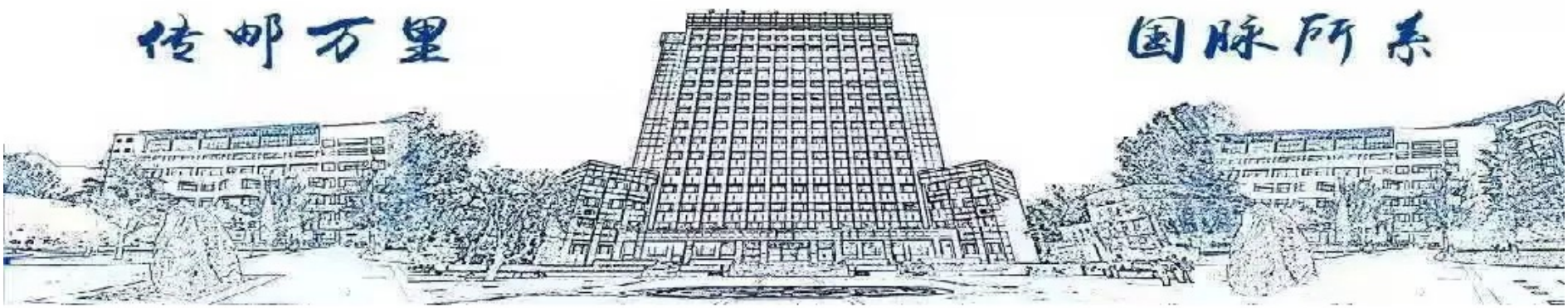
网络空间安全学院
School of Cyberspace Security, BUPT

信息安全数学基础

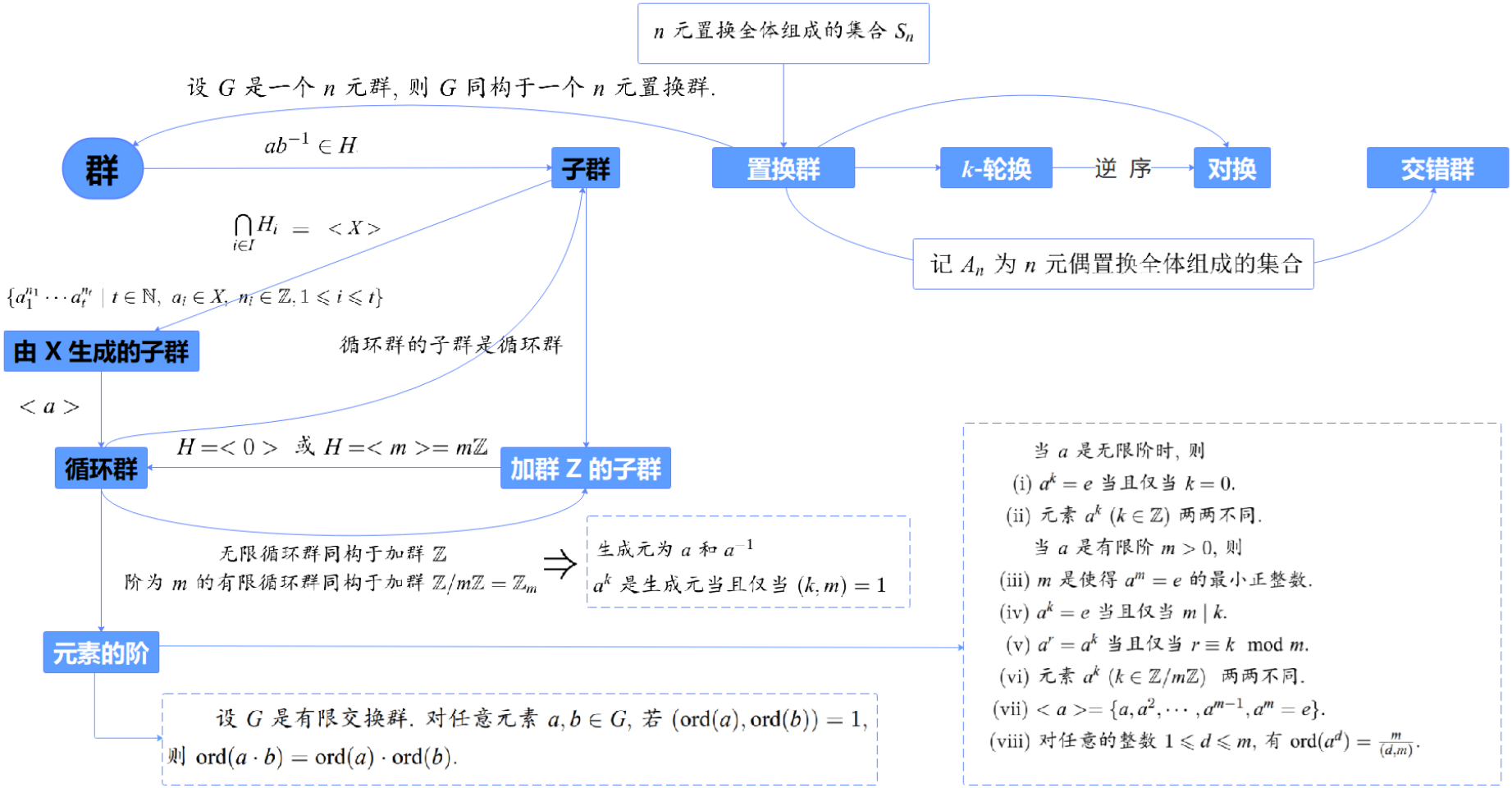
—— 环 (1)

信数课题组

北京邮电大学



上次课回顾


n 元置换全体组成的集合 S_n
设 G 是一个 n 元群, 则 G 同构于一个 n 元置换群.
群
$ab^{-1} \in H$
子群
置换群
k-轮换
逆 序
对换
交错群
$\bigcap_{i\in I} H_i = < X >$
记 A_n 为 n 元偶置换全体组成的集合
$\{a_1^{n_1} \cdots a_t^{n_t} \mid t \in \mathbb{N},\ a_i \in X,\ n_i \in \mathbb{Z}, 1 \leqslant i \leqslant t\}$
由 X 生成的子群
循环群的子群是循环群
$< a >$
$H =< 0 >$ 或 $H =< m >= m\mathbb{Z}$
循环群
加群 Z 的子群
无限循环群同构于加群 $\mathbb{Z}$
阶为 m 的有限循环群同构于加群 $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$
$\Rightarrow$
生成元为 a 和 a^{-1}
a^k 是生成元当且仅当 $(k, m) = 1$
元素的阶
当 a 是无限阶时, 则
(i) $a^k = e$ 当且仅当 $k = 0$.
(ii) 元素 a^k $(k \in \mathbb{Z})$ 两两不同.
当 a 是有限阶 $m > 0$, 则
(iii) m 是使得 $a^m = e$ 的最小正整数.
(iv) $a^k = e$ 当且仅当 $m \mid k$.
(v) $a^r = a^k$ 当且仅当 $r \equiv k \mod m$.
(vi) 元素 a^k $(k \in \mathbb{Z}/m\mathbb{Z})$ 两两不同.
(vii) $< a >= \{a, a^2, \cdots, a^{m-1}, a^m = e\}$.
(viii) 对任意的整数 $1 \leqslant d \leqslant m$, 有 $\mathrm{ord}(a^d) = \frac{m}{(d,m)}$.
设 G 是有限交换群. 对任意元素 $a, b \in G$, 若 $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$,
则 $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

目录

定义 7.1.1

设 R 是具有两种运算 (通常表示为加法和乘法) 的非空集合. 如果下面的条件成立:

(i) R 对于加法构成一个交换群.

(ii) (结合律) 对任意的 $a, b, c \in R$, 有 $(ab)c = a(bc)$.

(iii) (分配律) 对任意的 $a, b, c \in R$, 有

$$(a+b)c = ac + bc \quad \text{和} \quad a(b+c) = ab + ac.$$

则 R 叫作**环**.

例 7.1.1 整数环 $(\mathbb{Z}, +, \cdot)$

(i) $(\mathbb{Z}, +)$ 构成交换群. 即满足：

① 封闭性；

② 结合律；

③ 单位元 (零元) 0；

④ a 的逆为 $-a$, 负元；

⑤ 交换律 $a + b = b + a$.

(ii) $(\mathbb{Z}, \cdot)$ 构成半群. 即满足：

① 封闭性, $a \cdot b \in \mathbb{Z}, \forall\ a, b \in \mathbb{Z}$；

② 结合律 $(ab)c = a(bc)$.

(iii) 满足分配律：$\forall\ a, b, c \in \mathbb{Z}$,

$$\begin{cases} a(b + c) = ab + ac, \\ (b + c)a = ba + ca. \end{cases}$$

$\therefore$ $(\mathbb{Z}, +, \cdot)$ 是环.

定义 7.1.2

如果环 R 还满足：对任意的 $a, b \in R$, 有 $ab = ba$, 则 R 叫作**交换环**.

定义 7.1.2

如果环 R 还满足: 对任意的 $a, b \in R$, 有 $ab = ba$, 则 R 叫作**交换环**.

定义 7.1.3

如果环 R 中有一个元素 $e = 1_R$ 使得: 对任意的 $a \in R$, 有

$$a1_R = 1_R a = a,$$

则 R 叫作**有单位元环**.

定义 7.1.2

如果环 R 还满足: 对任意的 $a, b \in R$, 有 $ab = ba$, 则 R 叫作**交换环**.

定义 7.1.3

如果环 R 中有一个元素 $e = 1_R$ 使得: 对任意的 $a \in R$, 有

$$a1_R = 1_R a = a,$$

则 R 叫作**有单位元环**.

例 7.1.2 实数环 $(\mathbb{R}, +, \cdot)$ 有单位元, 则 $\mathbb{R}$ 叫做有单位元的环.

定理 7.1.1

设 R 是一个环, 则

(i) 对任意的 $a \in R$, 有 $0a = a0 = 0$.

(ii) 对任意的 $a, b \in R$, 有 $(-a)b = a(-b) = -ab$.

(iii) 对任意的 $a, b \in R$, 有 $(-a)(-b) = ab$.

(iv) 对任意的 $n \in \mathbb{Z}$, 任意的 $a, b \in R$, 有 $(na)b = a(nb) = nab$.

(v) 对任意的 $a_i, b_j \in R$, 有

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j.$$

定理 7.1.1

设 R 是一个环, 则

(i) 对任意的 $a \in R$, 有 $0a = a0 = 0$.

(ii) 对任意的 $a, b \in R$, 有 $(-a)b = a(-b) = -ab$.

(iii) 对任意的 $a, b \in R$, 有 $(-a)(-b) = ab$.

(iv) 对任意的 $n \in \mathbb{Z}$, 任意的 $a, b \in R$, 有 $(na)b = a(nb) = nab$.

(v) 对任意的 $a_i, b_j \in R$, 有

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j.$$

证: (i) 因为 $0a = (0+0)a = 0a + 0a$, 所以 $0a = 0$. 同理, $a0 = 0$.

(ii) 因为

$$(-a)b + ab = ((-a) + a)b = 0b = 0, a(-b) + ab = a((-b) + b) = a0 = 0,$$

所以 $(-a)b = a(-b) = -ab$.

(iii), (iv) 和 (v) 可由 (i) 和 (ii) 得到.

定理 7.1.2

设 R 是有单位元的环. 设 n 是正整数, $a, b, a_1, \cdots, a_r \in R$.

(i) 如果 $ab = ba$, 则 $(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}$.

(ii) 如果 $a_i a_j = a_j a_i, 1 \leqslant i, j \leqslant r$, 则

$$(a_1 + \cdots + a_r)^n = \sum_{i_1 + \cdots + i_r = n} \frac{n!}{i_1! \cdots i_r!} a_1^{i_1} \cdots a_r^{i_r}.$$

定理 7.1.2

设 R 是有单位元的环. 设 n 是正整数, $a, b, a_1, \cdots, a_r \in R$.

(i) 如果 $ab = ba$, 则 $(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}$.

(ii) 如果 $a_i a_j = a_j a_i, 1 \leqslant i, j \leqslant r$, 则

$$(a_1 + \cdots + a_r)^n = \sum_{i_1 + \cdots + i_r = n} \frac{n!}{i_1! \cdots i_r!} a_1^{i_1} \cdots a_r^{i_r}.$$

证: (i) 对 n 用数学归纳法. 当 $n = 1$ 时, 结论显然. 假设对 $n = s$ 时成立, 即有 $(a+b)^s = \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k}$. 则对 $n = s+1$ 时有 $(a+b)^{s+1}$

$$= (a+b)^s (a+b) = \left(\sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k} \right) (a+b)$$

$$\overset{ab=ba}{=} \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^{k+1} b^{s-k} + \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k+1}$$

$$= a^{s+1} + b^{s+1} + \sum_{k=0}^{s-1} \left(\frac{s!}{k!(s-k)!} a^{k+1} b^{s-k} + \frac{s!}{(k+1)!(s-k-1)!} a^{k+1} b^{s-k} \right)$$

$$= a^{s+1} + b^{s+1} + \sum_{k=0}^{s-1} \frac{(s+1)!}{(k+1)!(s-k)!} a^{k+1} b^{s-k}$$

$$= \sum_{k=0}^{s+1} \frac{(s+1)!}{k!(s+1-k)!} a^k b^{s+1-k}, \quad \text{即对 } n = s+1 \text{ 结论成立.}$$

$$= a^{s+1} + b^{s+1} + \sum_{k=0}^{s-1} \frac{(s+1)!}{(k+1)!(s-k)!} a^{k+1} b^{s-k}$$

$$= \sum_{k=0}^{s+1} \frac{(s+1)!}{k!(s+1-k)!} a^k b^{s+1-k}, \quad \text{即对 } n = s+1 \text{ 结论成立.}$$

(ii) 对 r 用数学归纳法. 当 $r = 2$ 时即为 (i) 的结论, 已经证明.

假设 $r \leqslant m$ 时结论成立. 当 $r = m+1$ 时, 由 (i) 及归纳假设得

$$(a_1 + \cdots + a_m + a_{m+1})^n = ((a_1 + \cdots + a_m) + a_{m+1})^n$$

$$= \sum_{i_{m+1}=0}^{n} \frac{n!}{i_{m+1}!(n-i_{m+1})!} (a_1 + \cdots + a_m)^{n-i_{m+1}} a_{m+1}^{i_{m+1}}$$

$$= \sum_{i_{m+1}=0}^{n} \frac{n!}{i_{m+1}!(n-i_{m+1})!} \sum_{i_1+\cdots+_m=n-i_{m+1}} \frac{(n-i_{m+1})!}{i_1! \cdots i_m!} a_1^{r_1} \cdots a_m^{i_m} a_{m+1}^{i_{m+1}}$$

$$= \sum_{i_1+\cdots+_m+i_{m+1}=n} \frac{n!}{i_1! \cdots i_m! i_{m+1}!} a_1^{r_1} \cdots a_m^{i_m} a_{m+1}^{i_{m+1}}, \quad \text{即对 } r = m+1 \text{ 结论成立.}$$

定义 7.1.4

设 a 是环 R 中的一个非零元, 如果存在非零元 $b \in R$ (对应地, 有 $c \in R$) 使得 $ab = 0$ (对应地, 有 $ca = 0$), 则称 a 为**左零因子** (对应地, 为**右零因子**). 如果同时为左零因子和右零因子, 则称 a 为**零因子**.

定义 7.1.4

设 a 是环 R 中的一个非零元, 如果存在非零元 $b \in R$ (对应地, 有 $c \in R$) 使得 $ab = 0$ (对应地, 有 $ca = 0$), 则称 a 为**左零因子** (对应地, 为**右零因子**). 如果同时为左零因子和右零因子, 则称 a 为**零因子**.

例 7.1.3 针对 $(\mathbb{Z}_6, +, \cdot)$, 其中 $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$ $= \{0, 1, 2, 3, 4, 5\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, "$+$" 是 $\oplus_6$, "$\cdot$" 是 $\otimes_6$.

$\because$ $[2][3] = [0] = [3][2]$.

$\therefore$ $[2]$ 是零因子, $[3]$ 是零因子.

综述: $\mathbb{Z}_6$ 是一个交换环, $[a][b] = [b][a]$; 有单位元 $[1]$; 有零因子环.

$\therefore$ $(\mathbb{Z}_6, +, \cdot)$ 是一个有零因子, 单位元的交换环.

定义 7.1.4

设 a 是环 R 中的一个非零元, 如果存在非零元 $b \in R$ (对应地, 有 $c \in R$) 使得 $ab = 0$ (对应地, 有 $ca = 0$), 则称 a 为**左零因子** (对应地, 为**右零因子**). 如果同时为左零因子和右零因子, 则称 a 为**零因子**.

例 7.1.3 针对 $(\mathbb{Z}_6, +, \cdot)$, 其中 $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$
$= \{0, 1, 2, 3, 4, 5\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, “$+$” 是 $\oplus_6$, “$\cdot$” 是 $\otimes_6$.

$\because$ $[2][3] = [0] = [3][2]$.

$\therefore$ $[2]$ 是零因子, $[3]$ 是零因子.

综述: $\mathbb{Z}_6$ 是一个交换环, $[a][b] = [b][a]$; 有单位元 $[1]$; 有零因子环.

$\therefore$ $(\mathbb{Z}_6, +, \cdot)$ 是一个有零因子, 单位元的交换环.

例 7.1.4 针对 $(\mathbb{Z}_5, +, \cdot)$, 其中 $\mathbb{Z}_5 = \mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$
$= \{0, 1, 2, 3, 4\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, “$+$” 是 $\oplus_5$, “$\cdot$” 是 $\otimes_5$.

$\mathbb{Z}_5$ 是一个交换环, $[a][b] = [b][a]$; 有单位元 $[1]$; 无零因子环.

定义 7.1.5

设 a 是有单位元 1_R 的环 R 中的一个元, 如果存在 $b \in R$ 使得 $ab = 1_R$, 则称 a 为**左逆元**. 这时, b 叫做 a 的**右逆元**. 如果同时为左逆元和右逆元, 则称 a 为**逆元**.

定义 7.1.5

设 a 是有单位元 1_R 的环 R 中的一个元, 如果存在 $b \in R$ 使得 $ab = 1_R$, 则称 a 为**左逆元**. 这时, b 叫做 a 的**右逆元**. 如果同时为左逆元和右逆元, 则称 a 为**逆元**.

例 7.1.5 有理数 $\mathbb{Q}$, $(\mathbb{Q}, +, \cdot)$ 满足

1) $(\mathbb{Q}, +)$ 交换加群.

2) $(\mathbb{Q}, \cdot)$ 半群.

3) 满足分配律.

$\therefore$ $(\mathbb{Q}, +, \cdot)$ 是环, 有单位元 1, 无零因子, $\forall\, a \in \mathbb{Q} \setminus \{0\}$, 逆元存在 $a^{-1} = \frac{1}{a}$.

希望一些环具有整数环 $\mathbb{Z}$ 的类似性质.

定义 7.1.6

设 R 是一个交换环, 如果 R 中有单位元, 但没有零因子, 则称 R 为整环.

希望一些环具有整数环 $\mathbb{Z}$ 的类似性质.

定义 7.1.6

设 R 是一个交换环, 如果 R 中有单位元, 但没有零因子, 则称 R 为**整环**.

例 7.1.6 整数 $\mathbb{Z}$, $(\mathbb{Z}, +, \cdot)$; 有理数 $\mathbb{Q}$, $(\mathbb{Q}, +, \cdot)$ 均为整环.

希望一些环具有整数环 $\mathbb{Z}$ 的类似性质.

定义 7.1.6

设 R 是一个交换环, 如果 R 中有单位元, 但没有零因子, 则称 R 为**整环**.

例 7.1.6 整数 $\mathbb{Z}$, $(\mathbb{Z}, +, \cdot)$; 有理数 $\mathbb{Q}$, $(\mathbb{Q}, +, \cdot)$ 均为整环.

我们也希望整数环的整除性也可以应用到环上.

定义 7.1.7

设 R 是一个交换环, $a, b \in R, b \neq 0$. 如果一个元素 $c \in R$ 使得 $a = bc$, 就称 b **整除** a 或者 a 被 b 整除, 记作 $b \mid a$.

(i) 当 b 整除 a 时, 把 b 叫做 a 的**因子**, 把 a 叫作 b 的**倍元**. 称环 R 中对于乘法有逆元的元素为**单位**. 如果 b, c 都不是单位, 就称 b 为 a 的**真因子**.

(ii) 对于环 R 中的非零元 a, 如果 a 不是单位, 且没有真因子, 则称 a 为**不可约元**或**既约元**. 也就是说, 如果有元素 $b, c \in R$ 使得 $a = bc$, 则 b 或 c 一定是单位.

(iii) 设 p 是环 R 中的非零元, 如果 p 不是单位, 且当 $p \mid ab$ 时, 有 $p \mid a$ 或 $p \mid b$, 则称 p 为**素元**.

(iv) 对于环 R 中的两个元素 $a, b \in R$, 如果存在单位 $u \in R$ 使得 $a = ub$, 则称 $a, b \in R$ 为**相伴的**, 称 a 为 b 的**相伴元**. 单位和 a 的相伴元也都是 a 的因子, 但不是真因子, 称这两类因子为 a 的**平凡因子**.

定义 7.1.8

设 R 为交换环, 如果 R 中有单位元, 且每个非零元都是可逆元, 即 R 对于加法构成一个交换群, $R^* = R \setminus \{0\}$ 对于乘法构成一个交换群, 且 R 中的加法和乘法运算满足分配律, 则称 R 为一个**域**.

定义 7.1.8

设 R 为交换环, 如果 R 中有单位元, 且每个非零元都是可逆元, 即 R 对于加法构成一个交换群, $R^* = R \setminus \{0\}$ 对于乘法构成一个交换群, 且 R 中的加法和乘法运算满足分配律, 则称 R 为一个**域**.

例 7.1.7 有理数 $\mathbb{Q}$, $(\mathbb{Q}, +, \cdot)$ 是域, 称为有理数域.

实数 $\mathbb{R}$, $(\mathbb{R}, +, \cdot)$ 是域, 称为实数域.

复数 $\mathbb{C}$, $(\mathbb{C}, +, \cdot)$ 是域, 称为复数域.

定义 7.1.8

设 R 为交换环, 如果 R 中有单位元, 且每个非零元都是可逆元, 即 R 对于加法构成一个交换群, $R^* = R \setminus \{0\}$ 对于乘法构成一个交换群, 且 R 中的加法和乘法运算满足分配律, 则称 R 为一个**域**.

例 7.1.7 有理数 $\mathbb{Q}$, $(\mathbb{Q}, +, \cdot)$ 是域, 称为有理数域.

实数 $\mathbb{R}$, $(\mathbb{R}, +, \cdot)$ 是域, 称为实数域.

复数 $\mathbb{C}$, $(\mathbb{C}, +, \cdot)$ 是域, 称为复数域.

例 7.1.8 设 p 是素数, $\mathbb{Z}_p = \{[0], [1], [2], \cdots, [p-1]\}$, 对 $(\mathbb{Z}_p, +, \cdot)$, 有

(i) $(\mathbb{Z}_p, +)$ 是交换加群.

(ii) $(\mathbb{Z}_p^*, \cdot)$ 是交换乘群.

(iii) $\forall\, a, b, c \in \mathbb{Z}_p, a \cdot (b + c) = a \cdot b + a \cdot c.$

$\therefore$ $(\mathbb{Z}_p, +, \cdot)$ 构成域.

例 7.1.9 $GF(2) = \{[0], [1]\}$ 称为二元域.

在 $(GP(2), +, \cdot)$ 中,

$+$ 即 “$\oplus_2$” , “模 2 加” , 可由数字信号的 “异或” 实现;

$\cdot$ 即”$\otimes_2$”, “模 2 乘” , 可由数字信号的 “与” 实现.

所以, 二元域 $GF(2)$ 是信息科学技术领域及信息安全领域应用最多的域之一.

本节讨论两个环之间的关系.

定义 7.2.1

设 R, R' 是两个环. 如果映射 $f: R \to R'$ 满足以下条件:

(i) 对任意的 $a, b \in R$, 有 $f(a+b) = f(a) + f(b)$;

(ii) 对任意的 $a, b \in R$, 有 $f(ab) = f(a)f(b)$,

则称 f 为**环同态**.

如果 f 是一对一的, 则称 f 为**单同态**; 如果 f 是满的, 则称 f 为**满同态**; 如果 f 是一一对应的, 则称 f 为**同构**.

本节讨论两个环之间的关系.

定义 7.2.1

设 R, R' 是两个环. 如果映射 $f: R \to R'$ 满足以下条件:

(i) 对任意的 $a, b \in R$, 有 $f(a+b) = f(a) + f(b)$;

(ii) 对任意的 $a, b \in R$, 有 $f(ab) = f(a)f(b)$,

则称 f 为**环同态**.

如果 f 是一对一的, 则称 f 为**单同态**; 如果 f 是满的, 则称 f 为**满同态**; 如果 f 是一一对应的, 则称 f 为**同构**.

定义 7.2.2

设 R, R' 是两个环, 如果存在一个 R 到 R' 的同构, 则称 R 与 R' 为**环同构**.

定义 7.2.3

设 R 是一个环. 若存在一个最小正整数 n 使得对任意 $a \in R$, 都有

$$na = \underbrace{a + \cdots + a}_{n \text{ 个 } a} = 0,$$

则称环 R 的**特征**为 n. 若不存在这样的正整数, 则称环 R 的特征为 0.

定义 7.2.3

设 R 是一个环. 若存在一个最小正整数 n 使得对任意 $a \in R$, 都有

$$na = \underbrace{a + \cdots + a}_{n \text{ 个 } a} = 0,$$

则称环 R 的**特征**为 n. 若不存在这样的正整数, 则称环 R 的特征为 0.

例 7.2.1 $n = 5, \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

$5[1] = [1] + [1] + [1] + [1] + [1] = [0]$,

且对于任意 $0 < m \leq 4, m[1] \neq [0]$.

另有 $5[0] = [0], 5[2] = 0, 5[3] = 0, 5[4] = 0$.

$\therefore$ $(\mathbb{Z}_5, +, \cdot)$ 的特征为 $n = 5$.

定义 7.2.3

设 R 是一个环. 若存在一个最小正整数 n 使得对任意 $a \in R$, 都有

$$na = \underbrace{a + \cdots + a}_{n \text{ 个 } a} = 0,$$

则称环 R 的**特征**为 n. 若不存在这样的正整数, 则称环 R 的特征为 0.

例 7.2.1 $n = 5, \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

$5[1] = [1] + [1] + [1] + [1] + [1] = [0]$,

且对于任意 $0 < m \leq 4, m[1] \neq [0]$.

另有 $5[0] = [0], 5[2] = 0, 5[3] = 0, 5[4] = 0$.

$\therefore$ $(\mathbb{Z}_5, +, \cdot)$ 的特征为 $n = 5$.

注: ① 无零因子环 R 的特征是有限整数 n, 那么 n 是一个素数.

② 在没有零因子的环 R 里, 所有不等于零的元, 对于加法来说, 阶都是一样的.

定理 7.2.1

设 R 是有单位元的交换环. 如果环 R 的特征是素数 p, 则对任意 $a, b \in R$, 有 $(a+b)^p = a^p + b^p$.

定理 7.2.1

设 R 是有单位元的交换环. 如果环 R 的特征是素数 p, 则对任意 $a, b \in R$, 有 $(a+b)^p = a^p + b^p$.

证：我们有 $(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k b^{p-k}$. 对于 $1 \leqslant k \leqslant p-1$, 有 $(p, k!(p-k)!) = 1$, 从而 $p \mid p \cdot \frac{(p-1)!}{k!(p-k)!}$. 这样, 由 R 的特征 p 为素数得到 $\frac{p!}{k!(p-k)!} a^k b^{p-k} = 0$. 因此, 结论成立.

定理 7.2.1

设 R 是有单位元的交换环. 如果环 R 的特征是素数 p, 则对任意 $a, b \in R$, 有 $(a+b)^p = a^p + b^p$.

证：我们有 $(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k b^{p-k}$. 对于 $1 \leqslant k \leqslant p-1$, 有 $(p, k!(p-k)!) = 1$, 从而 $p \mid p \cdot \frac{(p-1)!}{k!(p-k)!}$. 这样, 由 R 的特征 p 为素数得到 $\frac{p!}{k!(p-k)!} a^k b^{p-k} = 0$. 因此, 结论成立.

定理 7.2.2

如果域 K 的特征不为零, 则其特征必为素数.

定理 7.2.1

设 R 是有单位元的交换环. 如果环 R 的特征是素数 p, 则对任意 $a, b \in R$, 有 $(a+b)^p = a^p + b^p$.

证：我们有 $(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k b^{p-k}$. 对于 $1 \leqslant k \leqslant p-1$, 有 $(p, k!(p-k)!) = 1$, 从而 $p \mid p \cdot \frac{(p-1)!}{k!(p-k)!}$. 这样, 由 R 的特征 p 为素数得到 $\frac{p!}{k!(p-k)!} a^k b^{p-k} = 0$. 因此, 结论成立.

定理 7.2.2

如果域 K 的特征不为零, 则其特征必为素数.

证：设域 K 的特征为 n. 如果 n 不是素数, 则存在整数 $1 < n_1, n_2 < n$ 使得 $n = n_1 \cdot n_2$. $\therefore$ 对不等于零的元 a, $n_1 a \neq 0$, $n_2 a \neq 0$, 而 $(n_1 a)(n_2 a) = (n_1 n_2) a^2 = n a^2 = 0$. 但域中没有零因子, 与 $(n_1 a)(n_2 a) = 0$ 矛盾, 所以 n 是素数.

目录

定义 7.3.1

一个环 $(R,+,\cdot)$ 的非空子集 S $(S\subset R)$, 假如 S 对于环 R 的代数运算构成一个环, 则称 S 为 $(R,+,\cdot)$ 的**子环**. 相应地, 一个域 $(F,+,\cdot)$ 的非空子集 S $(S\subset F)$, 假如 S 对于域 F 的代数运算构成一个域, 则称 S 为 $(F,+,\cdot)$ 的**子域**.

定义 7.3.1

一个环 $(R,+,\cdot)$ 的非空子集 S $(S\subset R)$, 假如 S 对于环 R 的代数运算构成一个环, 则称 S 为 $(R,+,\cdot)$ 的**子环**. 相应地, 一个域 $(F,+,\cdot)$ 的非空子集 S $(S\subset F)$, 假如 S 对于域 F 的代数运算构成一个域, 则称 S 为 $(F,+,\cdot)$ 的**子域**.

例 7.3.1 整数环 $(\mathbb{Z},+,\cdot)$ 是 $(\mathbb{Q},+,\cdot)$ 的子环.

定义 7.3.1

一个环 $(R,+,\cdot)$ 的非空子集 S $(S\subset R)$, 假如 S 对于环 R 的代数运算构成一个环, 则称 S 为 $(R,+,\cdot)$ 的**子环**. 相应地, 一个域 $(F,+,\cdot)$ 的非空子集 S $(S\subset F)$, 假如 S 对于域 F 的代数运算构成一个域, 则称 S 为 $(F,+,\cdot)$ 的**子域**.

例 7.3.1 整数环 $(\mathbb{Z},+,\cdot)$ 是 $(\mathbb{Q},+,\cdot)$ 的子环.

例 7.3.2 证明: $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ 是 $(\mathbb{R},+,\cdot)$ 的子环.

定义 7.3.1

一个环 $(R,+,\cdot)$ 的非空子集 S $(S\subset R)$, 假如 S 对于环 R 的代数运算构成一个环, 则称 S 为 $(R,+,\cdot)$ 的**子环**. 相应地, 一个域 $(F,+,\cdot)$ 的非空子集 S $(S\subset F)$, 假如 S 对于域 F 的代数运算构成一个域, 则称 S 为 $(F,+,\cdot)$ 的**子域**.

例 7.3.1 整数环 $(\mathbb{Z},+,\cdot)$ 是 $(\mathbb{Q},+,\cdot)$ 的子环.

例 7.3.2 证明: $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ 是 $(\mathbb{R},+,\cdot)$ 的子环.

证: 显然 $\mathbb{Q}(\sqrt{2})$ 非空, 是实数集合 $\mathbb{Q}$ 的子集.

$$\forall\, x=a_1+b_1\sqrt{2}, y=a_2+b_2\sqrt{2}\in\mathbb{Q}(\sqrt{2}),$$

$$x-y=(a_1+b_1\sqrt{2})-(a_2+b_2\sqrt{2})=(a_1-a_2)+(b_1-b_2)\sqrt{2}\in\mathbb{Q}(\sqrt{2}),$$

$$\begin{aligned}x\cdot y&=(a_1+b_1\sqrt{2})\cdot(a_2+b_2\sqrt{2})\\&=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}\in\mathbb{Q}(\sqrt{2}),\end{aligned}$$

所以 $(\mathbb{Q}(\sqrt{2}),+,\cdot)$ 是 $(\mathbb{R},+,\cdot)$ 的子环.

目录

接下来讨论一种特别重要的子环, 就是理想. 理想在环论里的地位与正规子群在群论里的地位类似.

定义 7.3.2

设 R 是一个环, I 是 R 的子环.

如果任意的 $r \in R$ 和任意的 $a \in I$, 都有 $ra \in I$, 则称 I 为 R 的**左理想**.

如果任意的 $r \in R$ 和任意的 $a \in I$, 都有 $ar \in I$, 则称 I 为 R 的**右理想**.

如果 I 同时为左理想和右理想, 则称 I 为 R 的**理想**.

接下来讨论一种特别重要的子环, 就是理想. 理想在环论里的地位与正规子群在群论里的地位类似.

定义 7.3.2

设 R 是一个环, I 是 R 的子环.

如果任意的 $r \in R$ 和任意的 $a \in I$, 都有 $ra \in I$, 则称 I 为 R 的**左理想**.

如果任意的 $r \in R$ 和任意的 $a \in I$, 都有 $ar \in I$, 则称 I 为 R 的**右理想**.

如果 I 同时为左理想和右理想, 则称 I 为 R 的**理想**.

定理 7.3.1

环 R 的非空子集 I 是左 (对应地, 右) 理想的充要条件是:

(i) 对任意的 $a, b \in I$, 都有 $a - b \in I$.

(ii) 对任意的 $r \in R$ 和对任意的 $a \in I$, 都有 $ra \in I$ (对应地, 有 $ar \in I$).

注：(1) “理想 $\leftrightarrow$ 子环”的关系如下：

A. 理想一定是子环：由 (i) 可知理想 I 是一个加群, 由 (ii) 可知 I 对于乘法是封闭的.

B. 由 (ii), 不仅要求 I 的两个元的乘积必须在 I 里, 而且进一步要求 I 的一个任意元与 R 的一个任意元的乘积都必须在 I 里. 所以一个理想所适合的条件比一般子环要强些.

(2) 设 $(R, +, \cdot)$ 是一个环, I 是 R 的理想, 则 I 是 $(R, +)$ 的正规子群.

注：(1) “理想 $\leftrightarrow$ 子环”的关系如下：

A. 理想一定是子环：由 (i) 可知理想 I 是一个加群, 由 (ii) 可知 I 对于乘法是封闭的.

B. 由 (ii), 不仅要求 I 的两个元的乘积必须在 I 里, 而且进一步要求 I 的一个任意元与 R 的一个任意元的乘积都必须在 I 里. 所以一个理想所适合的条件比一般子环要强些.

(2) 设 $(R, +, \cdot)$ 是一个环, I 是 R 的理想, 则 I 是 $(R, +)$ 的正规子群.

注：一个环是不是一定有理想？

是！

至少有 2 个理想：

(i) 零理想：$I = \{0\}$, 只含有零元的集合.

(ii) 单位理想：$I = R$, R 本身.

例 7.3.3 $\{0\}$ 和 R 都是 R 的理想, 叫作 R 的**平凡理想**.

例 7.3.3 $\{0\}$ 和 R 都是 R 的理想, 叫作 R 的**平凡理想**.

例 7.3.4 两个理想的交集还是理想.

例 7.3.3 $\{0\}$ 和 R 都是 R 的理想, 叫作 R 的**平凡理想**.

例 7.3.4 两个理想的交集还是理想.

证：设 H_1 与 H_2 是环 R 的两个理想. 要证 $H_1 \cap H_2$ 是理想, 只需证明：

① $\forall\, a, b \in H_1 \cap H_2, a - b \in H_1 \cap H_2$.

② $\forall\, r \in R, a \in H_1 \cap H_2, ar \in H_1 \cap H_2, ra \in H_1 \cap H_2$.

例 7.3.3 $\{0\}$ 和 R 都是 R 的理想, 叫作 R 的**平凡理想**.

例 7.3.4 两个理想的交集还是理想.

证：设 H_1 与 H_2 是环 R 的两个理想. 要证 $H_1 \cap H_2$ 是理想, 只需证明：

① $\forall\, a, b \in H_1 \cap H_2, a - b \in H_1 \cap H_2$.

② $\forall\, r \in R, a \in H_1 \cap H_2, ar \in H_1 \cap H_2, ra \in H_1 \cap H_2$.

事实上,

① 对于 $\forall\, a, b \in H_1 \cap H_2$, 有 $a \in H_1, a \in H_2, b \in H_1, b \in H_2$.

$\because$ H_1 是理想, $\therefore$ $a - b \in H_1$.

又 $\because$ H_2 是理想, $\therefore$ $a - b \in H_2$.

$\therefore$ $a - b \in H_1 \cap H_2$.

例 7.3.3 $\{0\}$ 和 R 都是 R 的理想, 叫作 R 的**平凡理想**.

例 7.3.4 两个理想的交集还是理想.

证：设 H_1 与 H_2 是环 R 的两个理想. 要证 $H_1 \cap H_2$ 是理想, 只需证明：

① $\forall\, a, b \in H_1 \cap H_2, a - b \in H_1 \cap H_2$.

② $\forall\, r \in R, a \in H_1 \cap H_2, ar \in H_1 \cap H_2, ra \in H_1 \cap H_2$.

事实上,

① 对于 $\forall\, a, b \in H_1 \cap H_2$, 有 $a \in H_1, a \in H_2, b \in H_1, b \in H_2$.

$\because$ H_1 是理想, $\therefore$ $a - b \in H_1$.

又 $\because$ H_2 是理想, $\therefore$ $a - b \in H_2$.

$\therefore$ $a - b \in H_1 \cap H_2$.

② 设 $\forall\, r \in R$, $\forall\, a \in H_1 \cap H_2$, $\therefore$ $a \in H_1, a \in H_2$.

$\because$ H_1 是理想, $\therefore$ $ar \in H_1, ra \in H_1$.

又 $\because$ H_2 是理想, $\therefore$ $ar \in H_2, ra \in H_2$.

$\therefore$ $ar \in H_1 \cap H_2, ra \in H_1 \cap H_2$.

例 7.3.5 设 $\{A_j\}_{j\in J}$ 是环中的一族理想, 则 $\bigcap\limits_{j\in J} A_j$ 也是一个理想.

例 7.3.5 设 $\{A_j\}_{j\in J}$ 是环中的一族理想, 则 $\bigcap\limits_{j\in J} A_j$ 也是一个理想.

与此相关的, 还有以下结论:

① 两个子群的交, 是子群.

② 两个正规子群的交, 是正规子群.

③ 两个子环的交, 是子环.

④ 两个子整环的交, 是子整环.

⑤ 两个子域的交, 是子域.

⑥ 两个理想的交, 是理想.

定义 7.3.3

设 X 是环 R 的一个子集. 设 $\{A_j\}_{j\in J}$ 是环 R 中包含 X 的所有 (左) 理想, 则 $\bigcap\limits_{j\in J} A_j$ 称为由 X **生成的 (左) 理想**, 记作 (X). X 中的元素叫作理想 (X) 的**生成元**.

如果 $X=\{a_1,\cdots,a_n\}$, 则理想 (X) 记作 $(a_1,\cdots,a_n)$, 称为**有限生成的理想**. 由一个元素生成的理想 (a) 叫作**主理想**.

定理 7.3.2

环 $(R,+,\cdot),\forall\ a\in R$, 由 a 生成的主理想可表示为如下形式的元素：

$$(a)=\left\{\sum_{i=1}^{m}x_iay_i+sa+at+na\mid x_i,y_i,s,t\in R,n\in\mathbb{N}\right\}.$$

定理 7.3.2

环 $(R,+,\cdot)$, $\forall\ a\in R$, 由 a 生成的主理想可表示为如下形式的元素：

$$(a)=\left\{\sum_{i=1}^{m}x_iay_i+sa+at+na \mid x_i,y_i,s,t\in R,n\in\mathbb{N}\right\}.$$

注： (i) 两个这种形式的元相减, 显然还是一个这种形式的元.

(ii) 对 $r\in R$, 左乘 (a) 的一个元, 也得到一个这种形式的元, 即

$$[(rx_1)ay_1+(rx_2)ay_2+\cdots(rx_m)ay_m+rat]+(rs+nr)a.$$

(iii) 同理, $\forall\ r\in R$, 用 r 右乘上面的任意一元, 情形一样.

所以, 包含 a 的理想为 (a), 或者由 a 生成的理想为 (a).

一个主理想 (a) 的元的形式, 并不是永远像上面那样复杂.

① 当 R 是交换环时, (a) 的元显然都可以写成 $ra + na, (r \in R, n \in \mathbb{Z})$.

② 当 R 有单位元的时候, (a) 的元都可以写成 $\sum x_i a y_i, x_i, y_i \in R$.

因为此时 $sa = sa \cdot I_R, at = I_r \cdot at, na = (nI_R)aI_R$.

③ 当 R 既是交换环, 又有单位元时, (a) 的元形式特别简单, 可以写成 $ra \quad (r \in R)$.

一个主理想 (a) 的元的形式, 并不是永远像上面那样复杂.

① 当 R 是交换环时, (a) 的元显然都可以写成 $ra + na, (r \in R, n \in \mathbb{Z})$.

② 当 R 有单位元的时候, (a) 的元都可以写成 $\sum x_i a y_i, x_i, y_i \in R$.

因为此时 $sa = sa \cdot I_R, at = I_r \cdot at, na = (nI_R)aI_R$.

③ 当 R 既是交换环, 又有单位元时, (a) 的元形式特别简单, 可以写成 $ra \quad (r \in R)$.

定义 7.3.4

如果环 R 的所有理想都是主理想, 则称 R 为**主理想环**.

一个主理想 (a) 的元的形式, 并不是永远像上面那样复杂.

① 当 R 是交换环时, (a) 的元显然都可以写成 $ra+na, (r\in R, n\in\mathbb{Z})$.

② 当 R 有单位元的时候, (a) 的元都可以写成 $\sum x_iay_i, x_i, y_i\in R$.

因为此时 $sa=sa\cdot I_R, at=I_r\cdot at, na=(nI_R)aI_R$.

③ 当 R 既是交换环, 又有单位元时, (a) 的元形式特别简单, 可以写成 $ra\quad (r\in R)$.

定义 7.3.4

如果环 R 的所有理想都是主理想, 则称 R 为**主理想环**.

例 7.3.6 整数环 $(\mathbb{Z},+,\cdot)$ 有单位元, 可交换, 元素 $1\in\mathbb{Z}$, 则

(i) $(1)=\{r\cdot 1\mid r\in\mathbb{Z}\}=\mathbb{Z}$, 单位理想.

(ii) $(0)=\{r\cdot 0\mid r\in\mathbb{Z}\}=\{0\}$, 零理想.

(iii) $(2)=\{r\cdot 2\mid r\in\mathbb{Z}\}=\{$偶数$\}$, 偶数环.

现在, 设 $(R,+,\cdot)$ 是一个环, I 是 R 的一个理想, 则 I 是 $(R,+)$ 的一个正规子群.

现在, 设 $(R,+,\cdot)$ 是一个环, I 是 R 的一个理想, 则 I 是 $(R,+)$ 的一个正规子群.

我们考虑陪集集合 $\{a+I,b+I,c+I,\cdots\}=R/I$ 组成的商集, 定义以下运算:

$+$: $(a+I)+(b+I)=(a+b)+I$,

$\cdot$: $(a+I)\cdot(b+I)=(a\cdot b)+I$.

现在, 设 $(R,+,\cdot)$ 是一个环, I 是 R 的一个理想, 则 I 是 $(R,+)$ 的一个正规子群.

我们考虑陪集集合 $\{a+I,b+I,c+I,\cdots\}=R/I$ 组成的商集, 定义以下运算:

$+$: $(a+I)+(b+I)=(a+b)+I$,

$\cdot$: $(a+I)\cdot(b+I)=(a\cdot b)+I$.

可知, $(R/I,+,\cdot)$ 满足:

现在, 设 $(R,+,\cdot)$ 是一个环, I 是 R 的一个理想, 则 I 是 $(R,+)$ 的一个正规子群.

我们考虑陪集集合 $\{a+I,b+I,c+I,\cdots\}=R/I$ 组成的商集, 定义以下运算:

$+$: $(a+I)+(b+I)=(a+b)+I$,

$\cdot$: $(a+I)\cdot(b+I)=(a\cdot b)+I$.

可知, $(R/I,+,\cdot)$ 满足:

(i) $(R/I,+)$ 构成商群, 可交换;

现在, 设 $(R,+,\cdot)$ 是一个环, I 是 R 的一个理想, 则 I 是 $(R,+)$ 的一个正规子群.

我们考虑陪集集合 $\{a+I,b+I,c+I,\cdots\}=R/I$ 组成的商集, 定义以下运算:

$+$: $(a+I)+(b+I)=(a+b)+I$,

$\cdot$: $(a+I)\cdot(b+I)=(a\cdot b)+I$.

可知, $(R/I,+,\cdot)$ 满足:

(i) $(R/I,+)$ 构成商群, 可交换;

(ii) $(R/I,\cdot)$ 构成半群:

i) 封闭性. $\forall\ a+I,b+I\in R/I,(a+I)\cdot(b+I)=(a\cdot b)+I\in R/I$.

ii) 结合律. $\forall\ a+I,b+I,c+I\in R/I$, 有

$$[(a+I)\cdot(b+I)]\cdot(c+I)=[(ab)\cdot c]+I=[a\cdot(bc)]+I$$
$$=(a+I)\cdot[(b+I)\cdot(c+I)].$$

(iii) 分配律：$\forall\ a+I, b+I, c+I \in R/I$, 有

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

(iii) 分配律：$\forall\ a+I, b+I, c+I \in R/I$, 有

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

同理, $[(b+I)+(c+I)]\cdot(a+I) = (b+I)\cdot(a+I)+(c+I)\cdot(a+I)$.

(iii) 分配律：$\forall\ a+I, b+I, c+I \in R/I$, 有

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

同理, $[(b+I)+(c+I)]\cdot(a+I) = (b+I)\cdot(a+I)+(c+I)\cdot(a+I)$.

$\therefore$ $(R/I, +, \cdot)$ 构成环, 称其为 R 关于 I 的**商环**.

(iii) 分配律：$\forall\ a+I, b+I, c+I \in R/I$, 有

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

同理, $[(b+I)+(c+I)]\cdot(a+I) = (b+I)\cdot(a+I)+(c+I)\cdot(a+I)$.

$\therefore$ $(R/I, +, \cdot)$ 构成环, 称其为 R 关于 I 的**商环**.

定理 7.3.3

设 R 是一个环, I 是 R 的一个理想, 则 R/I 对于加法运算

$$(a+I)+(b+I) = (a+b)+I$$

和乘法运算

$$(a+I)(b+I) = (ab)+I$$

构成一个环. 当 R 是交换环或有单位元时, R/I 也是交换环或有单位元.

例 7.3.7 做出环 $\mathbb{Z}_6$ 关于主理想 $(3) = \{0, 3\}$ 的商环 $\mathbb{Z}_6/(3)$ 的运算表.

例 7.3.7 做出环 $\mathbb{Z}_6$ 关于主理想 $(3)=\{0,3\}$ 的商环 $\mathbb{Z}_6/(3)$ 的运算表.

解：$\because$ $(3)=\{0,3\},\mathbb{Z}_6=\{0,1,2,3,4,5\}$.

$\therefore$ $\mathbb{Z}_6$ 关于 (3) 的陪集有 3 个,

即 $(3)=0+(3)=\{0,3\},1+(3)=\{1,4\},2+(3)=\{2,5\}$.

故 $\mathbb{Z}_6/(3)=\{(3),1+(3),2+(3)\}$.

例 7.3.7 做出环 $\mathbb{Z}_6$ 关于主理想 $(3)=\{0,3\}$ 的商环 $\mathbb{Z}_6/(3)$ 的运算表.

解：$\because\ (3)=\{0,3\},\mathbb{Z}_6=\{0,1,2,3,4,5\}.$

$\therefore\ \mathbb{Z}_6$ 关于 (3) 的陪集有 3 个,

即 $(3)=0+(3)=\{0,3\},1+(3)=\{1,4\},2+(3)=\{2,5\}.$

故 $\mathbb{Z}_6/(3)=\{(3),1+(3),2+(3)\}.$

而由 $(a+H)+(b+H)=(a+b)+H,(a+H)\cdot(b+H)=ab+H$ 得

例 7.3.7 做出环 $\mathbb{Z}_6$ 关于主理想 $(3)=\{0,3\}$ 的商环 $\mathbb{Z}_6/(3)$ 的运算表.

解：$\because\ (3)=\{0,3\},\mathbb{Z}_6=\{0,1,2,3,4,5\}.$

$\therefore\ \mathbb{Z}_6$ 关于 (3) 的陪集有 3 个,

即 $(3)=0+(3)=\{0,3\},1+(3)=\{1,4\},2+(3)=\{2,5\}.$

故 $\mathbb{Z}_6/(3)=\{(3),1+(3),2+(3)\}.$

而由 $(a+H)+(b+H)=(a+b)+H,(a+H)\cdot(b+H)=ab+H$ 得

$+$	(3)	$1+(3)$	$2+(3)$
(3)	(3)	$1+(3)$	$2+(3)$
$1+(3)$	$1+(3)$	$2+(3)$	(3)
$2+(3)$	$2+(3)$	(3)	$1+(3)$

例 7.3.7 做出环 $\mathbb{Z}_6$ 关于主理想 $(3)=\{0,3\}$ 的商环 $\mathbb{Z}_6/(3)$ 的运算表.

解：$\because\ (3)=\{0,3\},\mathbb{Z}_6=\{0,1,2,3,4,5\}.$

$\therefore\ \mathbb{Z}_6$ 关于 (3) 的陪集有 3 个,

即 $(3)=0+(3)=\{0,3\},1+(3)=\{1,4\},2+(3)=\{2,5\}.$

故 $\mathbb{Z}_6/(3)=\{(3),1+(3),2+(3)\}.$

而由 $(a+H)+(b+H)=(a+b)+H,(a+H)\cdot(b+H)=ab+H$ 得

$+$	(3)	$1+(3)$	$2+(3)$
(3)	(3)	$1+(3)$	$2+(3)$
$1+(3)$	$1+(3)$	$2+(3)$	(3)
$2+(3)$	$2+(3)$	(3)	$1+(3)$

$\cdot$	(3)	$1+(3)$	$2+(3)$
(3)	(3)	(3)	(3)
$1+(3)$	(3)	$1+(3)$	$2+(3)$
$2+(3)$	(3)	$2+(3)$	$1+(3)$

现在, 给出环同态基本定理.

定理 7.3.4

设 f 是环 R 到环 R' 的同态, 则 f 的核 $\ker f$ 是 R 的理想. 反过来, 设 I 是环 R 的理想, 令

$$\begin{aligned} s: \ R &\to R/I, \\ a &\mapsto a+I, \end{aligned}$$

则 s 是满同态映射 (称为 $R \to R/I$ 的自然同态), 且 $\ker s = I$.

现在, 给出环同态基本定理.

定理 7.3.4

设 f 是环 R 到环 R' 的同态, 则 f 的核 $\ker f$ 是 R 的理想. 反过来, 设 I 是环 R 的理想, 令

$$\begin{aligned} s: \ R &\to R/I, \\ a &\mapsto a+I, \end{aligned}$$

则 s 是满同态映射 (称为 $R \to R/I$ 的自然同态), 且 $\ker s = I$.

证: i) 对 $\forall\, a, b \in \ker f, \ f(a) = f(b) = 0$.

$\therefore\ f(a-b) = f(a) - f(b) = 0 - 0 = 0.$

$\therefore\ a - b \in \ker f.$

ii) 对 $\forall\, r \in R, a \in \ker f, \ f(a) = 0$.

$\therefore\ f(ra) = f(r) \cdot f(a) = f(r) \cdot 0 = 0. \quad \therefore\ ra \in \ker f.$

同理, $ar \in \ker f$.

综上, $\ker f$ 是 R 的理想.

反过来, 对任意 $a, b \in R$, 有

$$s(a+b) = (a+b)+I = (a+I)(b+I) = s(a)+s(b),$$

$$s(ab) = ab+I = (a+I)(b+I) = s(a)s(b).$$

而对任意 $(a+I) \in R/I$, 有原像 a, 故 s 为 R 到 R/I 的满同态. 进而,

$$\ker s = \{a \mid a+I = I, a \in R\} = \{a \mid a \in I\} = I.$$

反过来, 对任意 $a, b \in R$, 有

$$s(a+b) = (a+b)+I = (a+I)(b+I) = s(a)+s(b),$$

$$s(ab) = ab+I = (a+I)(b+I) = s(a)s(b).$$

而对任意 $(a+I) \in R/I$, 有原像 a, 故 s 为 R 到 R/I 的满同态. 进而,

$$\ker s = \{a \mid a+I = I, a \in R\} = \{a \mid a \in I\} = I.$$

定理 7.3.5 (环同态基本定理)

设 f 是环 R 到环 R' 的同态, 则存在唯一的 $R/\ker f$ 到像子环 $f(R)$ 的同构 $\bar{f}$: $a+\ker f \mapsto f(a)$ 使得 $f = i \circ \bar{f} \circ s$, 其中 s 是环 R 到商环 $R/\ker f$ 的自然同态, $i : c \mapsto c$ 是 $f(R)$ 到 R' 的恒等映射, 即有以下的交换图.

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ s\downarrow & & \uparrow i \\ R/\ker f & \xrightarrow{\bar{f}} & f(R) \end{array}$$

定义 7.3.5

设 P 是环 R 的理想. 如果 $P \neq R$, 且对任意理想 $A, B, AB \subset P$, 有 $A \subset P$ 或 $B \subset P$, 则称 P 为 R 的**素理想**.

定义 7.3.5

设 P 是环 R 的理想. 如果 $P \neq R$, 且对任意理想 $A, B, AB \subset P$, 有 $A \subset P$ 或 $B \subset P$, 则称 P 为 R 的**素理想**.

定理 7.3.6

设 P 是环 R 的理想. 如果 $P \neq R$, 且对任意 $a, b \in R$, 当 $ab \in P$ 时, 有 $a \in P$ 或 $b \in P$, 则 P 是素理想.

反过来, 如果 P 是素理想, 且 R 是交换环, 则对于任意 $a, b \in R$, $ab \in P$, 有 $a \in P$ 或 $b \in P$.

定义 7.3.5

设 P 是环 R 的理想. 如果 $P \neq R$, 且对任意理想 $A, B, AB \subset P$, 有 $A \subset P$ 或 $B \subset P$, 则称 P 为 R 的**素理想**.

定理 7.3.6

设 P 是环 R 的理想. 如果 $P \neq R$, 且对任意 $a, b \in R$, 当 $ab \in P$ 时, 有 $a \in P$ 或 $b \in P$, 则 P 是素理想.

反过来, 如果 P 是素理想, 且 R 是交换环, 则对于任意 $a, b \in R$, $ab \in P$, 有 $a \in P$ 或 $b \in P$.

证：如果理想 A, B 使得 $AB \subset P, A \not\subset P$, 则存在元素 $a \in A, a \notin P$. 对任意元素 $b \in B$, 根据假设, 从 $ab \in AB \subset P$ 及 $a \notin P$ 可得到 $b \in P$. 这说明, $B \subset P$. 因此, P 是素理想.

定义 7.3.5

设 P 是环 R 的理想. 如果 $P \neq R$, 且对任意理想 $A, B, AB \subset P$, 有 $A \subset P$ 或 $B \subset P$, 则称 P 为 R 的**素理想**.

定理 7.3.6

设 P 是环 R 的理想. 如果 $P \neq R$, 且对任意 $a, b \in R$, 当 $ab \in P$ 时, 有 $a \in P$ 或 $b \in P$, 则 P 是素理想.

反过来, 如果 P 是素理想, 且 R 是交换环, 则对于任意 $a, b \in R$, $ab \in P$, 有 $a \in P$ 或 $b \in P$.

证：如果理想 A, B 使得 $AB \subset P, A \not\subset P$, 则存在元素 $a \in A, a \notin P$. 对任意元素 $b \in B$, 根据假设, 从 $ab \in AB \subset P$ 及 $a \notin P$ 可得到 $b \in P$. 这说明, $B \subset P$. 因此, P 是素理想.

反过来, 设 P 是素理想, 且 R 是交换环, 则对任意 $a, b \in R$, 满足 $ab \in P$, 有 $(a)(b) = (ab) \subset P$. 根据素理想的定义, 有 $(a) \subset P$ 或 $(b) \subset P$.

例 7.3.8 设 R 是整环, 零理想 $\{0\}$ 是素理想.

例 7.3.8 设 R 是整环, 零理想 $\{0\}$ 是素理想.

事实上, $\forall\, a, b \in R$, 若 $ab \in \{0\}$, 即 $ab = 0$.

$\because$ R 是整环, 无零因子. $\therefore$ $a = 0$ 或 $b = 0$, 即 $a \in \{0\}$ 或 $b \in \{0\}$.

$\therefore$ $\{0\}$ 是素理想.

例 7.3.8 设 R 是整环, 零理想 $\{0\}$ 是素理想.

事实上, $\forall\, a, b \in R$, 若 $ab \in \{0\}$, 即 $ab = 0$.

$\because$ R 是整环, 无零因子. $\therefore$ $a = 0$ 或 $b = 0$, 即 $a \in \{0\}$ 或 $b \in \{0\}$.

$\therefore$ $\{0\}$ 是素理想.

例 7.3.9 设 p 是素数, 则 $P = (p) = p\mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想.

例 7.3.8 设 R 是整环, 零理想 $\{0\}$ 是素理想.

事实上, $\forall\, a, b \in R$, 若 $ab \in \{0\}$, 即 $ab = 0$.

$\because$ R 是整环, 无零因子. $\therefore$ $a = 0$ 或 $b = 0$, 即 $a \in \{0\}$ 或 $b \in \{0\}$.

$\therefore$ $\{0\}$ 是素理想.

例 7.3.9 设 p 是素数, 则 $P = (p) = p\mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想.

证: $(p) = \{rp \mid r \in \mathbb{Z}, p \text{ 是素数}\}$.

对任意的整数 a, b, 若 $ab \in P = (p)$, 则 $p \mid ab$.

因为 p 是素数, 所以有 $p \mid a$ 或 $p \mid b$.

由此得到, $a \in P$ 或 $b \in P$.

根据定理 7.3.6, $P = (p) = p\mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想.

定理 7.3.7

在有单位元 $1_R \neq 0$ 的交换环 R 中，理想 P 是素理想的充要条件是商环 R/P 是整环.

定理 7.3.7

在有单位元 $1_R \neq 0$ 的交换环 R 中, 理想 P 是素理想的充要条件是商环 R/P 是整环.

证： (i) 因为环 R 有单位元 $1_R \neq 0$, 所以 R/P 有单位元 $1_R + P$ 和零元 $0_R + P = P$. 又因为 P 是素理想, 所以 $1_R + P \neq P$.

定理 7.3.7

在有单位元 $1_R \neq 0$ 的交换环 R 中, 理想 P 是素理想的充要条件是商环 R/P 是整环.

证： (i) 因为环 R 有单位元 $1_R \neq 0$, 所以 R/P 有单位元 $1_R + P$ 和零元 $0_R + P = P$. 又因为 P 是素理想, 所以 $1_R + P \neq P$.

(ii) 现在说明 R/P 无零因子且可交换.

事实上, 若 $(a + P)(b + P) = P$, 则 $ab + P = P$. 因此, $ab \in P$. 但 P 是交换环 R 的素理想, 根据定理 7.3.6, 得到 $a \in P$ 或 $b \in P$, 即 $a + P = P$ 或 $b + P = P$ 是 R/P 的零元. 而 R 是交换环, 则 R/P 可交换.

定理 7.3.7

在有单位元 $1_R \neq 0$ 的交换环 R 中, 理想 P 是素理想的充要条件是商环 R/P 是整环.

证： (i) 因为环 R 有单位元 $1_R \neq 0$, 所以 R/P 有单位元 $1_R + P$ 和零元 $0_R + P = P$. 又因为 P 是素理想, 所以 $1_R + P \neq P$.

(ii) 现在说明 R/P 无零因子且可交换.

事实上, 若 $(a + P)(b + P) = P$, 则 $ab + P = P$. 因此, $ab \in P$. 但 P 是交换环 R 的素理想, 根据定理 7.3.6, 得到 $a \in P$ 或 $b \in P$, 即 $a + P = P$ 或 $b + P = P$ 是 R/P 的零元. 而 R 是交换环, 则 R/P 可交换.

故商环 R/P 是整环.

定理 7.3.7

在有单位元 $1_R \neq 0$ 的交换环 R 中, 理想 P 是素理想的充要条件是商环 R/P 是整环.

证： (i) 因为环 R 有单位元 $1_R \neq 0$, 所以 R/P 有单位元 $1_R + P$ 和零元 $0_R + P = P$. 又因为 P 是素理想, 所以 $1_R + P \neq P$.

(ii) 现在说明 R/P 无零因子且可交换.

事实上, 若 $(a + P)(b + P) = P$, 则 $ab + P = P$. 因此, $ab \in P$. 但 P 是交换环 R 的素理想, 根据定理 7.3.6, 得到 $a \in P$ 或 $b \in P$, 即 $a + P = P$ 或 $b + P = P$ 是 R/P 的零元. 而 R 是交换环, 则 R/P 可交换.

故商环 R/P 是整环.

反过来, 对任意 $a, b \in R$, 满足 $ab \in P$, 有 $(a + P)(b + P) = ab + P = P$. 因为商环 R/P 是整环, 没有零因子, 所以 $a + P = P$ 或 $b + P = P$. 由此得到, $a \in P$ 或 $b \in P$. 所以, 理想 P 是素理想.

定义 7.3.6

设 M 是环 R 的 (左) 理想. 如果 $M \neq R$, 且对任意的理想 N, 使得 $M \subset N \subset R$, 有 $N = M$ 或 $N = R$, 则称 M 为 R 的**极大 (左) 理想**.

定义 7.3.6

设 M 是环 R 的 (左) 理想. 如果 $M \neq R$, 且对任意的理想 N, 使得 $M \subset N \subset R$, 有 $N = M$ 或 $N = R$, 则称 M 为 R 的**极大 (左) 理想**.

定理 7.3.8

在有单位元的非零环 R 中, 极大 (左) 理想总是存在的. 事实上, R 的每个 (左) 理想 ($\neq R$) 都包含在一个极大 (左) 理想中.

定义 7.3.6

设 M 是环 R 的 (左) 理想. 如果 $M \neq R$, 且对任意的理想 N, 使得 $M \subset N \subset R$, 有 $N = M$ 或 $N = R$, 则称 M 为 R 的**极大 (左) 理想**.

定理 7.3.8

在有单位元的非零环 R 中, 极大 (左) 理想总是存在的. 事实上, R 的每个 (左) 理想 ($\neq R$) 都包含在一个极大 (左) 理想中.

定理 7.3.9

设 R 是一个理想, 如果 $R^2 = R$ (特别地, 如果 R 有单位元, 则 R 的每个极大理想是素理想.

本课作业

1. 集合 $\{a+b\sqrt{5} \mid a,b \in \mathbb{Z}\}$ 关于实数中通常的加法与乘法是否构成环, 说明理由.
2. 设 R 是有单位元 e 的环, 证明 R 中的可逆元不是零因子.
3. 集合 $S=\left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x,y,z \in \mathbb{Z} \right\}$ 按通常矩阵加法与乘法构成环. 令

$$\begin{aligned} \psi: \quad S \quad &\to \mathbb{Z}; \\ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} &\mapsto z. \end{aligned}$$

证明: (1) ψ 为 S 到 $\mathbb{Z}$ 的满同态;

(2) 求 ψ 的核 $\ker \psi$, 并给出 $S/\ker \psi$ 到 $\mathbb{Z}$ 的一个同构映射.

4. 设 R 是交换环, I 是 R 的理想. 令 $J=\{r \in R \mid$ 存在 $n \in \mathbb{N}$ 使得 $r^n \in I\}$. 证明: J 是 R 的理想.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn