(b)\big) \\ &= (f+g)(a)+(f+g)(b). \end{aligned}$$

Thus $f+g \in \mathrm{End}A$ and so the addition defined above is indeed a binary operation on $\mathrm{End}A$.

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$.

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$.

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

- $(\mathrm{End}A, +)$ is an abelian group,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative, i.e., the composition of functions is associative,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative, i.e., the composition of functions is associative,
- for all $f, g, h \in \mathrm{End}A$,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative, i.e., the composition of functions is associative,
- for all $f, g, h \in \mathrm{End}A$, $f \circ (g + h) = f \circ g + f \circ h$,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative, i.e., the composition of functions is associative,
- for all $f, g, h \in \mathrm{End}A$, $f \circ (g + h) = f \circ g + f \circ h$,
- for all $f, g, h \in \mathrm{End}A$,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative, i.e., the composition of functions is associative,
- for all $f, g, h \in \mathrm{End}A$, $f \circ (g + h) = f \circ g + f \circ h$,
- for all $f, g, h \in \mathrm{End}A$, $(f + g) \circ h = f \circ h + g \circ h$,

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Indeed, we need to check

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative, i.e., the composition of functions is associative,
- for all $f, g, h \in \mathrm{End}A$, $f \circ (g + h) = f \circ g + f \circ h$,
- for all $f, g, h \in \mathrm{End}A$, $(f + g) \circ h = f \circ h + g \circ h$,
- for all $f \in \mathrm{End}A$, $f \circ 1_A = 1_A \circ f = f$.

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. These two are clear.

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative, i.e., the composition of functions is associative,
- for all $f, g, h \in \mathrm{End}A$, $f \circ (g + h) = f \circ g + f \circ h$,
- for all $f, g, h \in \mathrm{End}A$, $(f + g) \circ h = f \circ h + g \circ h$,
- for all $f \in \mathrm{End}A$, $f \circ 1_A = 1_A \circ f = f$.

Example

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

With this addition and composition of functions as multiplication, $\mathrm{End}A$ is a (usually noncommutative) ring with identity $1_A : A \to A$. Hence we only need to check these three.

- $(\mathrm{End}A, +)$ is an abelian group,
- the multiplication is associative, i.e., the composition of functions is associative,
- for all $f, g, h \in \mathrm{End}A$, $f \circ (g + h) = f \circ g + f \circ h$,
- for all $f, g, h \in \mathrm{End}A$, $(f + g) \circ h = f \circ h + g \circ h$,
- for all $f \in \mathrm{End}A$, $f \circ 1_A = 1_A \circ f = f$.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

Proof. For all $a \in A$,

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

Proof. For all $a \in A$,

$\big((f+g)+h\big)(a)$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

Proof. For all $a \in A$,

$$\big((f+g)+h\big)(a) = (f+g)(a) + h(a)$$

by the definition of $(f+g)+h$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

Proof. For all $a \in A$,

$$\big((f+g)+h\big)(a) = (f+g)(a)+h(a) = \big(f(a)+g(a)\big)+h(a)$$

by the definition of $f+g$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

Proof. For all $a \in A$,

$$\big((f+g)+h\big)(a) = (f+g)(a)+h(a) = \big(f(a)+g(a)\big)+h(a)$$
$$= f(a)+\big(g(a)+h(a)\big)$$

because $+$ is associative

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

Proof. For all $a \in A$,

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

by the definition of $g+h$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

Proof. For all $a \in A$,

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

by the definition of $f+(g+h)$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,

Proof. For all $a \in A$,

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

so $(f+g)+h = f+(g+h)$.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,

Proof. It is obvious that the zero map is an endomorphism

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,

Proof. It is obvious that the zero map is an endomorphism and $f + 0 = 0 + f = f$ for all $f \in \mathrm{End}A$.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,

Proof. It is obvious that the zero map is an endomorphism and $f + 0 = 0 + f = f$ for all $f \in \mathrm{End}A$. Thus, the zero map is the additive identity in $\mathrm{End}A$.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$,

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$,

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Note that $\forall\ a, b \in A$,

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Note that $\forall\, a, b \in A$, $(-f)(a+b)$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Note that $\forall\, a, b \in A$, $(-f)(a+b) = -\big(f(a+b)\big)$

by the definition of $-f$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Note that $\forall\, a, b \in A$,

$$(-f)(a+b) = -\big(f(a+b)\big) = -\big(f(a)+f(b)\big)$$

because f is a homomorphism

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Note that $\forall\, a, b \in A$,

$$\begin{aligned}(-f)(a+b) &= -\big(f(a+b)\big) = -\big(f(a)+f(b)\big) \\ &= -f(a)+(-f(b))\end{aligned}$$

because A is an abelian group

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Note that $\forall\, a, b \in A$,

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

by the definition of $-f$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Note that $\forall\, a, b \in A$,

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

Hence $-f$ is a group homomorphism

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Note that $\forall\, a, b \in A$,

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

Hence $-f$ is a group homomorphism and so $-f \in \mathrm{End}A$.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Next, it is easy to check that $f + (-f) = (-f) + f = 0$.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,

Proof. We first show that $-f \in \mathrm{End}A$. Next, it is easy to check that $f + (-f) = (-f) + f = 0$. Hence, $-f$ is the additive inverse of f.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,
- $f+g = g+f$ for all $f, g \in \mathrm{End}A$.

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,
- $f+g = g+f$ for all $f, g \in \mathrm{End}A$.

Proof. Note that for all $a \in A$,

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,
- $f+g = g+f$ for all $f, g \in \mathrm{End}A$.

Proof. Note that for all $a \in A$,

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

by the definition of $f+g$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,
- $f+g = g+f$ for all $f, g \in \mathrm{End}A$.

Proof. Note that for all $a \in A$,

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

because A is abelian

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,
- $f+g = g+f$ for all $f, g \in \mathrm{End}A$.

Proof. Note that for all $a \in A$,

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

by the definition of $g+f$

$(\mathrm{End}A, +)$ is an abelian group

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$,

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

- $(f+g)+h = f+(g+h)$ for all $f, g, h \in \mathrm{End}A$,
- the zero map $0 : A \to A$, defined by $a \mapsto 0$ for all $a \in A$, is the additive identity,
- for each $f \in \mathrm{End}A$, the map $-f : A \to A$, defined by $a \mapsto -f(a)$ for all $a \in A$, is the additive inverse of f,
- $f+g = g+f$ for all $f, g \in \mathrm{End}A$.

Proof. Note that for all $a \in A$,
$(f+g)(a) = f(a)+g(a) = g(a)+f(a) = (g+f)(a)$.
Hence $f+g = g+f$.

$f \circ (g + h) = f \circ g + f \circ h$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

$$f \circ (g + h) = f \circ g + f \circ h$$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for all $a \in A$,

$f \circ (g + h) = f \circ g + f \circ h$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for all $a \in A$,

$$\big(f \circ (g + h)\big)(a)$$

$f \circ (g + h) = f \circ g + f \circ h$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for all $a \in A$,

$$\big(f \circ (g+h)\big)(a) = f\big((g+h)(a)\big)$$

by the definition of composition of functions

$f \circ (g + h) = f \circ g + f \circ h$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for all $a \in A$,

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

by the definition of $g + h$

$f \circ (g + h) = f \circ g + f \circ h$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for all $a \in A$,

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

because f is a homomorphism

$f \circ (g + h) = f \circ g + f \circ h$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for all $a \in A$,

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

by the definition of composition of functions

$f \circ (g + h) = f \circ g + f \circ h$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for all $a \in A$,

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

by the definition of $+$ in $\mathrm{End}A$

$f \circ (g + h) = f \circ g + f \circ h$

Let $(A, +)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

Note that for all $a \in A$,

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

Hence $f \circ (g + h) = f \circ g + f \circ h$.

$$(f+g)\circ h = f\circ h + g\circ h$$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

$(f+g)\circ h = f\circ h + g\circ h$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

This can be proved similarly.

$(f+g)\circ h = f\circ h + g\circ h$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

This can be proved similarly. More precisely, for all $a \in A$,

$(f+g)\circ h = f\circ h + g\circ h$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

This can be proved similarly. More precisely, for all $a \in A$,

$$\big((f+g)\circ h\big)(a)$$

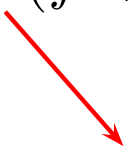
$(f+g)\circ h = f\circ h + g\circ h$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

This can be proved similarly. More precisely, for all $a \in A$,

$$\big((f+g)\circ h\big)(a) = (f+g)\big(h(a)\big)$$



by the definition of composition of functions

$(f+g)\circ h = f\circ h + g\circ h$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

This can be proved similarly. More precisely, for all $a \in A$,

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

by the definition of $+$ in $\mathrm{End}A$.

$(f+g)\circ h = f\circ h + g\circ h$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

This can be proved similarly. More precisely, for all $a \in A$,

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

by the definition of composition of functions

$(f+g)\circ h = f\circ h + g\circ h$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rcccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

This can be proved similarly. More precisely, for all $a \in A$,

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

by the definition of $+$ in $\mathrm{End}A$.

$(f+g)\circ h = f\circ h + g\circ h$

Let $(A,+)$ be an abelian group and let $\mathrm{End}A$ be the set of all endomorphisms $f : A \to A$. For all $f, g \in \mathrm{End}A$, define

$$\begin{array}{rccc} f+g & : & A & \longrightarrow & A \\ & & a & \longmapsto & f(a)+g(a) \end{array}$$

This can be proved similarly. More precisely, for all $a \in A$,

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

Hence $(f+g)\circ h = f\circ h + g\circ h$.

Remark

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

Remark

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

- Then $(R, \cdot)$ is a semigroup.

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R,

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.
- $a^0 := 1_R$ if R has an identity 1_R.

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.
- $a^0 := 1_R$ if R has an identity 1_R.
- By Theorem I.1.9, $a^m \cdot a^n = a^{m+n}$

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.
- $a^0 := 1_R$ if R has an identity 1_R.
- By Theorem I.1.9, $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.
- $a^0 := 1_R$ if R has an identity 1_R.
- By Theorem I.1.9, $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

Moreover, if we define, for $a, b \in R$, $a - b := a + (-b)$,

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.
- $a^0 := 1_R$ if R has an identity 1_R.
- By Theorem I.1.9, $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

Moreover, if we define, for $a, b \in R$, $a - b := a + (-b)$, then it is easy to check that,

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.
- $a^0 := 1_R$ if R has an identity 1_R.
- By Theorem I.1.9, $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

Moreover, if we define, for $a, b \in R$, $a - b := a + (-b)$, then it is easy to check that, $\forall a, b, c \in R$,

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.
- $a^0 := 1_R$ if R has an identity 1_R.
- By Theorem I.1.9, $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

Moreover, if we define, for $a, b \in R$, $a - b := a + (-b)$, then it is easy to check that, $\forall a, b, c \in R$,

- $a(b - c) = ab - ac$,

Remark

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

- Then $(R, \cdot)$ is a semigroup.
- If R has an identity 1_R, then $(R, \cdot)$ is a monoid.

Hence $\forall a \in R$ and $\forall m, n \in \mathbb{N}$,

- $a^n := \underbrace{aa \cdots a}_{n \text{ factors}}$.
- $a^0 := 1_R$ if R has an identity 1_R.
- By Theorem I.1.9, $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

Moreover, if we define, for $a, b \in R$, $a - b := a + (-b)$, then it is easy to check that, $\forall a, b, c \in R$,

- $a(b - c) = ab - ac$, and
- $(a - b)c = ac - bc$.

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is called the binomial coefficient.

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is called the binomial coefficient.

Theorem (1.6 Binomial Theorem)**.** Let R be a ring with identity.

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is called the binomial coefficient.

Theorem (1.6 Binomial Theorem)**.** Let R be a ring with identity. For $n \in \mathbb{N}$, $a, b, a_1, a_2, \ldots, a_s \in R$,

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is called the binomial coefficient.

Theorem (1.6 Binomial Theorem)**.** Let R be a ring with identity. For $n \in \mathbb{N}$, $a, b, a_1, a_2, \ldots, a_s \in R$,

- if $ab = ba$,

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ is called the binomial coefficient.

Theorem (1.6 Binomial Theorem)**.** Let R be a ring with identity. For $n \in \mathbb{N}$, $a, b, a_1, a_2, \ldots, a_s \in R$,

- if $ab = ba$, then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$;

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is called the binomial coefficient.

Theorem (1.6 Binomial Theorem)**.** Let R be a ring with identity. For $n \in \mathbb{N}$, $a, b, a_1, a_2, \ldots, a_s \in R$,

- if $ab = ba$, then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$;
- if $a_i a_j = a_j a_i \ \forall i, j$,

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ is called the binomial coefficient.

Theorem (1.6 Binomial Theorem)**.** Let R be a ring with identity. For $n \in \mathbb{N}$, $a, b, a_1, a_2, \ldots, a_s \in R$,

- if $ab = ba$, then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$;
- if $a_i a_j = a_j a_i \ \forall i, j$, then $(a_1 + a_2 + \cdots + a_s)^n =$

Binomial Coefficients

RECALL: For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ is called the binomial coefficient.

Theorem (1.6 Binomial Theorem)**.** Let R be a ring with identity. For $n \in \mathbb{N}$, $a, b, a_1, a_2, \ldots, a_s \in R$,

- if $ab = ba$, then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$;
- if $a_i a_j = a_j a_i \ \forall i, j$, then $(a_1 + a_2 + \cdots + a_s)^n =$

$$\sum_{i_1+i_2+\cdots+i_s=n} \frac{n!}{(i_1!)(i_2!)\cdots(i_s!)} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}.$$

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings.

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$,

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a + b) = f(a) + f(b)$

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

Remark. Even if R and S both have identities 1_R and 1_S,

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

Remark. Even if R and S both have identities 1_R and 1_S, we do NOT require that a homomorphism of rings maps 1_R to 1_S.

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

Remark. Even if R and S both have identities 1_R and 1_S, we do NOT require that a homomorphism of rings maps 1_R to 1_S.

Remark. The class of all rings together with all ring homomorphisms forms a (concrete) category.

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups,

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups, a homomorphism of rings $f : R \to S$ is a monomorphism

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups, a homomorphism of rings $f : R \to S$ is a monomorphism (resp. epimorphism, isomorphism) of rings

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups, a homomorphism of rings $f : R \to S$ is a monomorphism (resp. epimorphism, isomorphism) of rings if f is injective (resp. surjective, bijective).

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups, a homomorphism of rings $f : R \to S$ is a monomorphism (resp. epimorphism, isomorphism) of rings if f is injective (resp. surjective, bijective).
- A monomorphism of rings $R \to S$ is sometimes called

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups, a homomorphism of rings $f : R \to S$ is a monomorphism (resp. epimorphism, isomorphism) of rings if f is injective (resp. surjective, bijective).
- A monomorphism of rings $R \to S$ is sometimes called an embedding of R in S.

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups, a homomorphism of rings $f : R \to S$ is a monomorphism (resp. epimorphism, isomorphism) of rings if f is injective (resp. surjective, bijective).
- A monomorphism of rings $R \to S$ is sometimes called an embedding of R in S.
- An isomorphism $R \to R$ is called an automorphism of R.

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups, a homomorphism of rings $f : R \to S$ is a monomorphism (resp. epimorphism, isomorphism) of rings if f is injective (resp. surjective, bijective).
- A monomorphism of rings $R \to S$ is sometimes called an embedding of R in S.
- An isomorphism $R \to R$ is called an automorphism of R.
- The kernel of a homomorphism of rings $f : R \to S$ is $\operatorname{Ker} f = \{r \in R \mid f(r) = 0\}$.

Ring Homomorphisms

Definition (1.7)**.** Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings if $\forall a, b \in R$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

- As homomorphisms of groups, a homomorphism of rings $f : R \to S$ is a monomorphism (resp. epimorphism, isomorphism) of rings if f is injective (resp. surjective, bijective).
- A monomorphism of rings $R \to S$ is sometimes called an embedding of R in S.
- An isomorphism $R \to R$ is called an automorphism of R.
- The kernel of a homomorphism of rings $f : R \to S$ is $\operatorname{Ker} f = \{r \in R \mid f(r) = 0\}$.
  The image of f is $\operatorname{Im} f = \{f(r) \mid r \in R\}$.

More on Group Rings

Example. Let G and H be multiplicative groups and

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups.

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right)$$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings.

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$\overline{f}\left(\sum_{i=1}^{n} r_i g_i + \sum_{i=1}^{n} s_i g_i\right)$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i + \sum_{i=1}^{n} s_i g_i\right) = \overline{f}\left(\sum_{i=1}^{n} (r_i + s_i) g_i\right)$$

by the definition of $+$ in $R(G)$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\begin{aligned}\overline{f}\left(\textstyle\sum_{i=1}^{n} r_i g_i + \sum_{i=1}^{n} s_i g_i\right) &= \overline{f}\left(\textstyle\sum_{i=1}^{n} (r_i + s_i) g_i\right) \\ &= \textstyle\sum_{i=1}^{n} (r_i + s_i) f(g_i)\end{aligned}$$

by the definition of $\overline{f}$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\begin{aligned}\overline{f}\left(\sum_{i=1}^{n} r_i g_i + \sum_{i=1}^{n} s_i g_i\right) &= \overline{f}\left(\sum_{i=1}^{n}(r_i + s_i) g_i\right) \\ &= \sum_{i=1}^{n}(r_i + s_i) f(g_i) \\ &= \sum_{i=1}^{n} r_i f(g_i) + \sum_{i=1}^{n} s_i f(g_i)\end{aligned}$$

by the definition of $+$ in $R(G)$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\begin{aligned}
\overline{f}\left(\textstyle\sum_{i=1}^{n} r_i g_i + \sum_{i=1}^{n} s_i g_i\right) &= \overline{f}\left(\textstyle\sum_{i=1}^{n} (r_i + s_i) g_i\right) \\
&= \textstyle\sum_{i=1}^{n} (r_i + s_i) f(g_i) \\
&= \textstyle\sum_{i=1}^{n} r_i f(g_i) + \sum_{i=1}^{n} s_i f(g_i) \\
&= \overline{f}\left(\textstyle\sum_{i=1}^{n} r_i g_i\right) + \overline{f}\left(\textstyle\sum_{i=1}^{n} s_i g_i\right).
\end{aligned}$$

↓

by the definition of composition of $\overline{f}$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$\overline{f}\left(\left(\sum_{i=1}^{n} r_i g_i\right)\left(\sum_{i=1}^{n} s_i g_i\right)\right)$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\overline{f}\left(\left(\sum_{i=1}^{n} r_i g_i\right)\left(\sum_{i=1}^{n} s_i g_i\right)\right) = \overline{f}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j g_i g_j\right)$$

by the definition of multiplication in $R(G)$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\overline{f}\left(\left(\sum_{i=1}^{n} r_i g_i\right)\left(\sum_{i=1}^{n} s_i g_i\right)\right) = \overline{f}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j g_i g_j\right)$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j f(g_i g_j)$$

by the definition of $\overline{f}$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\overline{f}\left(\left(\sum_{i=1}^{n} r_i g_i\right)\left(\sum_{i=1}^{n} s_i g_i\right)\right) = \overline{f}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j g_i g_j\right)$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j f(g_i g_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j f(g_i) f(g_j)$$

because f is a group homomorphism

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\overline{f}\left(\left(\sum_{i=1}^{n} r_i g_i\right)\left(\sum_{i=1}^{n} s_i g_i\right)\right) = \overline{f}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j g_i g_j\right)$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j f(g_i g_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j f(g_i) f(g_j)$$
$$= \left(\sum_{i=1}^{n} r_i f(g_i)\right)\left(\sum_{i=1}^{n} s_i f(g_i)\right)$$

by the definition of multiplication in $R(G)$

More on Group Rings

Example. Let G and H be multiplicative groups and let $f : G \to H$ be a homomorphism of groups. Let R be a ring and define $\overline{f} : R(G) \to R(H)$ by

$$\overline{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

Then $\overline{f}$ is a homomorphism of rings. Indeed, for all $\sum_{i=1}^{n} r_i g_i, \sum_{i=1}^{n} s_i g_i \in R(G)$,

$$\begin{aligned}
&\overline{f}\big(\big(\textstyle\sum_{i=1}^{n} r_i g_i\big)\big(\sum_{i=1}^{n} s_i g_i\big)\big) = \overline{f}\big(\sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j g_i g_j\big)\\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j f(g_i g_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j f(g_i) f(g_j)\\
&= \big(\textstyle\sum_{i=1}^{n} r_i f(g_i)\big)\big(\sum_{i=1}^{n} s_i f(g_i)\big)\\
&= \overline{f}\big(\textstyle\sum_{i=1}^{n} r_i g_i\big)\overline{f}\big(\sum_{i=1}^{n} s_i g_i\big).
\end{aligned}$$

by the definition of $\overline{f}$

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \, \forall a \in R$,

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \, \forall a \in R$, let n be the least positive integer such that $na = 0 \, \forall a \in R$.

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \, \forall a \in R$, let n be the least positive integer such that $na = 0 \, \forall a \in R$. Then R is said to have characteristic n

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \, \forall a \in R$, let n be the least positive integer such that $na = 0 \, \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \, \forall a \in R$, let n be the least positive integer such that $na = 0 \, \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists,

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R.

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R. For all $m \in \mathbb{N}$,

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R. For all $m \in \mathbb{N}$,

- if $ma = 0$ for all $a \in R$, then $m1_R = 0$;

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R. For all $m \in \mathbb{N}$,

- if $ma = 0$ for all $a \in R$, then $m1_R = 0$;
- if $m1_R = 0$,

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R. For all $m \in \mathbb{N}$,

- if $ma = 0$ for all $a \in R$, then $m1_R = 0$;
- if $m1_R = 0$, then for all $a \in R$, $ma = m(a \cdot 1_R)$

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R. For all $m \in \mathbb{N}$,

- if $ma = 0$ for all $a \in R$, then $m1_R = 0$;
- if $m1_R = 0$, then for all $a \in R$, $ma = m(a \cdot 1_R) = a(m1_R)$

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R. For all $m \in \mathbb{N}$,

- if $ma = 0$ for all $a \in R$, then $m1_R = 0$;
- if $m1_R = 0$, then for all $a \in R$, $ma = m(a \cdot 1_R) = a(m1_R)$ $= a0$

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R. For all $m \in \mathbb{N}$,

- if $ma = 0$ for all $a \in R$, then $m1_R = 0$;
- if $m1_R = 0$, then for all $a \in R$, $ma = m(a \cdot 1_R) = a(m1_R)$ $= a0 = 0$.

Characteristic of a Ring

Definition (1.8)**.** Let R be a ring.

- If there exists a positive integer m such that $ma = 0 \; \forall a \in R$, let n be the least positive integer such that $na = 0 \; \forall a \in R$. Then R is said to have characteristic n and we denote $\text{char } R = n$.
- If no such m exists, R is said to have characteristic zero and we denote $\text{char } R = 0$

Remark. Suppose R is a ring with identity 1_R. For all $m \in \mathbb{N}$,

- if $ma = 0$ for all $a \in R$, then $m1_R = 0$;
- if $m1_R = 0$, then for all $a \in R$, $ma = m(a \cdot 1_R) = a(m1_R)$ $= a0 = 0$.

Thus $\{m \in \mathbb{N} \mid ma = 0 \text{ for all } a \in R\} = \{m \in \mathbb{N} \mid m1_R = 0\}$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\text{char } R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.

Proof. This is because

$n = \min\{m \in \mathbb{N} \mid ma = 0 \text{ for all } a \in R\}$

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.

Proof. This is because

$n = \min\{m \in \mathbb{N} \mid ma = 0 \text{ for all } a \in R\}$

$= \min\{m \in \mathbb{N} \mid m1_R = 0\}$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors,

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,)

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number,

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number, then $n = m\ell$ for some integers m, ℓ with $1 < m, \ell < n$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number, then $n = m\ell$ for some integers m, ℓ with $1 < m, \ell < n$. Since $m \in \mathbb{N}$ and $m < n$,

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number, then $n = m\ell$ for some integers m, ℓ with $1 < m, \ell < n$. Since $m \in \mathbb{N}$ and $m < n$, $m1_R \neq 0$;

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number, then $n = m\ell$ for some integers m, ℓ with $1 < m, \ell < n$. Since $m \in \mathbb{N}$ and $m < n$, $m1_R \neq 0$; similarly, $\ell 1_R \neq 0$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number, then $n = m\ell$ for some integers m, ℓ with $1 < m, \ell < n$. Since $m \in \mathbb{N}$ and $m < n$, $m1_R \neq 0$; similarly, $\ell 1_R \neq 0$. On the other hand, $(m1_R)(\ell 1_R) = (m\ell)1_R$

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number, then $n = m\ell$ for some integers m, ℓ with $1 < m, \ell < n$. Since $m \in \mathbb{N}$ and $m < n$, $m1_R \neq 0$; similarly, $\ell 1_R \neq 0$. On the other hand,
$(m1_R)(\ell 1_R) = (m\ell)1_R = n1_R$

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number, then $n = m\ell$ for some integers m, ℓ with $1 < m, \ell < n$. Since $m \in \mathbb{N}$ and $m < n$, $m1_R \neq 0$; similarly, $\ell 1_R \neq 0$. On the other hand,
$(m1_R)(\ell 1_R) = (m\ell)1_R = n1_R = 0$,

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.

Proof. If n is not a prime number, then $n = m\ell$ for some integers m, ℓ with $1 < m, \ell < n$. Since $m \in \mathbb{N}$ and $m < n$, $m1_R \neq 0$; similarly, $\ell 1_R \neq 0$. On the other hand, $(m1_R)(\ell 1_R) = (m\ell)1_R = n1_R = 0$, which contradicts the assumption that R has no zero divisors.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$. Conversely, let $m \in \operatorname{Ker} \varphi$,

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$. Conversely, let $m \in \operatorname{Ker} \varphi$, i.e., $m1_R = 0$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$. Conversely, let $m \in \operatorname{Ker} \varphi$, i.e., $m1_R = 0$. Write $m = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$. Conversely, let $m \in \operatorname{Ker} \varphi$, i.e., $m1_R = 0$. Write $m = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $0 = m1_R = qn1_R + r1_R$

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$. Conversely, let $m \in \operatorname{Ker} \varphi$, i.e., $m1_R = 0$. Write $m = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $0 = m1_R = qn1_R + r1_R = r1_R$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$. Conversely, let $m \in \operatorname{Ker} \varphi$, i.e., $m1_R = 0$. Write $m = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $0 = m1_R = qn1_R + r1_R = r1_R$. By the minimality of n, we have $r = 0$

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$. Conversely, let $m \in \operatorname{Ker} \varphi$, i.e., $m1_R = 0$. Write $m = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $0 = m1_R = qn1_R + r1_R = r1_R$. By the minimality of n, we have $r = 0$ and so $m = qn \in \langle n \rangle$.

Theorem (1.9)

Let R be a ring with identity 1_R with $\operatorname{char} R = n > 0$.

- n is the least positive integer such that $n1_R = 0$.
- If R has no zero divisors, (in particular if R is an integral domain,) then n is prime.
- If
$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & R \\ & & m & \longmapsto & m1_R \end{array}$$
then φ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$.

Proof. It is clear that $\langle n \rangle \subseteq \operatorname{Ker} \varphi$. Conversely, let $m \in \operatorname{Ker} \varphi$, i.e., $m1_R = 0$. Write $m = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $0 = m1_R = qn1_R + r1_R = r1_R$. By the minimality of n, we have $r = 0$ and so $m = qn \in \langle n \rangle$. This completes the proof.

Theorem (1.10)

Every ring R may be embedded in a ring S with identity.

Theorem (1.10)

Every ring R may be embedded in a ring S with identity.

Moreover, the ring S

Theorem (1.10)

Every ring R may be embedded in a ring S with identity.

Moreover, the ring S (which is not unique)

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\mathrm{char}\, S = 0$.

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\mathrm{char}\, S = 0$.

- Take $S = \mathbb{Z} \oplus R$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\mathrm{char}\, S = 0$.

- Take $S = \mathbb{Z} \oplus R$ and $\forall k_1, k_2 \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\operatorname{char} S = 0$.

- Take $S = \mathbb{Z} \oplus R$ and $\forall k_1, k_2 \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(k_1, r_1) + (k_2, r_2) = (k_1 + k_2, r_1 + r_2)$$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\operatorname{char} S = 0$.

- Take $S = \mathbb{Z} \oplus R$ and $\forall k_1, k_2 \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(k_1, r_1) + (k_2, r_2) = (k_1 + k_2, r_1 + r_2)$$

$$(k_1, r_1) \cdot (k_2, r_2) = (k_1 k_2, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\operatorname{char} S = 0$.

- Take $S = \mathbb{Z} \oplus R$ and $\forall k_1, k_2 \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(k_1, r_1) + (k_2, r_2) = (k_1 + k_2, r_1 + r_2)$$
$$(k_1, r_1) \cdot (k_2, r_2) = (k_1 k_2, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Then $(S, +, \cdot)$ is a ring with identity $(1, 0)$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\operatorname{char} S = 0$.

- Take $S = \mathbb{Z} \oplus R$ and $\forall k_1, k_2 \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(k_1, r_1) + (k_2, r_2) = (k_1 + k_2, r_1 + r_2)$$

$$(k_1, r_1) \cdot (k_2, r_2) = (k_1 k_2, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Then $(S, +, \cdot)$ is a ring with identity $(1, 0)$ and $\operatorname{char} S = 0$.

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\operatorname{char} S = 0$.

- Take $S = \mathbb{Z} \oplus R$ and $\forall k_1, k_2 \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(k_1, r_1) + (k_2, r_2) = (k_1 + k_2, r_1 + r_2)$$
$$(k_1, r_1) \cdot (k_2, r_2) = (k_1 k_2, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Then $(S, +, \cdot)$ is a ring with identity $(1, 0)$ and $\operatorname{char} S = 0$.

Moreover, $f : R \longrightarrow S$ is a monomorphism,

$$r \longmapsto (0, r)$$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. We first show that we can choose S with $\operatorname{char} S = 0$.

- Take $S = \mathbb{Z} \oplus R$ and $\forall k_1, k_2 \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(k_1, r_1) + (k_2, r_2) = (k_1 + k_2, r_1 + r_2)$$
$$(k_1, r_1) \cdot (k_2, r_2) = (k_1 k_2, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Then $(S, +, \cdot)$ is a ring with identity $(1, 0)$ and $\operatorname{char} S = 0$.

Moreover, $f : R \longrightarrow S$ is a monomorphism,

$$r \longmapsto (0, r)$$

i.e., an embedding.

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\mathrm{char}\, R = n > 0$,

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\mathrm{char}\, R = n > 0$, we can choose S with $\mathrm{char}\, S = n$.

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\operatorname{char} R = n > 0$, we can choose S with $\operatorname{char} S = n$.

- Take $S = \mathbb{Z}_n \oplus R$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\text{char}\, R = n > 0$, we can choose S with $\text{char}\, S = n$.

- Take $S = \mathbb{Z}_n \oplus R$ and $\forall \overline{k_1}, \overline{k_2} \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\operatorname{char} R = n > 0$, we can choose S with $\operatorname{char} S = n$.

- Take $S = \mathbb{Z}_n \oplus R$ and $\forall \overline{k_1}, \overline{k_2} \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(\overline{k_1}, r_1) + (\overline{k_2}, r_2) = (\overline{k_1} + \overline{k_2}, r_1 + r_2)$$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\operatorname{char} R = n > 0$, we can choose S with $\operatorname{char} S = n$.

- Take $S = \mathbb{Z}_n \oplus R$ and $\forall \overline{k_1}, \overline{k_2} \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(\overline{k_1}, r_1) + (\overline{k_2}, r_2) = (\overline{k_1} + \overline{k_2}, r_1 + r_2)$$
$$(\overline{k_1}, r_1) \cdot (\overline{k_2}, r_2) = (\overline{k_1 k_2}, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\operatorname{char} R = n > 0$, we can choose S with $\operatorname{char} S = n$.

- Take $S = \mathbb{Z}_n \oplus R$ and $\forall \overline{k_1}, \overline{k_2} \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(\overline{k_1}, r_1) + (\overline{k_2}, r_2) = (\overline{k_1} + \overline{k_2}, r_1 + r_2)$$
$$(\overline{k_1}, r_1) \cdot (\overline{k_2}, r_2) = (\overline{k_1 k_2}, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Then $(S, +, \cdot)$ is a ring with identity $(\overline{1}, 0)$

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\operatorname{char} R = n > 0$, we can choose S with $\operatorname{char} S = n$.

- Take $S = \mathbb{Z}_n \oplus R$ and $\forall \overline{k_1}, \overline{k_2} \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(\overline{k_1}, r_1) + (\overline{k_2}, r_2) = (\overline{k_1} + \overline{k_2}, r_1 + r_2)$$
$$(\overline{k_1}, r_1) \cdot (\overline{k_2}, r_2) = (\overline{k_1 k_2}, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Then $(S, +, \cdot)$ is a ring with identity $(\overline{1}, 0)$ and $\operatorname{char} S = n$.

Theorem (1.10)

Every ring R may be embedded in a ring S with identity. Moreover, the ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Next, we show that if $\operatorname{char} R = n > 0$, we can choose S with $\operatorname{char} S = n$.

- Take $S = \mathbb{Z}_n \oplus R$ and $\forall \overline{k_1}, \overline{k_2} \in \mathbb{Z}$ and $\forall r_1, r_2 \in R$, let

$$(\overline{k_1}, r_1) + (\overline{k_2}, r_2) = (\overline{k_1} + \overline{k_2}, r_1 + r_2)$$
$$(\overline{k_1}, r_1) \cdot (\overline{k_2}, r_2) = (\overline{k_1 k_2}, k_1 r_2 + k_2 r_1 + r_1 r_2).$$

Then $(S, +, \cdot)$ is a ring with identity $(\overline{1}, 0)$ and $\operatorname{char} S = n$.

Moreover, $f : R \longrightarrow S$ is a monomorphism,

$$r \longmapsto (\overline{0}, r)$$

i.e., an embedding.

Exercise for Section III.1

2, 3, 5, 6, 11, 12, 14, 16.

Chapter III: Rings

Chapter III: Rings

Section III.2: Ideals

Chapter III: Rings

Section III.2: Ideals

Just as normal subgroups play a crucial role in the theory of groups,

Chapter III: Rings

Section III.2: Ideals

Just as normal subgroups play a crucial role in the theory of groups, ideals play an analogous role in the study of rings.

Ideals

Ideals

Definition (2.1)**.** Let R be a ring.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

(i) S is closed under the operations of addition and multiplication in R,

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

(i) S is closed under the operations of addition and multiplication in R,

(ii) S is a ring under these operations.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

(i) S is closed under the operations of addition and multiplication in R,

(ii) S is a ring under these operations.

- Let I be a subring of R.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.

  ⋆ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Example. Every ring has two ideals, namely R itself

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Example. Every ring has two ideals, namely R itself and the trivial ideal $\{0\}$.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Example. Every ring has two ideals, namely R itself and the trivial ideal $\{0\}$. We denote the trivial ideal 0.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Example. If R is a ring,

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Example. If R is a ring, then the center of R

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Example. If R is a ring, then the center of R is the set $C = \{c \in R \mid cr = rc \; \forall r \in R\}$.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Example. If R is a ring, then the center of R is the set $C = \{c \in R \mid cr = rc \; \forall r \in R\}$. C is a subring of R,

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Example. If R is a ring, then the center of R is the set $C = \{c \in R \mid cr = rc \; \forall r \in R\}$. C is a subring of R, but may NOT be an ideal.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Remark. The assumption that I is a subring of R

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Remark. The assumption that I is a subring of R can be replaced by the assumption that I is a subgroup of R.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Remark. The assumption that I is a subring of R can be replaced by the assumption that I is a subgroup of R. This is because if we have "$r \in R$ and $a \in I \implies ar \in I$",

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Remark. The assumption that I is a subring of R can be replaced by the assumption that I is a subgroup of R. This is because if we have "$r \in R$ and $a \in I \implies ar \in I$", then we have "$a, b \in I \implies ab \in I$",

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a subring of R.
  - $\star$ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - $\star$ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - $\star$ I is an ideal if it is both a left and right ideal.

Remark. The assumption that I is a subring of R can be replaced by the assumption that I is a subgroup of R. This is because if we have "$r \in R$ and $a \in I \implies ar \in I$", then we have "$a, b \in I \implies ab \in I$", since $b \in I$ gives us $b \in R$.

Ideals

Definition (2.1)**.** Let R be a ring.

- A subring S is a nonempty subset of R such that

  (i) S is closed under the operations of addition and multiplication in R,

  (ii) S is a ring under these operations.

- Let I be a *subgroup* of R.
  - ⋆ I is a right ideal if $r \in R$ and $a \in I \implies ar \in I$.
  - ⋆ I is a left ideal if $r \in R$ and $a \in I \implies ra \in I$.
  - ⋆ I is an ideal if it is both a left and right ideal.

Remark. The assumption that I is a subring of R can be replaced by the assumption that I is a subgroup of R. This is because if we have "$r \in R$ and $a \in I \implies ar \in I$", then we have "$a, b \in I \implies ab \in I$", since $b \in I$ gives us $b \in R$.

Remark

Let $f : R \to S$ be a ring homomorphism.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.

  In fact, if J is an ideal of S,

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism,

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$,

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$.
Note that $f(ar) = f(a)f(r) \in J$

because f is a ring homomorphism

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$.
Note that $f(ar) = f(a)f(r) \in J$

because $f(a) \in J$, $f(r) \in S$, and J is an ideal of S

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$. Note that $f(ar)=f(a)f(r)\in J$ and $f(ra)=f(r)f(a)\in J$.

because f is a ring homomorphism

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$. Note that $f(ar)=f(a)f(r)\in J$ and $f(ra)=f(r)f(a)\in J$.

because $f(a) \in J$, $f(r) \in S$, and J is an ideal of S

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$. Note that $f(ar)=f(a)f(r)\in J$ and $f(ra)=f(r)f(a)\in J$. Hence, $ar, ra \in f^{-1}(J)$.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$. Note that $f(ar)=f(a)f(r)\in J$ and $f(ra)=f(r)f(a)\in J$. Hence, $ar, ra \in f^{-1}(J)$. There, $f^{-1}(J)$ is an ideal of R.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$. Note that $f(ar)=f(a)f(r)\in J$ and $f(ra)=f(r)f(a)\in J$. Hence, $ar, ra \in f^{-1}(J)$. There, $f^{-1}(J)$ is an ideal of R. Since $\mathrm{Ker}\ f = f^{-1}(0)$,

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

Proof. Since J is a subgroup of $(S, +)$ and since f is a group homomorphism, $f^{-1}(J)$ is a subgroup of R. Hence, we only need to show that $\forall a \in f^{-1}(J)$ and $\forall r \in R$, $ar, ra \in f^{-1}(J)$. Note that $f(ar)=f(a)f(r)\in J$ and $f(ra)=f(r)f(a)\in J$. Hence, $ar, ra \in f^{-1}(J)$. There, $f^{-1}(J)$ is an ideal of R. Since $\mathrm{Ker}\ f = f^{-1}(0)$, $\mathrm{Ker}\ f$ is an ideal of R.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.
- However, if I is an ideal of R,

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.
- However, if I is an ideal of R, $f(I)$ may not be an ideal of S.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.
- However, if I is an ideal of R, $f(I)$ may not be an ideal of S.
  In particular, $\mathrm{Im}\ f$ may not be an ideal of S.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.
- However, if I is an ideal of R, $f(I)$ may not be an ideal of S.
  In particular, $\mathrm{Im}\, f$ may not be an ideal of S.

Example. Consider the ring homomorphism $f : \mathbb{Z} \to \mathbb{Q}$ given by $f(n) = n$.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.
- However, if I is an ideal of R, $f(I)$ may not be an ideal of S.
  In particular, $\mathrm{Im}\, f$ may not be an ideal of S.

Example. Consider the ring homomorphism $f : \mathbb{Z} \to \mathbb{Q}$ given by $f(n) = n$. Then $\mathrm{Im}\, f = \mathbb{Z}$, which is not an ideal of $\mathbb{Q}$;

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\, f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.
- However, if I is an ideal of R, $f(I)$ may not be an ideal of S.
  In particular, $\mathrm{Im}\, f$ may not be an ideal of S.

Example. Consider the ring homomorphism $f : \mathbb{Z} \to \mathbb{Q}$ given by $f(n) = n$. Then $\mathrm{Im}\, f = \mathbb{Z}$, which is not an ideal of $\mathbb{Q}$; for example, $\frac{1}{2} \cdot 3 = \frac{3}{2} \notin \mathbb{Z}$, even though $\frac{1}{2} \in \mathbb{Q}$ and $3 \in \mathbb{Z}$.

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.
- However, if I is an ideal of R, $f(I)$ may not be an ideal of S.
  In particular, $\mathrm{Im}\ f$ may not be an ideal of S.

Example. Consider the ring homomorphism $f : \mathbb{Z} \to \mathbb{Q}$ given by $f(n) = n$. Then $\mathrm{Im}\ f = \mathbb{Z}$, which is not an ideal of $\mathbb{Q}$; for example, $\frac{1}{2} \cdot 3 = \frac{3}{2} \notin \mathbb{Z}$, even though $\frac{1}{2} \in \mathbb{Q}$ and $3 \in \mathbb{Z}$. In fact, the only ideal I of $\mathbb{Z}$ such that $f(I)$ is an ideal of $\mathbb{Q}$

Remark

Let $f : R \to S$ be a ring homomorphism.

- $\mathrm{Ker}\ f$ is an ideal of R.
  In fact, if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.
- However, if I is an ideal of R, $f(I)$ may not be an ideal of S.
  In particular, $\mathrm{Im}\ f$ may not be an ideal of S.

Example. Consider the ring homomorphism $f : \mathbb{Z} \to \mathbb{Q}$ given by $f(n) = n$. Then $\mathrm{Im}\ f = \mathbb{Z}$, which is not an ideal of $\mathbb{Q}$; for example, $\frac{1}{2} \cdot 3 = \frac{3}{2} \notin \mathbb{Z}$, even though $\frac{1}{2} \in \mathbb{Q}$ and $3 \in \mathbb{Z}$. In fact, the only ideal I of $\mathbb{Z}$ such that $f(I)$ is an ideal of $\mathbb{Q}$ is $I = 0$.

Proper Ideals

Definition. A proper ideal is an ideal I of R

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R.

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii).

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i).

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R.

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R. Then there exists $u^{-1} \in R$.

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R. Then there exists $u^{-1} \in R$. For all $r \in R$,

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R. Then there exists $u^{-1} \in R$. For all $r \in R$, since $r = (ru^{-1})u$,

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R. Then there exists $u^{-1} \in R$. For all $r \in R$, since $r = (ru^{-1})u$, $ru^{-1} \in R$,

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R. Then there exists $u^{-1} \in R$. For all $r \in R$, since $r = (ru^{-1})u$, $ru^{-1} \in R$, and $u \in I$,

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R. Then there exists $u^{-1} \in R$. For all $r \in R$, since $r = (ru^{-1})u$, $ru^{-1} \in R$, and $u \in I$, we have $r = (ru^{-1})u \in I$.

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R. Then there exists $u^{-1} \in R$. For all $r \in R$, since $r = (ru^{-1})u$, $ru^{-1} \in R$, and $u \in I$, we have $r = (ru^{-1})u \in I$. Thus $R \subseteq I$

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Proof. It is clear that (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Hence we only need to show (iii) $\Longrightarrow$ (i). Let $u \in I$ be a unit in R. Then there exists $u^{-1} \in R$. For all $r \in R$, since $r = (ru^{-1})u$, $ru^{-1} \in R$, and $u \in I$, we have $r = (ru^{-1})u \in I$. Thus $R \subseteq I$ and so $I = R$.

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Remark. Left proper ideals and right proper ideals are defined similarly as in the above Definition.

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Remark. Left proper ideals and right proper ideals are defined similarly as in the above Definition. The same statement as in the above Remark holds true for both left ideals and right ideals;

Proper Ideals

Definition. A proper ideal is an ideal I of R such that $I \neq 0$ and $I \neq R$.

Remark. Let R be a ring with identity 1_R and let I be an ideal of R. Then the following conditions are equivalent:

(i) $I = R$;

(ii) $1_R \in I$;

(iii) I contains a unit of R.

Remark. Left proper ideals and right proper ideals are defined similarly as in the above Definition. The same statement as in the above Remark holds true for both left ideals and right ideals; the proof is the same or practically the same.

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Proof. Since (i) tells us that I is a subgroup of R,

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Proof. Since (i) tells us that I is a subgroup of R, this follows from our remark to the definition of ideals.

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Corollary (2.3)**.** Let $\{A_i \mid i \in I\}$ be a family of (left or right) ideals in a ring R.

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Corollary (2.3)**.** Let $\{A_i \mid i \in I\}$ be a family of (left or right) ideals in a ring R. Then $\bigcap_{i \in I} A_i$ is a (left or right) ideal.

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Corollary (2.3)**.** Let $\{A_i \mid i \in I\}$ be a family of (left or right) ideals in a ring R. Then $\bigcap_{i \in I} A_i$ is a (left or right) ideal.

Proof. This is easy to check using Theorem (2.2).

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Corollary (2.3)**.** Let $\{A_i \mid i \in I\}$ be a family of (left or right) ideals in a ring R. Then $\bigcap_{i \in I} A_i$ is a (left or right) ideal.

Definition (2.4)**.** Let X be a subset of a ring R

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Corollary (2.3)**.** Let $\{A_i \mid i \in I\}$ be a family of (left or right) ideals in a ring R. Then $\bigcap_{i \in I} A_i$ is a (left or right) ideal.

Definition (2.4)**.** Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X.

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Corollary (2.3)**.** Let $\{A_i \mid i \in I\}$ be a family of (left or right) ideals in a ring R. Then $\bigcap_{i \in I} A_i$ is a (left or right) ideal.

Definition (2.4)**.** Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Corollary (2.3)**.** Let $\{A_i \mid i \in I\}$ be a family of (left or right) ideals in a ring R. Then $\bigcap_{i \in I} A_i$ is a (left or right) ideal.

Definition (2.4)**.** Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X.

Theorem (2.2)

A nonempty subset I of a ring R is a left (resp. right) ideal if and only if

(i) $a, b \in I \implies a - b \in I$,

(ii) $a \in I$ and $r \in R \implies ra \in I$ (resp. $ar \in I$).

Corollary (2.3)**.** Let $\{A_i \mid i \in I\}$ be a family of (left or right) ideals in a ring R. Then $\bigcap_{i \in I} A_i$ is a (left or right) ideal.

Definition (2.4)**.** Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

Definition (2.4)**.** Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

Definition (2.4)**.** Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$,

Definition (2.4)**.** Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, \ldots, x_n)$

Definition (2.4). Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, \ldots, x_n)$ and is said to be finitely generated.

Definition (2.4). Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, \ldots, x_n)$ and is said to be finitely generated.
- An ideal (x), generated by a single element,

Definition (2.4). Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, \ldots, x_n)$ and is said to be finitely generated.
- An ideal (x), generated by a single element, is called a principal ideal.

Definition (2.4). Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, \ldots, x_n)$ and is said to be finitely generated.
- An ideal (x), generated by a single element, is called a principal ideal.
- A principal ideal ring is a ring in which every ideal is principal.

Definition (2.4). Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, \ldots, x_n)$ and is said to be finitely generated.
- An ideal (x), generated by a single element, is called a principal ideal.
- A principal ideal ring is a ring in which every ideal is principal.
- A principal ideal ring which is an integral domain is called

Definition (2.4). Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, \ldots, x_n)$ and is said to be finitely generated.
- An ideal (x), generated by a single element, is called a principal ideal.
- A principal ideal ring is a ring in which every ideal is principal.
- A principal ideal ring which is an integral domain is called a principal ideal domain

Definition (2.4). Let X be a subset of a ring R and let $\{A_i \mid i \in I\}$ be the family of all (left or right) ideals in R which contain X. Then $(X) := \bigcap_{i \in I} A_i$ is called the (left or right) ideal generated by X. The elements of X are called generators of the ideal (X).

- If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, \ldots, x_n)$ and is said to be finitely generated.
- An ideal (x), generated by a single element, is called a principal ideal.
- A principal ideal ring is a ring in which every ideal is principal.
- A principal ideal ring which is an integral domain is called a principal ideal domain or simply a PID.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form ra

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as$

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na$

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
    This is because $ra = ra1_R$,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
    This is because $ra = ra1_R$, $as = 1_R as$,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$. This is because $ra = ra1_R$, $as = 1_R as$, and $na = (n1_R)a1_R$.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then
    $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then
    $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
    This is because a commutes with every element in R,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then
    $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then
    $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
    This is because a commutes with every element in R, and so we have $ra + as + \sum_{i=1}^{m} r_i a s_i = ra + sa + \sum_{i=1}^{m} r_i s_i a$

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then
    $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then
    $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
    This is because a commutes with every element in R, and so we have $ra + as + \sum_{i=1}^{m} r_i a s_i = ra + sa + \sum_{i=1}^{m} r_i s_i a$
    $= \left(r + s + \sum_{i=1}^{m} r_i s_i\right) a$,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
    This is because a commutes with every element in R, and so we have $ra + as + \sum_{i=1}^{m} r_i a s_i = ra + sa + \sum_{i=1}^{m} r_i s_i a$ $= \left(r + s + \sum_{i=1}^{m} r_i s_i\right) a$, which is an element of the form ra.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $Ra = \{ra \mid r \in R\}$ is a left ideal of R

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $Ra = \{ra \mid r \in R\}$ is a left ideal of R and $aR = \{ar \mid r \in R\}$ is a right ideal of R.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $Ra = \{ra \mid r \in R\}$ is a left ideal of R and $aR = \{ar \mid r \in R\}$ is a right ideal of R.
  - ⋆ If R has an identity, then $a \in Ra$ and $a \in aR$.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $Ra = \{ra \mid r \in R\}$ is a left ideal of R and $aR = \{ar \mid r \in R\}$ is a right ideal of R.
  - ⋆ If R has an identity, then $a \in Ra$ and $a \in aR$.
    This is because $a = 1_R a \in Ra$

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $Ra = \{ra \mid r \in R\}$ is a left ideal of R and $aR = \{ar \mid r \in R\}$ is a right ideal of R.
  - ⋆ If R has an identity, then $a \in Ra$ and $a \in aR$.
    This is because $a = 1_R a \in Ra$ and $a = a1_R \in aR$.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $Ra = \{ra \mid r \in R\}$ is a left ideal of R and $aR = \{ar \mid r \in R\}$ is a right ideal of R.
  - ⋆ If R has an identity, then $a \in Ra$ and $a \in aR$.
  - ⋆ If R has an identity

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $Ra = \{ra \mid r \in R\}$ is a left ideal of R and $aR = \{ar \mid r \in R\}$ is a right ideal of R.
  - ⋆ If R has an identity, then $a \in Ra$ and $a \in aR$.
  - ⋆ If R has an identity and a is in the center of R,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $Ra = \{ra \mid r \in R\}$ is a left ideal of R and $aR = \{ar \mid r \in R\}$ is a right ideal of R.
  - ⋆ If R has an identity, then $a \in Ra$ and $a \in aR$.
  - ⋆ If R has an identity and a is in the center of R, then $Ra = (a) = aR$.

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- If R has an identity

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then
    $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then
    $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- If R has an identity and X is in the center of R,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- If R has an identity and X is in the center of R, then the ideal (X) consists of all finite sums

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- If R has an identity and X is in the center of R, then the ideal (X) consists of all finite sums $r_1 a_1 + \cdots + r_m a_m$

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- If R has an identity and X is in the center of R, then the ideal (X) consists of all finite sums $r_1 a_1 + \cdots + r_m a_m$ with $m \in \mathbb{N}$,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- If R has an identity and X is in the center of R, then the ideal (X) consists of all finite sums $r_1 a_1 + \cdots + r_m a_m$ with $m \in \mathbb{N}$, $r_1, \ldots, r_m \in R$,

Theorem (2.5)

Let R be a ring, $a \in R$, and $X \subseteq R$.

- The principal ideal (a) consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, where $r, s, r_i, s_i \in R$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$.
  - ⋆ If R has an identity, then $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R,\ m \in \mathbb{N}\}$.
  - ⋆ If a is in the center of R, then $(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- If R has an identity and X is in the center of R, then the ideal (X) consists of all finite sums $r_1 a_1 + \cdots + r_m a_m$ with $m \in \mathbb{N}$, $r_1, \ldots, r_m \in R$, $a_1, \ldots, a_m \in X$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- AB

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
- $A_1 A_2 \cdots A_n$ denotes the set of

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
- $A_1 A_2 \cdots A_n$ denotes the set of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in A_i$ for $i = 1, 2, \ldots, n$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
- $A_1 A_2 \cdots A_n$ denotes the set of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in A_i$ for $i = 1, 2, \ldots, n$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
- $A_1 A_2 \cdots A_n$ denotes the set of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in A_i$ for $i = 1, 2, \ldots, n$.
  - ⋆ If $A_1 = A_2 = \cdots = A_n = A$,

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
- $A_1 A_2 \cdots A_n$ denotes the set of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in A_i$ for $i = 1, 2, \ldots, n$.
  - ⋆ If $A_1 = A_2 = \cdots = A_n = A$,
    $A_1 A_2 \cdots A_n$

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
- $A_1 A_2 \cdots A_n$ denotes the set of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in A_i$ for $i = 1, 2, \ldots, n$.
  - ⋆ If $A_1 = A_2 = \cdots = A_n = A$,
    $A_1 A_2 \cdots A_n = \underbrace{AA \cdots A}_{n \text{ factors}}$

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
- $A_1 A_2 \cdots A_n$ denotes the set of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in A_i$ for $i = 1, 2, \ldots, n$.
  - ⋆ If $A_1 = A_2 = \cdots = A_n = A$,
    $A_1 A_2 \cdots A_n = \underbrace{AA \cdots A}_{n \text{ factors}} = A^n$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
  - ⋆ If $A = \{a\}$,

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
  - ⋆ If $A = \{a\}$, then $aB = AB$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
  - ⋆ If $A = \{a\}$, then $aB = AB$.
  - ⋆ If $B = \{b\}$,

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
  - ⋆ If $A = \{a\}$, then $aB = AB$.
  - ⋆ If $B = \{b\}$, then $Ab = AB$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
  - ⋆ If $A = \{a\}$, then $aB = AB$.
  - ⋆ If $B = \{b\}$, then $Ab = AB$.
  - ⋆ If B is closed under addition,

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
  - ⋆ If $A = \{a\}$, then $aB = AB$.
  - ⋆ If $B = \{b\}$, then $Ab = AB$.
  - ⋆ If B is closed under addition, $aB = \{ab \mid b \in B\}$.

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
  - ⋆ If $A = \{a\}$, then $aB = AB$.
  - ⋆ If $B = \{b\}$, then $Ab = AB$.
  - ⋆ If B is closed under addition, $aB = \{ab \mid b \in B\}$.
  - ⋆ If A is closed under addition,

Notations

Let A, B, A_1, A_2, . . ., A_n be nonempty subsets of a ring R.

- $A_1 + A_2 + \cdots + A_n$
  $= \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i = 1, 2, \ldots, n\}$.
- $AB = \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$.
  - ⋆ If $A = \{a\}$, then $aB = AB$.
  - ⋆ If $B = \{b\}$, then $Ab = AB$.
  - ⋆ If B is closed under addition, $aB = \{ab \mid b \in B\}$.
  - ⋆ If A is closed under addition, $Ab = \{ab \mid a \in A\}$.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C)$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC)$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC) = ABC$.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC) = ABC$.
- $B(A_1 + A_2 + \cdots + A_n)$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC) = ABC$.
- $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC) = ABC$.
- $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$.
- $(A_1 + A_2 + \cdots + A_n)C$

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC) = ABC$.
- $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$.
- $(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots + A_nC$.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC) = ABC$.
- $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$.
- $(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots + A_nC$.

These can all be checked directly, so I skip the proofs here. Please practice proving them after the class.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC) = ABC$.
- $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$.
- $(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots + A_nC$.

These can all be checked directly, so I skip the proofs here.

Please practice proving them after the class.

Notation

$$A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ \forall i\}$$

$$A_1 A_2 \cdots A_n = \Big\{ \sum_{\text{finite}} a_1 a_2 \cdots a_n \mid a_i \in A_i,\ \forall i \Big\}$$

Theorem (2.6)**.** Let A, B, C and $A_1, A_2, \ldots, A_n$ be (left or right) ideals in a ring R.

- $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are (left or right) ideals.
- $(A + B) + C = A + (B + C) = A + B + C$.
- $(AB)C = A(BC) = ABC$.
- $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$.
- $(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots + A_nC$.

These can all be checked directly, so I skip the proofs here. Please practice proving them after the class.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.

Then the additive quotient group R/I

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.)

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.)
Suppose $a+I = \alpha+I$ and $b+I = \beta+I$,

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.)
Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$,

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$, i.e., $ab-\alpha\beta \in I$.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$, i.e., $ab-\alpha\beta \in I$. Note that

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$, i.e., $ab-\alpha\beta \in I$. Note that $ab-\alpha\beta = ab-a\beta+a\beta-\alpha\beta$

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$, i.e., $ab-\alpha\beta \in I$. Note that $ab-\alpha\beta = ab-a\beta+a\beta-\alpha\beta$ $= a(b-\beta)+(a-\alpha)\beta$.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$, i.e., $ab-\alpha\beta \in I$. Note that $ab-\alpha\beta = ab-a\beta+a\beta-\alpha\beta$ $= a(b-\beta)+(a-\alpha)\beta$. Since $a \in R,\ b-\beta \in I \Rightarrow a(b-\beta) \in I$

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$, i.e., $ab-\alpha\beta \in I$. Note that $ab-\alpha\beta = ab-a\beta+a\beta-\alpha\beta$ $= a(b-\beta)+(a-\alpha)\beta$. Since $a \in R,\ b-\beta \in I \Rightarrow a(b-\beta) \in I$ and $a-\alpha \in I,\ \beta \in R \Rightarrow (a-\alpha)\beta \in I$,

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$, i.e., $ab-\alpha\beta \in I$. Note that $ab-\alpha\beta = ab-a\beta+a\beta-\alpha\beta$ $= a(b-\beta)+(a-\alpha)\beta$. Since $a \in R,\ b-\beta \in I \Rightarrow a(b-\beta) \in I$ and $a-\alpha \in I,\ \beta \in R \Rightarrow (a-\alpha)\beta \in I$, $ab-\alpha\beta \in I$

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Proof. We only need to check that the multiplication is well-defined. (The remaining properties are clear or easy to see.) Suppose $a+I = \alpha+I$ and $b+I = \beta+I$, i.e., $a-\alpha \in I$ and $b-\beta \in I$. We want to show that $ab+I = \alpha\beta+I$, i.e., $ab-\alpha\beta \in I$. Note that $ab-\alpha\beta = ab-a\beta+a\beta-\alpha\beta$ $= a(b-\beta)+(a-\alpha)\beta$. Since $a \in R,\ b-\beta \in I \Rightarrow a(b-\beta) \in I$ and $a-\alpha \in I,\ \beta \in R \Rightarrow (a-\alpha)\beta \in I$, $ab-\alpha\beta \in I$ and so $ab+I = \alpha\beta+I$.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.

Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Moreover, if R is commutative

Theorem (2.7)

Let R be a ring and let I be an ideal of R.

Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Moreover, if R is commutative or has identity,

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Moreover, if R is commutative or has identity, then the same is true for R/I.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Moreover, if R is commutative or has identity, then the same is true for R/I.

Proof. If R is commutative,

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Moreover, if R is commutative or has identity, then the same is true for R/I.

Proof. If R is commutative, it is easy to see that R/I is also commutative.

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Moreover, if R is commutative or has identity, then the same is true for R/I.

Proof. If R is commutative, it is easy to see that R/I is also commutative. If R is a ring with identity 1_R,

Theorem (2.7)

Let R be a ring and let I be an ideal of R.
Then the additive quotient group R/I is a ring with multiplication given by

$$(a+I)(b+I) = ab+I \quad \forall a, b \in R.$$

Moreover, if R is commutative or has identity, then the same is true for R/I.

Proof. If R is commutative, it is easy to see that R/I is also commutative. If R is a ring with identity 1_R, it is easy to see that $1_R + I$ is the identity of R/I.

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings,

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R.

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely,

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R,

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

is an epimorphism

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

is an epimorphism of rings

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

is an epimorphism of rings with kernel I.

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R.

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R. Conversely, since I is a subgroup of the abelian group R,

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R. Conversely, since I is a subgroup of the abelian group R, by Theorem (I.5.5), the map π is an epimorphism of groups with kernel I.

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r+I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R. Conversely, since I is a subgroup of the abelian group R, by Theorem (I.5.5), the map π is an epimorphism of groups with kernel I. Moreover, for all $a, b \in R$,

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R. Conversely, since I is a subgroup of the abelian group R, by Theorem (I.5.5), the map π is an epimorphism of groups with kernel I. Moreover, for all $a, b \in R$, $\pi(ab) = ab + I$

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r+I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R. Conversely, since I is a subgroup of the abelian group R, by Theorem (I.5.5), the map π is an epimorphism of groups with kernel I. Moreover, for all $a, b \in R$, $\pi(ab) = ab + I$
$= (a + I)(b + I)$

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r+I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R. Conversely, since I is a subgroup of the abelian group R, by Theorem (I.5.5), the map π is an epimorphism of groups with kernel I. Moreover, for all $a, b \in R$, $\pi(ab) = ab + I$ $= (a+I)(b+I) = \pi(a)\pi(b)$.

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r+I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R. Conversely, since I is a subgroup of the abelian group R, by Theorem (I.5.5), the map π is an epimorphism of groups with kernel I. Moreover, for all $a, b \in R$, $\pi(ab) = ab + I$ $= (a+I)(b+I) = \pi(a)\pi(b)$. Thus π is a ring homomorphism,

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r+I \end{array}$$

is an epimorphism of rings with kernel I.

Proof. In a previous remark, we have proved that $\mathrm{Ker}\ f$ is an ideal in R. Conversely, since I is a subgroup of the abelian group R, by Theorem (I.5.5), the map π is an epimorphism of groups with kernel I. Moreover, for all $a, b \in R$, $\pi(ab) = ab + I$ $= (a+I)(b+I) = \pi(a)\pi(b)$. Thus π is a ring homomorphism, and so π is an epimorphism of rings.

Theorem (2.8)

If $f : R \to S$ is a homomorphism of rings, then $\mathrm{Ker}\ f$ is an ideal in R. Conversely, if I is an ideal in R, then the map

$$\begin{array}{rcccc} \pi & : & R & \longrightarrow & R/I \\ & & r & \longmapsto & r + I \end{array}$$

is an epimorphism of rings with kernel I.

Definition. The map π is called the canonical epimorphism or the canonical projection.

Exercise for Section III.2

1, 2, 3, 10, 11, 13, 16, 18.