Algebraic Structure (代数结构)
Chapter 2: Ring Fundamentals

刘胜利

liu-sl@cs.sjtu.edu.cn
密码与信息安全实验室
计算机科学与工程系
上海交通大学

Rings

Definition 1.1 (Ring)

A ring $R(+,\cdot)$ is an abelian additive group with a multiplication operation $(a,b)\mapsto ab$ that is associative and satisfies:

- **Distributive law:** $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$ for all $a,b,c\in R$;

If there is a element 1 satisfying $a1=1a=a$ for all a in R. Then we call the element 1 the multiplicative identity, written simply as 1, and the additive identity as 0.

环$(R,+,\cdot)$的性质

- $(R,+)$构成一个交换群；
- $(R,\cdot)$构成一个半群：满足封闭性和结合律；
- 加法对乘法满足分配律。

如果$(R,\cdot)$有单位元1，就称R是一个有单位元的环；如果$(R,\cdot)$满足交换律，就称R是一个交换环；

Rings

Definition 1.1 (Ring)

A ring $R(+,\cdot)$ is an abelian additive group with a multiplication operation $(a,b)\mapsto ab$ that is associative and satisfies:

- **Distributive law:** $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$ for all $a,b,c\in R$;

If there is a element 1 satisfying $a1=1a=a$ for all a in R. Then we call the element 1 the multiplicative identity, written simply as 1, and the additive identity as 0.

环$(R,+,\cdot)$的性质

- $(R,+)$构成一个交换群；
- $(R,\cdot)$构成一个半群：满足封闭性和结合律；
- 加法对乘法满足分配律。

如果$(R,\cdot)$有单位元1，就称R是一个有单位元的环；如果$(R,\cdot)$满足交换律，就称R是一个交换环；

Rings

Definition 1.1 (Ring)

A ring $R(+,\cdot)$ is an abelian additive group with a multiplication operation $(a,b) \mapsto ab$ that is associative and satisfies:

- **Distributive law:** $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in R$;

If there is a element 1 satisfying $a1 = 1a = a$ for all a in R. Then we call the element 1 the multiplicative identity, written simply as 1, and the additive identity as 0.

环$(R,+,\cdot)$的性质

- $(R,+)$构成一个交换群；
- $(R,\cdot)$构成一个半群：满足封闭性和结合律；
- 加法对乘法满足分配律。

如果$(R,\cdot)$有单位元1，就称R是一个有单位元的环；如果$(R,\cdot)$满足交换律，就称R是一个交换环；

Rings

Definition 1.1 (Ring)

A ring $R(+,\cdot)$ is an abelian additive group with a multiplication operation $(a,b)\mapsto ab$ that is associative and satisfies:

- **Distributive law:** $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$ for all $a,b,c\in R$;

If there is a element 1 satisfying $a1=1a=a$ for all a in R. Then we call the element 1 the multiplicative identity, written simply as 1, and the additive identity as 0.

环$(R,+,\cdot)$的性质

- $(R,+)$构成一个交换群；
- $(R,\cdot)$构成一个半群：满足封闭性和结合律；
- 加法对乘法满足分配律。

如果$(R,\cdot)$有单位元1，就称R是一个有单位元的环；如果$(R,\cdot)$满足交换律，就称R是一个交换环；

Rings

Definition 1.1 (Ring)

A ring $R(+,\cdot)$ is an abelian additive group with a multiplication operation $(a,b)\mapsto ab$ that is associative and satisfies:

- **Distributive law:** $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$ for all $a,b,c\in R$;

If there is a element 1 satisfying $a1=1a=a$ for all a in R. Then we call the element 1 the multiplicative identity, written simply as 1, and the additive identity as 0.

环$(R,+,\cdot)$的性质

- $(R,+)$构成一个交换群；
- $(R,\cdot)$构成一个半群：满足封闭性和结合律；
- 加法对乘法满足分配律。

如果$(R,\cdot)$有单位元1，就称R是一个有单位元的环；如果$(R,\cdot)$满足交换律，就称R是一个交换环；

Rings

Definition 1.1 (Ring)

A ring $R(+,\cdot)$ is an abelian additive group with a multiplication operation $(a,b)\mapsto ab$ that is associative and satisfies:

- **Distributive law:** $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$ for all $a,b,c\in R$;

If there is a element 1 satisfying $a1=1a=a$ for all a in R. Then we call the element 1 the multiplicative identity, written simply as 1, and the additive identity as 0.

环$(R,+,\cdot)$的性质

- $(R,+)$构成一个交换群;
- $(R,\cdot)$构成一个半群:满足封闭性和结合律;
- 加法对乘法满足分配律。

如果$(R,\cdot)$有单位元1,就称R是一个有单位元的环;如果$(R,\cdot)$满足交换律,就称R是一个交换环;

Rings

特殊的环：零环$R = 0$。

Fact 1.2

If $a, b, c \in R$ while R is a ring, then we have the following properties.

1. $a0 = 0a = 0$.
2. $(-a)b = a(-b) = -(ab)$.
3. $(-1)(-1) = 1$.
4. $(-a)(-b) = ab$.
5. $a(b - c) = ab - ac$.
6. $(a - b)c = ac - bc$.
7. $1 \neq 0$. 如果R中至少有两个元素，则$1 \neq 0$。
8. 1 *is unique.*

零因子，单位，整环，除环

Definition 1.3 (Zero Divisors and Unit)

- If a and b are nonzero but $ab = 0$, then a and b are zero divisors.
- If $a \in R$ and for some $b \in R$ we have $ab = ba = 1$, we say a is a unit or *invertible*.

- Cancelation law holds in R iff there is no zero divisors in R.
- All units of R forms a multiplicative group, denoted by $(R^*, \cdot)$.

Definition 1.4 (Integral Domain)

An integral domain is a ring that is commutative under multiplication, has a multiplicative identity element, and has no divisors of 0.

Example: $\mathbb{Z}$.

零因子，单位，整环，除环

Definition 1.3 (Zero Divisors and Unit)

- If a and b are nonzero but $ab = 0$, then a and b are zero divisors.
- If $a \in R$ and for some $b \in R$ we have $ab = ba = 1$, we say a is a unit or *invertible*.

- Cancelation law holds in R iff there is no zero divisors in R.
- All units of R forms a multiplicative group, denoted by $(R^*, \cdot)$.

Definition 1.4 (Integral Domain)

An integral domain is a ring that is commutative under multiplication, has a multiplicative identity element, and has no divisors of 0.

Example: $\mathbb{Z}$.

零因子，单位，整环，除环

Definition 1.3 (Zero Divisors and Unit)

- If a and b are nonzero but $ab = 0$, then a and b are zero divisors.
- If $a \in R$ and for some $b \in R$ we have $ab = ba = 1$, we say a is a unit or *invertible*.

- Cancelation law holds in R iff there is no zero divisors in R.
- All units of R forms a multiplicative group, denoted by $(R^*, \cdot)$.

Definition 1.4 (Integral Domain)

An integral domain is a ring that is commutative under multiplication, has a multiplicative identity element, and has no divisors of 0.

Example: $\mathbb{Z}$.

零因子，单位，整环，除环

Definition 1.3 (Zero Divisors and Unit)

- If a and b are nonzero but $ab = 0$, then a and b are zero divisors.
- If $a \in R$ and for some $b \in R$ we have $ab = ba = 1$, we say a is a unit or *invertible*.

- Cancelation law holds in R iff there is no zero divisors in R.
- All units of R forms a multiplicative group, denoted by $(R^*, \cdot)$.

Definition 1.4 (Integral Domain)

An integral domain is a ring that is commutative under multiplication, has a multiplicative identity element, and has no divisors of 0.

Example: $\mathbb{Z}$.

零因子，单位，整环，除环

Definition 1.3 (Zero Divisors and Unit)

- If a and b are nonzero but $ab = 0$, then a and b are zero divisors.
- If $a \in R$ and for some $b \in R$ we have $ab = ba = 1$, we say a is a unit or *invertible*.

- Cancelation law holds in R iff there is no zero divisors in R.
- All units of R forms a multiplicative group, denoted by $(R^*, \cdot)$.

Definition 1.4 (Integral Domain)

An integral domain is a ring that is commutative under multiplication, has a multiplicative identity element, and has no divisors of 0.

Example: $\mathbb{Z}$.

除环和域

Definition 1.5 (division ring)

An division ring is a ring in which every nonzero element a has a multiplicative inverse a^{-1}

Definition 1.6 (field)

- A field is a commutative division ring.

Fact 1.7

Any finite integral domain is a field

Proof.

Observe that if $a \neq 0$, the map $x \to ax, x \in R$, is injective because R is an integral domain.
If R is finite, the map is surjective as well, so that $ax = 1$ for some x. □

除环和域

Definition 1.5 (division ring)

An division ring is a ring in which every nonzero element a has a multiplicative inverse a^{-1}

Definition 1.6 (field)

- A field is a commutative division ring.

Fact 1.7

Any finite integral domain is a field

Proof.

Observe that if $a \neq 0$, the map $x \to ax, x \in R$, is injective because R is an integral domain.
If R is finite, the map is surjective as well, so that $ax = 1$ for some x. □

除环和域

Definition 1.5 (division ring)

An division ring is a ring in which every nonzero element a has a multiplicative inverse a^{-1}

Definition 1.6 (field)

- A field is a commutative division ring.

Fact 1.7

Any finite integral domain is a field

Proof.

Observe that if $a \neq 0$, the map $x \to ax, x \in R$, is injective because R is an integral domain.
If R is finite, the map is surjective as well, so that $ax = 1$ for some x. □

环的特征

Definition 1.8 (characteristic)

The characteristic of a ring R (written Char R) is the smallest positive integer such that $n1 = 0$, where $n1$ is an abbreviation for $1 + 1 + \ldots + 1$ (n times).

- If $n1$ is never 0, we say R has characteristic 0.
- If R is an integral domain and Char $R \neq 0$, then Char R must be a prime number. For if Char $R = n = rs$ where r and s are positive integers greater than 1, then $(r1)(s1) = n1 = 0$, so either $r1$ or $s1$ is 0, contradicting the minimality of n.

环的特征

Definition 1.8 (characteristic)

The characteristic of a ring R (written Char R) is the smallest positive integer such that $n1 = 0$, where $n1$ is an abbreviation for $1 + 1 + \ldots + 1$ (n times).

- If $n1$ is never 0, we say R has characteristic 0.
- If R is an integral domain and Char $R \neq 0$, then Char R must be a prime number. For if Char $R = n = rs$ where r and s are positive integers greater than 1, then $(r1)(s1) = n1 = 0$, so either $r1$ or $s1$ is 0, contradicting the minimality of n.

环的特征

Definition 1.8 (characteristic)

The characteristic of a ring R (written Char R) is the smallest positive integer such that $n1 = 0$, where $n1$ is an abbreviation for $1 + 1 + \ldots + 1$ (n times).

- If $n1$ is never 0, we say R has characteristic 0.
- If R is an integral domain and Char $R \neq 0$, then Char R must be a prime number. For if Char $R = n = rs$ where r and s are positive integers greater than 1, then $(r1)(s1) = n1 = 0$, so either $r1$ or $s1$ is 0, contradicting the minimality of n.

环的特征

Definition 1.8 (characteristic)

The characteristic of a ring R (written Char R) is the smallest positive integer such that $n1 = 0$, where $n1$ is an abbreviation for $1 + 1 + \ldots + 1$ (n times).

- If $n1$ is never 0, we say R has characteristic 0.
- If R is an integral domain and Char $R \neq 0$, then Char R must be a prime number. For if Char $R = n = rs$ where r and s are positive integers greater than 1, then $(r1)(s1) = n1 = 0$, so either $r1$ or $s1$ is 0, contradicting the minimality of n.

环的示例

Examples 1.9

1. The integers $\mathbb{Z}$ form an integral domain that is not a field.
2. Let $\mathbb{Z}_n$ be the integers modulo n, that is, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition and multiplication mod n.$\mathbb{Z}_n$ is a ring, which is a field iff n is prime.
3. If $n \geq 2$, then the set $M_n(R)$ of all n by n matrices with coefficients from a ring R forms a noncommutative ring.
4. If R is a ring, then $R[X]$, the set of all polynomials in X with coefficients in R, is also a ring under ordinary polynomial addition and multiplication, as is $R[X_1, \ldots, X_n]$, the set of polynomials in n variables $X_i, 1 \leq i \leq n$, with coefficients in R.

环的示例

Examples 1.9

1. The integers $\mathbb{Z}$ form an integral domain that is not a field.
2. Let $\mathbb{Z}_n$ be the integers modulo n, that is, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition and multiplication mod n. $\mathbb{Z}_n$ is a ring, which is a field iff n is prime.
3. If $n \geq 2$, then the set $M_n(R)$ of all n by n matrices with coefficients from a ring R forms a noncommutative ring.
4. If R is a ring, then $R[X]$, the set of all polynomials in X with coefficients in R, is also a ring under ordinary polynomial addition and multiplication, as is $R[X_1, \ldots, X_n]$, the set of polynomials in n variables $X_i, 1 \leq i \leq n$, with coefficients in R.

环的示例

Examples 1.9

1. The integers $\mathbb{Z}$ form an integral domain that is not a field.
2. Let $\mathbb{Z}_n$ be the integers modulo n, that is, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition and multiplication mod n.$\mathbb{Z}_n$ is a ring, which is a field iff n is prime.
3. If $n \geq 2$, then the set $M_n(R)$ of all n by n matrices with coefficients from a ring R forms a noncommutative ring.
4. If R is a ring, then $R[X]$, the set of all polynomials in X with coefficients in R, is also a ring under ordinary polynomial addition and multiplication, as is $R[X_1, \ldots, X_n]$, the set of polynomials in n variables $X_i, 1 \leq i \leq n$, with coefficients in R.

环的示例

Examples 1.9

1. The integers $\mathbb{Z}$ form an integral domain that is not a field.
2. Let $\mathbb{Z}_n$ be the integers modulo n, that is, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition and multiplication mod $n.\mathbb{Z}_n$ is a ring, which is a field iff n is prime.
3. If $n \geq 2$, then the set $M_n(R)$ of all n by n matrices with coefficients from a ring R forms a noncommutative ring.
4. If R is a ring, then $R[X]$, the set of all polynomials in X with coefficients in R, is also a ring under ordinary polynomial addition and multiplication, as is $R[X_1, \ldots, X_n]$, the set of polynomials in n variables $X_i, 1 \leq i \leq n$, with coefficients in R.

环上的广义分配律

Lemma 1.10 (Generalized associative law)

The generalized associative law holds for multiplication in a ring. There is also a generalized distributive law:

$$(a_1 + \ldots + a_m)(b_1 + \ldots + b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j.$$

Proof.

- First set $m = 1$ and work by induction on n, using the left distributive law $a(b + c) = ab + ac$.
- Then use induction on m and the right distributive law $(a + b)c = ac + bc$ on $(a_1 + \ldots + a_m + a_{m+1})(b_1 + \ldots + b_n)$.

□

环上的广义分配律

Lemma 1.10 (Generalized associative law)

The generalized associative law holds for multiplication in a ring. There is also a generalized distributive law:

$$(a_1 + \ldots + a_m)(b_1 + \ldots + b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j.$$

Proof.

- First set $m = 1$ and work by induction on n, using the left distributive law $a(b + c) = ab + ac$.
- Then use induction on m and the right distributive law $(a + b)c = ac + bc$ on $(a_1 + \ldots + a_m + a_{m+1})(b_1 + \ldots + b_n)$.

□

环上的二项式定理

Lemma 1.11 (Binomial Theorem)

The Binomial Theorem $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ *is valid in any ring, if* $ab = ba$.

Proof.

Easy to prove by induction. □

环上的二项式定理

Lemma 1.11 (Binomial Theorem)

The Binomial Theorem $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ *is valid in any ring, if* $ab = ba$.

Proof.

Easy to prove by induction. □

子环及其性质

Definition 1.12 (subring)

A subring of a ring R is a subset S or R that forms a ring under the operation of addition and multipliation defined on R.

Theorem 1.13 (子环的交仍是子环)

设R_1, R_2是R的子环，记为$R_1, R_2 \leq R$。那么$R_1 \cap R_2$也是R的子环。

Definition 1.14 (集合生成的子环，子环的生成元集)

设S是环R的子集，记为$S \subseteq R$。R中含子集S的最小的子环，称为集合S在R中生成的子环，记为$< S >$，并称S是$< S >$的生成元集。

Theorem 1.15 (集合生成的子环的性质)

设Σ是R中所有含集合S的子环组成的集合。则$\bigcap_{A \in \Sigma} A$为R中含S最小的子环，且$< S > = \bigcap_{A \in \Sigma} A$。

子环及其性质

Definition 1.12 (subring)

A subring of a ring R is a subset S or R that forms a ring under the operation of addition and multipliation defined on R.

Theorem 1.13 (子环的交仍是子环)

设R_1, R_2是R的子环，记为$R_1, R_2 \leq R$。那么$R_1 \cap R_2$也是R的子环。

Definition 1.14 (集合生成的子环，子环的生成元集)

设S是环R的子集，记为$S \subseteq R$。R中含子集S的最小的子环，称为集合S在R中生成的子环，记为$< S >$，并称S是$< S >$的生成元集。

Theorem 1.15 (集合生成的子环的性质)

设Σ是R中所有含集合S的子环组成的集合。则$\bigcap_{A\in\Sigma} A$为R中含S最小的子环，且$< S > = \bigcap_{A\in\Sigma} A$。

子环及其性质

Definition 1.12 (subring)

A subring of a ring R is a subset S or R that forms a ring under the operation of addition and multipliation defined on R.

Theorem 1.13 (子环的交仍是子环)

设R_1, R_2是R的子环，记为$R_1, R_2 \leq R$。那么$R_1 \cap R_2$也是R的子环。

Definition 1.14 (集合生成的子环，子环的生成元集)

设S是环R的子集，记为$S \subseteq R$。R中含子集S的最小的子环，称为集合S在R中生成的子环，记为$< S >$，并称S是$< S >$的生成元集。

Theorem 1.15 (集合生成的子环的性质)

设Σ是R中所有含集合S的子环组成的集合。则$\bigcap_{A \in \Sigma} A$为R中含S最小的子环，且$< S > = \bigcap_{A \in \Sigma} A$。

子环及其性质

Definition 1.12 (subring)

A subring of a ring R is a subset S or R that forms a ring under the operation of addition and multipliation defined on R.

Theorem 1.13 (子环的交仍是子环)

设R_1, R_2是R的子环，记为$R_1, R_2 \leq R$。那么$R_1 \cap R_2$也是R的子环。

Definition 1.14 (集合生成的子环，子环的生成元集)

设S是环R的子集，记为$S \subseteq R$。R中含子集S的最小的子环，称为集合S在R中生成的子环，记为$< S >$，并称S是$< S >$的生成元集。

Theorem 1.15 (集合生成的子环的性质)

设Σ是R中所有含集合S的子环组成的集合。则$\bigcap_{A \in \Sigma} A$为R中含S最小的子环，且$< S > = \bigcap_{A \in \Sigma} A$。

Examples for subrings

对于任意的整数d，$d\mathbb{Z}$是$\mathbb{Z}$的子环。
$\mathbb{Z}[i] = \{a + b\sqrt{-1},\ a, b \in \mathbb{Z}\}$是一个整环，称为高斯整环。
对于$\mathbb{Z}$的任意子环，其形式都是$d\mathbb{Z}$。

Homomorphisms

Definition 2.1 (ring homomorphism)

If $f : R \mapsto S$, where R and S are rings, we say that f is a ring homomorphism if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$, and $f(1_R) = 1_S$.

环同态只涉及有1环。

Example 2.2

Let $f : \mathbb{Z} \mapsto M_n(R), n \geq 2$, be defined by $f(n) = nE_{11}$ (E_{11} means matrix with 1 in row 1 and col 1, and 0's elsewhere). Then we have $f(a+b) = f(a) + f(b), f(ab) = f(a)f(b)$, but $f(1) \neq I_n$. Thus f is not a ring homomorphism.

Homomorphisms

Definition 2.1 (ring homomorphism)

If $f : R \mapsto S$, where R and S are rings, we say that f is a ring homomorphism if $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$, and $f(1_R) = 1_S$.

环同态只涉及有1环。

Example 2.2

Let $f : \mathbb{Z} \mapsto M_n(R), n \geq 2$, be defined by $f(n) = nE_{11}$ (E_{11} means matrix with 1 in row 1 and col 1, and 0's elsewhere). Then we have $f(a + b) = f(a) + f(b), f(ab) = f(a)f(b)$, but $f(1) \neq I_n$. Thus f is not a ring homomorphism.

Homomorphisms

Definition 2.1 (ring homomorphism)

If $f : R \mapsto S$, where R and S are rings, we say that f is a ring homomorphism if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$, and $f(1_R) = 1_S$.

环同态只涉及有1环。

Example 2.2

Let $f : \mathbb{Z} \mapsto M_n(R), n \geq 2$, be defined by $f(n) = nE_{11}$ (E_{11} means matrix with 1 in row 1 and col 1, and 0's elsewhere). Then we have $f(a+b) = f(a) + f(b), f(ab) = f(a)f(b)$, but $f(1) \neq I_n$. Thus f is not a ring homomorphism.

环同态的核

Definition 2.3 (Kernel)

If $f : R \mapsto S$ is a ring homomorphism, its kernel is:

$$\mathrm{Ker} f = \{r \in R : f(r) = 0\};$$

f is injective iff $\mathrm{Ker} f = \{0\}$.

设K是环同态$f : R \mapsto S$ 的内核，即$K = \mathrm{Ker} f$。则

- K是R的一个子环；若$a, b \in K$，则

  $$f(a - b) = f(a) - f(b) = 0 - 0 = 0,$$

  即$a - b \in K$，所以$(K, +)$是R的子群；
  若$a, b \in K$，则$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0$，
  满足封闭性，所以$(K, \cdot)$是一个半群。
- K是一种特殊的子环：若$a \in K, r \in R$，

  $$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0, \quad f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$$

环同态的核

Definition 2.3 (Kernel)

If $f : R \mapsto S$ is a ring homomorphism, its kernel is:

$$\mathrm{Ker} f = \{r \in R : f(r) = 0\};$$

f is injective iff $\mathrm{Ker} f = \{0\}$.

设K是环同态$f : R \mapsto S$ 的内核，即$K = \mathrm{Ker} f$。则

- K是R的一个子环；若$a, b \in K$，则

  $$f(a-b) = f(a) - f(b) = 0 - 0 = 0,$$

  即$a - b \in K$，所以$(K, +)$是R的子群；
  若$a, b \in K$，则$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0$，
  满足封闭性，所以$(K, \cdot)$是一个半群。
- K是一种特殊的子环：若$a \in K, r \in R$，

  $$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0 \qquad f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$$

环同态的核

Definition 2.3 (Kernel)

If $f : R \mapsto S$ is a ring homomorphism, its kernel is:

$$\mathrm{Ker} f = \{r \in R : f(r) = 0\};$$

f is injective iff $\mathrm{Ker} f = \{0\}$.

设K是环同态$f : R \mapsto S$ 的内核，即$K = \mathrm{Ker} f$。则

- K是R的一个子环；若$a, b \in K$，则

  $$f(a - b) = f(a) - f(b) = 0 - 0 = 0,$$

  即$a - b \in K$，所以$(K, +)$是R的子群；

  若$a, b \in K$，则$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0$，

  满足封闭性，所以$(K, \cdot)$是一个半群。

- K是一种特殊的子环：若$a \in K, r \in R$，

  $$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0, \quad f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$$

环同态的核

Definition 2.3 (Kernel)

If $f : R \mapsto S$ is a ring homomorphism, its kernel is:

$$\mathrm{Ker} f = \{r \in R : f(r) = 0\};$$

f is injective iff $\mathrm{Ker} f = \{0\}$.

设K是环同态$f : R \mapsto S$ 的内核，即$K = \mathrm{Ker} f$。则

- K是R的一个子环；若$a, b \in K$，则

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0,$$

  即$a - b \in K$，所以$(K, +)$是R的子群；
  若$a, b \in K$，则$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0$，
  满足封闭性，所以$(K, \cdot)$是一个半群。
- K是一种特殊的子环：若$a \in K, r \in R$，

$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0 \qquad f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$$

环同态的核

Definition 2.3 (Kernel)

If $f : R \mapsto S$ is a ring homomorphism, its kernel is:

$$\mathrm{Ker} f = \{r \in R : f(r) = 0\};$$

f is injective iff $\mathrm{Ker} f = \{0\}$.

设K是环同态$f : R \mapsto S$ 的内核，即$K = \mathrm{Ker} f$。则

- K是R的一个子环；若$a, b \in K$，则

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0,$$

  即$a - b \in K$，所以$(K, +)$是R的子群；
  若$a, b \in K$，则$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0$，
  满足封闭性，所以$(K, \cdot)$是一个半群。
- K是一种特殊的子环：若$a \in K, r \in R$，

$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0, \qquad f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$$

Ideals

Definition 2.4 (Ideals)

Let I be a subset of the ring R, and consider the following three properties:

1. I is an additive subgroup of R;
2. If $a \in I$ and $r \in R$ then $ra \in I$, i.e., $rI \subseteq I$ for every $r \in R$;
3. If $a \in I$ and $r \in R$ then $ar \in I$, i.e., $Ir \subseteq I$ for every $r \in R$

If (1) and (2) hold, I is said to be a left ideal of R.
If (1) and (3) hold, I is said to be a right ideal of R.
If all three properties are satisfied, I is said to be an ideal of R, a proper ideal if $I \neq R$, a nontrivial ideal if I is either R nor $\{0\}$.

Fact 2.5

$Kerf$ is an ideal of R.

Ideals

Definition 2.4 (Ideals)

Let I be a subset of the ring R, and consider the following three properties:

1. I is an additive subgroup of R;
2. If $a \in I$ and $r \in R$ then $ra \in I$, i.e., $rI \subseteq I$ for every $r \in R$;
3. If $a \in I$ and $r \in R$ then $ar \in I$, i.e., $Ir \subseteq I$ for every $r \in R$

If (1) and (2) hold, I is said to be a left ideal of R.
If (1) and (3) hold, I is said to be a right ideal of R.
If all three properties are satisfied, I is said to be an ideal of R, a proper ideal if $I \neq R$, a nontrivial ideal if I is either R nor $\{0\}$.

Fact 2.5

$Kerf$ is an ideal of R.

Ideals

Definition 2.4 (Ideals)

Let I be a subset of the ring R, and consider the following three properties:

1. I is an additive subgroup of R;
2. If $a \in I$ and $r \in R$ then $ra \in I$, i.e., $rI \subseteq I$ for every $r \in R$;
3. If $a \in I$ and $r \in R$ then $ar \in I$, i.e., $Ir \subseteq I$ for every $r \in R$

If (1) and (2) hold, I is said to be a left ideal of R.
If (1) and (3) hold, I is said to be a right ideal of R.
If all three properties are satisfied, I is said to be an ideal of R, a proper ideal if $I \neq R$, a nontrivial ideal if I is either R nor $\{0\}$.

Fact 2.5

$Ker f$ is an ideal of R.

Ideals

Definition 2.4 (Ideals)

Let I be a subset of the ring R, and consider the following three properties:

1. I is an additive subgroup of R;
2. If $a \in I$ and $r \in R$ then $ra \in I$, i.e., $rI \subseteq I$ for every $r \in R$;
3. If $a \in I$ and $r \in R$ then $ar \in I$, i.e., $Ir \subseteq I$ for every $r \in R$

If (1) and (2) hold, I is said to be a left ideal of R.
If (1) and (3) hold, I is said to be a right ideal of R.
If all three properties are satisfied, I is said to be an ideal of R, a proper ideal if $I \neq R$, a nontrivial ideal if I is either R nor $\{0\}$.

Fact 2.5

$Kerf$ is an ideal of R.

Ideals

Definition 2.4 (Ideals)

Let I be a subset of the ring R, and consider the following three properties:

1. I is an additive subgroup of R;
2. If $a \in I$ and $r \in R$ then $ra \in I$, i.e., $rI \subseteq I$ for every $r \in R$;
3. If $a \in I$ and $r \in R$ then $ar \in I$, i.e., $Ir \subseteq I$ for every $r \in R$

If (1) and (2) hold, I is said to be a left ideal of R.
If (1) and (3) hold, I is said to be a right ideal of R.
If all three properties are satisfied, I is said to be an ideal of R, a proper ideal if $I \neq R$, a nontrivial ideal if I is either R nor $\{0\}$.

Fact 2.5

$Kerf$ is an ideal of R.

Quotient Rings

Definition 2.6 (Quotient Rings)

Let I be a proper ideal of R. we can define $R/I = \{r + I : r \in R\}$ and the multiplication of cosets in the natural way:

$$(r + I)(s + I) = rs + I.$$

Then $(R/I,$ 陪集加法，陪集乘法$)$ forms a ring, called the quotient ring of R by I.

商环的性质

$(R/I,$ 陪集加法)构成了商群；

R/I中所定义的陪集乘法$(r+I)(s+I)=rs+I$的合理性：

设$r+I=r'+I$且$s+I=s'+I$，则$\exists i_r, i_s \in I$使得$r=r'+i_r$且$s=s'+i_s$。

由于$rs-r's'=(r'+i_r)(s'+i_s)-r's'=i_rs'+r'i_s+i_ri_s \in I$，所以$rs+I=r's'+I$。

- If R has an identity, then the identity of R/I is $1+I$.
- The zero element is $0+I$.
- If R is a commutative ring, so is R/I.

商环的性质

$(R/I,$ 陪集加法)构成了商群；
R/I中所定义的陪集乘法$(r+I)(s+I)=rs+I$的合理性：
设$r+I=r'+I$且$s+I=s'+I$，则$\exists i_r, i_s \in I$使得$r=r'+i_r$且$s=s'+i_s$。
由于$rs-r's'=(r'+i_r)(s'+i_s)-r's'=i_rs'+r'i_s+i_ri_s \in I$，所以$rs+I=r's'+I$。

- If R has an identity, then the identity of R/I is $1+I$.
- The zero element is $0+I$.
- If R is a commutative ring, so is R/I.

商环的性质

$(R/I,$ 陪集加法$)$构成了商群；

R/I中所定义的陪集乘法$(r+I)(s+I)=rs+I$的合理性：

设$r+I=r'+I$且$s+I=s'+I$，则$\exists i_r, i_s \in I$使得$r=r'+i_r$且$s=s'+i_s$。

由于$rs-r's'=(r'+i_r)(s'+i_s)-r's'=i_rs'+r'i_s+i_ri_s \in I$，所以$rs+I=r's'+I$。

- If R has an identity, then the identity of R/I is $1+I$.
- The zero element is $0+I$.
- If R is a commutative ring, so is R/I.

商环的性质

$(R/I,$ 陪集加法$)$构成了商群；
R/I中所定义的陪集乘法$(r+I)(s+I)=rs+I$的合理性：
设$r+I=r'+I$且$s+I=s'+I$，则$\exists i_r, i_s \in I$使得$r=r'+i_r$且$s=s'+i_s$。
由于$rs-r's'=(r'+i_r)(s'+i_s)-r's'=i_rs'+r'i_s+i_ri_s \in I$，所以$rs+I=r's'+I$。

- If R has an identity, then the identity of R/I is $1+I$.
- The zero element is $0+I$.
- If R is a commutative ring, so is R/I.

商环的性质

$(R/I,$ 陪集加法)构成了商群；
R/I中所定义的陪集乘法$(r+I)(s+I)=rs+I$的合理性：
设$r+I=r'+I$且$s+I=s'+I$，则$\exists i_r, i_s \in I$使得$r=r'+i_r$且$s=s'+i_s$。
由于$rs-r's'=(r'+i_r)(s'+i_s)-r's'=i_rs'+r'i_s+i_ri_s \in I$，所以$rs+I=r's'+I$。

- If R has an identity, then the identity of R/I is $1+I$.
- The zero element is $0+I$.
- If R is a commutative ring, so is R/I.

商环的性质

$(R/I,$ 陪集加法)构成了商群；
R/I中所定义的陪集乘法$(r+I)(s+I)=rs+I$的合理性：
设$r+I=r'+I$且$s+I=s'+I$，则$\exists i_r, i_s \in I$使得$r=r'+i_r$且$s=s'+i_s$。
由于$rs-r's'=(r'+i_r)(s'+i_s)-r's'=i_rs'+r'i_s+i_ri_s \in I$，所以$rs+I=r's'+I$。

- If R has an identity, then the identity of R/I is $1+I$.
- The zero element is $0+I$.
- If R is a commutative ring, so is R/I.

商环的性质

$(R/I,$ 陪集加法)构成了商群；
R/I中所定义的陪集乘法$(r+I)(s+I)=rs+I$的合理性：
设$r+I=r'+I$且$s+I=s'+I$，则$\exists i_r, i_s \in I$使得$r=r'+i_r$且$s=s'+i_s$。
由于$rs-r's'=(r'+i_r)(s'+i_s)-r's'=i_rs'+r'i_s+i_ri_s \in I$，所以$rs+I=r's'+I$。

- If R has an identity, then the identity of R/I is $1+I$.
- The zero element is $0+I$.
- If R is a commutative ring, so is R/I.

理想与环同态内核的关系

Lemma 2.7

Every proper ideal I is the kernel of a ring homomorphism.

Proof.

Define a natural map $\pi : R \mapsto R/I$ by $\pi(r) = r + I$. We know its kernel is I. To verify π preserves multiplication, note that

$$\pi(rs) = rs + I = (r + I)(s + I) = \pi(r)\pi(s);$$

since

$$\pi(1_R) = 1_R + I = 1_{R/I},$$

π is a ring homomorphism. □

理想与环同态内核的关系

Lemma 2.7

Every proper ideal I is the kernel of a ring homomorphism.

Proof.

Define a natural map $\pi : R \mapsto R/I$ by $\pi(r) = r + I$. We know its kernel is I. To verify π preserves multiplication, note that

$$\pi(rs) = rs + I = (r + I)(s + I) = \pi(r)\pi(s);$$

since

$$\pi(1_R) = 1_R + I = 1_{R/I},$$

π is a ring homomorphism. □

单环同态

Lemma 2.8

If $f : R \mapsto S$ is a ring homomorphism and the only ideals of R are $\{0\}$ and R, then R is injective.

Proof.

Let $I = \mathrm{Ker} f$. If $I = R$ then f is identically zero, and is therefore not legal since $f(1_R) = 1_S \neq 0_S$. Thus $I = \{0\}$, so that f is injective. □

- 如果一个有1环只存在平凡理想，那么，这个环所可能定义的环同态是一个单同态；
- 除环只存在平凡理想，因此除环只能定义一个单环同态；
- 域只存在平凡理想，因此域也只能定义一个单环同态。

单环同态

Lemma 2.8

If $f : R \mapsto S$ is a ring homomorphism and the only ideals of R are $\{0\}$ and R, then R is injective.

Proof.

Let $I = \mathrm{Ker} f$. If $I = R$ then f is identically zero, and is therefore not legal since $f(1_R) = 1_S \neq 0_S$. Thus $I = \{0\}$, so that f is injective. □

- 如果一个有1环只存在平凡理想，那么，这个环所可能定义的环同态是一个单同态；
- 除环只存在平凡理想，因此除环只能定义一个单环同态；
- 域只存在平凡理想，因此域也只能定义一个单环同态。

单环同态

Lemma 2.8

If $f : R \mapsto S$ is a ring homomorphism and the only ideals of R are $\{0\}$ and R, then R is injective.

Proof.

Let $I = \mathrm{Ker} f$. If $I = R$ then f is identically zero, and is therefore not legal since $f(1_R) = 1_S \neq 0_S$. Thus $I = \{0\}$, so that f is injective. □

- 如果一个有1环只存在平凡理想，那么，这个环所可能定义的环同态是一个单同态；
- 除环只存在平凡理想，因此除环只能定义一个单环同态；
- 域只存在平凡理想，因此域也只能定义一个单环同态。

单环同态

Lemma 2.8

If $f : R \mapsto S$ is a ring homomorphism and the only ideals of R are $\{0\}$ and R, then R is injective.

Proof.

Let $I = \mathrm{Ker} f$. If $I = R$ then f is identically zero, and is therefore not legal since $f(1_R) = 1_S \neq 0_S$. Thus $I = \{0\}$, so that f is injective. □

- 如果一个有1环只存在平凡理想，那么，这个环所可能定义的环同态是一个单同态；
- 除环只存在平凡理想，因此除环只能定义一个单环同态；
- 域只存在平凡理想，因此域也只能定义一个单环同态。

单环同态

Lemma 2.8

If $f : R \mapsto S$ is a ring homomorphism and the only ideals of R are $\{0\}$ and R, then R is injective.

Proof.

Let $I = \mathrm{Ker} f$. If $I = R$ then f is identically zero, and is therefore not legal since $f(1_R) = 1_S \neq 0_S$. Thus $I = \{0\}$, so that f is injective. □

- 如果一个有1环只存在平凡理想，那么，这个环所可能定义的环同态是一个单同态；
- 除环只存在平凡理想，因此除环只能定义一个单环同态；
- 域只存在平凡理想，因此域也只能定义一个单环同态。

集合生成的理想、主理想

Definition 2.9 (ideal generated by a set)

If X is a nonempty subset of the ring R (R has 1), then $\langle X\rangle$ will denote the ideal generated by X, that is, the smallest ideal of R that contains X. Explicitly,

$\langle X\rangle = \left\{\sum_{x\in X} xr_i + \sum_{x\in X} r_j x + \sum_{x\in X} r_u x r_v + \sum_{x\in X} x \mid r_i, r_j, r_u, r_v \in R\right\}$

若R是一个有1环，则

$\langle X\rangle = \{\sum_{x\in X} r_u x r_v \mid r_u, r_v \in R\}$

若R是一个有1交换环，$\langle X\rangle = \{\sum_i r_i x_i \text{ with } r_i \in R \text{and } x_i \in X.\}$

- An ideal generated by a single element a is called a principal ideal and is denoted by $\langle a\rangle$. In this case, $X = \{a\}$.

集合生成的理想、主理想

Definition 2.9 (ideal generated by a set)

If X is a nonempty subset of the ring R (R has 1), then $\langle X\rangle$ will denote the ideal generated by X, that is, the smallest ideal of R that contains X. Explicitly,

$\langle X\rangle = \left\{\sum_{x\in X} xr_i + \sum_{x\in X} r_j x + \sum_{x\in X} r_u x r_v + \sum_{x\in X} x \mid r_i, r_j, r_u, r_v \in R\right\}$

若R是一个有1环，则

$\langle X\rangle = \{\sum_{x\in X} r_u x r_v \mid r_u, r_v \in R\}$

若R是一个有1交换环，$\langle X\rangle = \{\sum_i r_i x_i \text{ with } r_i \in R \text{and } x_i \in X.\}$

- An ideal generated by a single element a is called a principal ideal and is denoted by $\langle a\rangle$. In this case, $X = \{a\}$.

集合生成的理想、主理想

Definition 2.9 (ideal generated by a set)

If X is a nonempty subset of the ring R (R has 1), then $\langle X\rangle$ will denote the ideal generated by X, that is, the smallest ideal of R that contains X. Explicitly,

$\langle X\rangle = \left\{\sum_{x\in X} xr_i + \sum_{x\in X} r_j x + \sum_{x\in X} r_u x r_v + \sum_{x\in X} x \mid r_i, r_j, r_u, r_v \in R\right\}$

若R是一个有1环，则

$\langle X\rangle = \{\sum_{x\in X} r_u x r_v \mid r_u, r_v \in R\}$

若R是一个有1交换环，$\langle X\rangle = \{\sum_i r_i x_i \text{ with } r_i \in R \text{and } x_i \in X.\}$

- An ideal generated by a single element a is called a principal ideal and is denoted by $\langle a\rangle$. In this case, $X = \{a\}$.

集合生成的理想、主理想

Definition 2.9 (ideal generated by a set)

If X is a nonempty subset of the ring R (R has 1), then $\langle X\rangle$ will denote the ideal generated by X, that is, the smallest ideal of R that contains X. Explicitly,

$\langle X\rangle = \left\{\sum_{x\in X} xr_i + \sum_{x\in X} r_j x + \sum_{x\in X} r_u x r_v + \sum_{x\in X} x \mid r_i, r_j, r_u, r_v \in R\right\}$

若R是一个有1环，则

$\langle X\rangle = \{\sum_{x\in X} r_u x r_v \mid r_u, r_v \in R\}$

若R是一个有1交换环，$\langle X\rangle = \{\sum_i r_i x_i \text{ with } r_i \in R \text{and } x_i \in X.\}$

- An ideal generated by a single element a is called a principal ideal and is denoted by $\langle a\rangle$. In this case, $X = \{a\}$.

理想的性质

Fact 2.10

In a commutative ring with 1, the principal ideal generated by a is

$$< a >= \{ra : r \in R\} = Ra = aR,$$

the set of all multiples of a, sometimes denoted by Ra.

Definition 2.11 (sum of two ideals)

The sum of two ideals I and J , defined as $\{x + y : x \in I, y \in J\}$.

- It follows from the distributive law that $I + J$ is also an ideal.
- Similarly, the sum of two left[rignt] ideas is a left[right] ideal.
- nI也是理想，$n = 2, 3, \cdots$。

Given two ideals I and J, $I \cap J$ is also an ideal.

理想的性质

Fact 2.10

In a commutative ring with 1, the principal ideal generated by a is

$$< a >= \{ra : r \in R\} = Ra = aR,$$

the set of all multiples of a, sometimes denoted by Ra.

Definition 2.11 (sum of two ideals)

The sum of two ideals I and J , defined as $\{x + y : x \in I, y \in J\}$.

- It follows from the distributive law that $I + J$ is also an ideal.
- Similarly, the sum of two left[rignt] ideas is a left[right] ideal.
- nI也是理想，$n = 2, 3, \cdots$。

Given two ideals I and J, $I \cap J$ is also an ideal.

理想的性质

Fact 2.10

In a commutative ring with 1, the principal ideal generated by a is

$$< a >= \{ra : r \in R\} = Ra = aR,$$

the set of all multiples of a, sometimes denoted by Ra.

Definition 2.11 (sum of two ideals)

The sum of two ideals I and J , defined as $\{x + y : x \in I, y \in J\}$.

- It follows from the distributive law that $I + J$ is also an ideal.
- Similarly, the sum of two left[rignt] ideas is a left[right] ideal.
- nI也是理想，$n = 2, 3, \cdots$。

Given two ideals I and J, $I \cap J$ is also an ideal.

理想的性质

Fact 2.10

In a commutative ring with 1, the principal ideal generated by a is

$$< a >= \{ra : r \in R\} = Ra = aR,$$

the set of all multiples of a, sometimes denoted by Ra.

Definition 2.11 (sum of two ideals)

The sum of two ideals I and J , defined as $\{x + y : x \in I, y \in J\}$.

- It follows from the distributive law that $I + J$ is also an ideal.
- Similarly, the sum of two left[rignt] ideas is a left[right] ideal.
- nI也是理想，$n = 2, 3, \cdots$。

Given two ideals I and J, $I \cap J$ is also an ideal.

理想的性质

Fact 2.10

In a commutative ring with 1, the principal ideal generated by a is

$$< a >= \{ra : r \in R\} = Ra = aR,$$

the set of all multiples of a, sometimes denoted by Ra.

Definition 2.11 (sum of two ideals)

The sum of two ideals I and J , defined as $\{x + y : x \in I, y \in J\}$.

- It follows from the distributive law that $I + J$ is also an ideal.
- Similarly, the sum of two left[rignt] ideas is a left[right] ideal.
- nI也是理想，$n = 2, 3, \cdots$。

Given two ideals I and J, $I \cap J$ is also an ideal.

理想的性质

Fact 2.10

In a commutative ring with 1, the principal ideal generated by a is

$$< a >= \{ra : r \in R\} = Ra = aR,$$

the set of all multiples of a, sometimes denoted by Ra.

Definition 2.11 (sum of two ideals)

The sum of two ideals I and J , defined as $\{x + y : x \in I, y \in J\}$.

- It follows from the distributive law that $I + J$ is also an ideal.
- Similarly, the sum of two left[rignt] ideas is a left[right] ideal.
- nI也是理想，$n = 2, 3, \cdots$。

Given two ideals I and J, $I \cap J$ is also an ideal.

The Isomorphism Theorems For Rings

Suppose I is an ideal of the ring R, f is a ring homomorphism from R to S with kernel K, and π is the natural map, as indicated in following figure.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd}$$

We want to find a homomorphism $\overline{f} : R/I \to S$.

Theorem 3.1 (Factor Theorem For Rings)

Any ring homomorphism whose kernel contains I can be factored through R/I. In other words, there is a unique ring homomorphism $\overline{f} : R \mapsto S$ that makes the diagram commutative. Furthermore,

1. *$\overline{f}$ is an epimorphism iff f is an epimorphism;*
2. *$\overline{f}$ is a monomorphism iff $Kerf = I$;*
3. *$\overline{f}$ is an isomorphism iff f is an epimorphism and $Kerf = I$.*

Proof.

The only possible way to define $\overline{f}$ is $\overline{f}(a+I) = f(a)$. To verify that $\overline{f}$ is well-defined, note that if $a+I = b+I$, then $a-b \in I \subset K$, so $f(a-b) = 0$, i.e., $f(a) = f(b)$.

Since f is a ring homomorphism, so is $\overline{f}$.

From the prove of ring homomorphism, we can prove (1), (2) and (3). □

Theorem 3.1 (Factor Theorem For Rings)

Any ring homomorphism whose kernel contains I can be factored through R/I. In other words, there is a unique ring homomorphism $\overline{f} : R \mapsto S$ that makes the diagram commutative. Furthermore,

1. *$\overline{f}$ is an epimorphism iff f is an epimorphism;*
2. *$\overline{f}$ is a monomorphism iff $Kerf = I$;*
3. *$\overline{f}$ is an isomorphism iff f is an epimorphism and $Kerf = I$.*

Proof.

The only possible way to define $\overline{f}$ is $\overline{f}(a+I) = f(a)$. To verify that $\overline{f}$ is well-defined, note that if $a+I = b+I$, then $a-b \in I \subset K$, so $f(a-b) = 0$, i.e., $f(a) = f(b)$.
Since f is a ring homomorphism, so is $\overline{f}$.
From the prove of ring homomorphism, we can prove (1), (2) and (3). □

Theorem 3.1 (Factor Theorem For Rings)

Any ring homomorphism whose kernel contains I can be factored through R/I. In other words, there is a unique ring homomorphism $\overline{f}: R \mapsto S$ that makes the diagram commutative. Furthermore,

1. *$\overline{f}$ is an epimorphism iff f is an epimorphism;*
2. *$\overline{f}$ is a monomorphism iff $Kerf = I$;*
3. *$\overline{f}$ is an isomorphism iff f is an epimorphism and $Kerf = I$.*

Proof.

The only possible way to define $\overline{f}$ is $\overline{f}(a+I) = f(a)$. To verify that $\overline{f}$ is well-defined, note that if $a+I = b+I$, then $a-b \in I \subset K$, so $f(a-b) = 0$, i.e., $f(a) = f(b)$.

Since f is a ring homomorphism, so is $\overline{f}$.

From the prove of ring homomorphism, we can prove (1), (2) and (3). □

Theorem 3.1 (Factor Theorem For Rings)

Any ring homomorphism whose kernel contains I can be factored through R/I. In other words, there is a unique ring homomorphism $\overline{f} : R \mapsto S$ that makes the diagram commutative. Furthermore,

1. *$\overline{f}$ is an epimorphism iff f is an epimorphism;*
2. *$\overline{f}$ is a monomorphism iff $Kerf = I$;*
3. *$\overline{f}$ is an isomorphism iff f is an epimorphism and $Kerf = I$.*

Proof.

The only possible way to define $\overline{f}$ is $\overline{f}(a+I) = f(a)$. To verify that $\overline{f}$ is well-defined, note that if $a+I = b+I$, then $a-b \in I \subset K$, so $f(a-b) = 0$, i.e., $f(a) = f(b)$.

Since f is a ring homomorphism, so is $\overline{f}$.

From the prove of ring homomorphism, we can prove (1), (2) and (3). □

Theorem 3.1 (Factor Theorem For Rings)

Any ring homomorphism whose kernel contains I can be factored through R/I. In other words, there is a unique ring homomorphism $\overline{f} : R \mapsto S$ that makes the diagram commutative. Furthermore,

1. *$\overline{f}$ is an epimorphism iff f is an epimorphism;*
2. *$\overline{f}$ is a monomorphism iff $Kerf = I$;*
3. *$\overline{f}$ is an isomorphism iff f is an epimorphism and $Kerf = I$.*

Proof.

The only possible way to define $\overline{f}$ is $\overline{f}(a + I) = f(a)$. To verify that $\overline{f}$ is well-defined, note that if $a + I = b + I$, then $a - b \in I \subset K$, so $f(a - b) = 0$, i.e., $f(a) = f(b)$.
Since f is a ring homomorphism, so is $\overline{f}$.
From the prove of ring homomorphism, we can prove (1), (2) and (3). □

Theorem 3.2 (First Isomorphism Theorem For Rings)

If $f : R \mapsto S$ is a ring homomorphism with kernel K, then the image of f is isomorphic to R/K.

Proof.

Apply the factor theorem with $I = K$, and note that f is an epimorphism onto its image. □

Theorem 3.2 (First Isomorphism Theorem For Rings)

If $f : R \mapsto S$ is a ring homomorphism with kernel K, then the image of f is isomorphic to R/K.

Proof.

Apply the factor theorem with $I = K$, and note that f is an epimorphism onto its image. $\square$

Theorem 3.3 (Second Isomorphism Theorem For Rings)

Let I be an ideal of the ring R, and let S be a subring of R. Then

1. $S + I$ *is a subring of* R;
2. I *is an ideal of* $S + I$;
3. $S \cap I$ *is an ideal of* S;
4. $(S + I)/I$ *is isomorphic to* $S/(S \cap I)$.

Proof.

1. Verify $S + I$ is an additive subgroup of R that contains 1_R and is closed under multiplication.
2. Since I is an ideal of R, it must be an ideal of subring $S + I$.

□

Theorem 3.3 (Second Isomorphism Theorem For Rings)

Let I be an ideal of the ring R, and let S be a subring of R. Then

1. *$S + I$ is a subring of R;*
2. *I is an ideal of $S + I$;*
3. *$S \cap I$ is an ideal of S;*
4. *$(S + I)/I$ is isomorphic to $S/(S \cap I)$.*

Proof.

1. Verify $S + I$ is an additive subgroup of R that contains 1_R and is closed under multiplication.
2. Since I is an ideal of R, it must be an ideal of subring $S + I$.

□

Theorem 3.3 (Second Isomorphism Theorem For Rings)

Let I be an ideal of the ring R, and let S be a subring of R. Then

1. $S + I$ *is a subring of* R;
2. I *is an ideal of* $S + I$;
3. $S \cap I$ *is an ideal of* S;
4. $(S + I)/I$ *is isomorphic to* $S/(S \cap I)$.

Proof.

1. Verify $S + I$ is an additive subgroup of R that contains 1_R and is closed under multiplication.
2. Since I is an ideal of R, it must be an ideal of subring $S + I$.

□

Theorem 3.3 (Second Isomorphism Theorem For Rings)

Let I be an ideal of the ring R, and let S be a subring of R. Then

1. $S + I$ *is a subring of* R;
2. I *is an ideal of* $S + I$;
3. $S \cap I$ *is an ideal of* S;
4. $(S + I)/I$ *is isomorphic to* $S/(S \cap I)$.

Proof.

1. Verify $S + I$ is an additive subgroup of R that contains 1_R and is closed under multiplication.
2. Since I is an ideal of R, it must be an ideal of subring $S + I$.

□

Theorem 3.3 (Second Isomorphism Theorem For Rings)

Let I be an ideal of the ring R, and let S be a subring of R. Then

1. $S + I$ *is a subring of* R;
2. I *is an ideal of* $S + I$;
3. $S \cap I$ *is an ideal of* S;
4. $(S + I)/I$ *is isomorphic to* $S/(S \cap I)$.

Proof.

1. Verify $S + I$ is an additive subgroup of R that contains 1_R and is closed under multiplication.
2. Since I is an ideal of R, it must be an ideal of subring $S + I$.

□

Theorem 3.3 (Second Isomorphism Theorem For Rings)

Let I be an ideal of the ring R, and let S be a subring of R. Then

1. $S + I$ *is a subring of* R;
2. I *is an ideal of* $S + I$;
3. $S \cap I$ *is an ideal of* S;
4. $(S + I)/I$ *is isomorphic to* $S/(S \cap I)$.

Proof.

1. Verify $S + I$ is an additive subgroup of R that contains 1_R and is closed under multiplication.
2. Since I is an ideal of R, it must be an ideal of subring $S + I$.

Theorem 3.3 (Second Isomorphism Theorem For Rings)

Let I be an ideal of the ring R, and let S be a subring of R. Then

1. $S + I$ *is a subring of* R;
2. I *is an ideal of* $S + I$;
3. $S \cap I$ *is an ideal of* S;
4. $(S + I)/I$ *is isomorphic to* $S/(S \cap I)$.

Proof.

1. Verify $S + I$ is an additive subgroup of R that contains 1_R and is closed under multiplication.
2. Since I is an ideal of R, it must be an ideal of subring $S + I$.

□

Proof.

1. It follows from the definitions of subring and ideal.
2. Let $\pi : R \mapsto R/I$ be the natural map, and let π_0 be the restriction of π to S. Then π_0 is a ring homomorphism whose kernel is $S \cap I$ and whose image is
$$\{a + I : a \in S\} = (S + I)/I.$$
By the first isomorphism theorem, $S/\mathrm{Ker}\pi_0$ is isomorphic to the image of π_0.

□

Proof.

1. It follows from the definitions of subring and ideal.
2. Let $\pi : R \mapsto R/I$ be the natural map, and let π_0 be the restriction of π to S. Then π_0 is a ring homomorphism whose kernel is $S \cap I$ and whose image is

$$\{a + I : a \in S\} = (S + I)/I.$$

By the first isomorphism theorem, $S/\mathrm{Ker}\pi_0$ is isomorphic to the image of π_0.

$\square$

Theorem 3.4 (Third Isomorphism Theorem For Rings)

Let I and J be ideals of the ring R, with $I \subset J$. Then J/I is an ideal of R/I, and $R/J \cong (R/I)/(J/I)$.

Proof.

Define $f : R/I \mapsto R/J$ by $f(a+I) = a+J$. By definition of addition and multiplication of cosets in a quotient ring, f is a ring homomorphism. Now

$$\begin{aligned} \mathrm{Ker} f &= \{a+I : a+J = J\} \\ &= \{a+I : a \in J\} = J/I \end{aligned}$$

and

$$im f = \{a+J : a \in R\} = R/J.$$

The result follows from the first isomorphism theorem for rings. □

Theorem 3.4 (Third Isomorphism Theorem For Rings)

Let I and J be ideals of the ring R, with $I \subset J$. Then J/I is an ideal of R/I, and $R/J \cong (R/I)/(J/I)$.

Proof.

Define $f : R/I \mapsto R/J$ by $f(a+I) = a+J$. By definition of addition and multiplication of cosets in a quotient ring, f is a ring homomorphism. Now

$$\begin{aligned}\mathrm{Ker} f &= \{a+I : a+J = J\} \\ &= \{a+I : a \in J\} = J/I\end{aligned}$$

and

$$imf = \{a+J : a \in R\} = R/J.$$

The result follows from the first isomorphism theorem for rings. □

环的一一对应定理

Theorem 3.5 (Correspondence Theorem For Rings)

If I is an ideal of the ring R, then the map $S \to S/I$ sets up a one-to-one correspondence between the set of all subrings of R containing I and the set of all subrings of R/I, as well as a one-to-one correspondence between the set of all ideals of R containing I and the set of all ideals of R/I. The inverse of the map is $Q \to \pi^{-1}(Q)$, where π is the canonical map: $R \to R/I$.

- If S is a subring of R, then S/I is a quotient ring, and $S/I \subseteq R/I$, so S/I is subring of R/I.
- If $\{k + I \mid k \in K\}$ is subring of R/I, then $\{k + I \mid k \in K\} = (K + I)/I$. Let $S = K + I$. We prove that $S = K + I$ is a subring of R. Obviously, S is a subgroup of R(by property of group homomorphism). It suffices to prove closure under multiplication. Let $s_1, s_2 \in S$, then $(s_1 + I)(s_2 + I) \in (K + I)/I$, i.e., there exists $k + i$ such that $s_1 s_2 - (k + i) \in I$. So

环的一一对应定理

Theorem 3.5 (Correspondence Theorem For Rings)

If I is an ideal of the ring R, then the map $S \to S/I$ sets up a one-to-one correspondence between the set of all subrings of R containing I and the set of all subrings of R/I, as well as a one-to-one correspondence between the set of all ideals of R containing I and the set of all ideals of R/I. The inverse of the map is $Q \to \pi^{-1}(Q)$, where π is the canonical map: $R \to R/I$.

- If S is a subring of R, then S/I is a quotient ring, and $S/I \subseteq R/I$, so S/I is subring of R/I.
- If $\{k + I \mid k \in K\}$ is subring of R/I, then $\{k + I \mid k \in K\} = (K + I)/I$. Let $S = K + I$. We prove that $S = K + I$ is a subring of R. Obviously, S is a subgroup of R(by property of group homomorphism). It suffices to prove closure under multiplication. Let $s_1, s_2 \in S$, then $(s_1 + I)(s_2 + I) \in (K + I)/I$, i.e., there exists $k + i$ such that $s_1 s_2 - (k + i) \in I$. So

环的一一对应定理

- If S is a subring of R, then S/I is a quotient ring, and $S/I \subseteq R/I$, so S/I is subring of R/I.
- If $\{k+I \mid k \in K\}$ is subring of R/I, then $\{k+I \mid k \in K\} = (K+I)/I$. Let $S = K+I$. We prove that $S = K+I$ is a subring of R. Obviously, S is a subgroup of R(by property of group homomorphism). It suffices to prove closure under multiplication. Let $s_1, s_2 \in S$, then $(s_1+I)(s_2+I) \in (K+I)/I$, i.e., there exists $k+i$ such that $s_1s_2 - (k+i) \in I$. So $s_1s_2 - k - i = i'$ for some $i' \in I$. Therefore, $s_1s_2 \in K+I$.
- If J is ideal of R, then J/I is a ideal of R/I by the third isomorphism theorem.
- If $\{k+I \mid k \in K\} = (K+I)/I$ is ideal of R/I, then for all $k \in K$ and $r \in R$, $(k+I)(r+I) \in (K+I)/I$. Hence $\exists k'$ such that $kr - k' \in I \subseteq K+I$. Then $\exists k'', i''$ such that $kr - k' = k'' + i''$. So $kr \in K+I$. Consequently $K+I$ is an ideal of R.

环的外直积

If $R_1, \cdots, R_n$ are rings, the direct product of the R_i, denoted by $R_1 \otimes \ldots \otimes R_n$, is defined as the ring of n-tuples

$$R_1 \times \ldots \times R_n = \{(a_1, \ldots, a_n), a_i \in R_i\}$$

with componentwise addition and multiplication, that is,

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

and

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Chinese Remainder Theorem

Let R be a ring. $a, b \in R$ and I is an ideal of R, we say that

$$a \equiv b \mod I \ if \ a - b \in I.$$

The ideals I and J in the ring R are relatively prime if $I + J = R$.

Chinese Remainder Theorem

Let R be an arbitrary ring,and let $I_1, \ldots, I_n$ be ideals in R that are relatively prime in pairs, that is, $I_i + I_j = R$ for all $i \neq j$.

1. If $a_1 = 1$ and $a_j = 0$ for $j = 2, \ldots, n$, then there is an element $a \in R$ such that $a \equiv a_i \mod I_i$ for all $i = 1, \ldots, n$. More generally,
2. If $a_1, \ldots, a_n$ are arbitrary elements of R, there is an element $a \in R$ such that $a \equiv a_i \mod I_i$ for all $i = 1, \ldots, n$.
3. If b is another element of R such that $b \equiv a_i \mod I_i$ for all $i = 1, \ldots, n$, then
$$b \equiv a \mod I_1 \cap I_2 \cap \ldots \cap I_n.$$
Conversely, if $b \equiv a \mod \bigcap_{i=1}^{n} I_i$, then
$$b \equiv a_i \mod I_i$$
for all i.
4. $$R/\bigcap^{n} I_i \cong R/I_1 \times R/I_2 \cdots \times R/I_n.$$

作业(环I)

1. page 119: 习题3-1：1, 4, 17, 18.
2. page 129: 习题3-2：2, 9.
3. 证明：对于$N \in \mathbb{Z}^+$，环$\mathbb{Z}_N$的所有的理想是$d\mathbb{Z}_N$，其中$d = 0$或者$d|N$。
4. page 138: 习题3-3：9，13，17.
5. page 147: 习题3-4：5,7(2)(3).