

第五章 环和域

1. \mathbb{Z} 为整数环, 在集合 $S = \mathbb{Z} \times \mathbb{Z}$ 上定义

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc).$$

证明 S 在这两个运算下成一具有单位元素的环。

证明:

(1) 对于加法, 封闭性显然, 由整数的加法的结合律和交换律可知题目中所定义的加法同样满足结合律和交换律; 零元是 $(0, 0)$, 因为 $(a, b) + (0, 0) = (0, 0) + (a, b) = (a, b)$; (a, b) 的负元为 $(-a, -b)$, 因为 $(a, b) + (-a, -b) = (a - a, b - b) = (0, 0)$ 。因此, $\mathbb{Z} \times \mathbb{Z}$ 对于所定义的加法构成加法交换群。

(2) 对于乘法, 封闭性显然,

1) 结合律:

$$\begin{aligned} ((a, b)(c, d))(e, f) &= (ac + bd, ad + bc)(e, f) = (ace + bdf + adf + bcf, acf + bdf + ade + bce) \\ (a, b)((c, d)(e, f)) &= (a, b)(ce + df, cf + de) = (ace + adf + bcf + bde, acf + ade + bce + bdf) \end{aligned}$$

即有 $((a, b)(c, d))(e, f) = (a, b)((c, d)(e, f))$, 因此乘法满足结合律。

2) 单位元:

若 $(a, b)(c, d) = (ac + bd, ad + bc) = (a, b)$, 则有 $c = 1, d = 0$, 即单位元为 $(1, 0)$ 。

(3) 乘法对加法的分配律:

$$\begin{aligned} (a, b)((c, d) + (e, f)) &= (a, b)(c + e, d + f) = (ac + ae + bd + bf, ad + af + bc + be) \\ (a, b)(c, d) + (a, b)(e, f) &= (ac + bd, ad + bc) + (ae + bf, af + be) \\ &= (ac + ae + bd + bf, ad + af + bc + be) \end{aligned}$$

因此, 乘法对加法的分配律成立。

综上所述, S 在这两个运算下成一具有单位元素的环。

2. 在整数集 \mathbb{Z} 上重新定义加法 “ \oplus ” 与乘法 “ \odot ” 为

$$a \oplus b = ab, a \odot b = a + b$$

试问 \mathbb{Z} 在这两个运算下是否成一环。

答: 不能构成环。因为乘法对加法不满足分配律。

$$a \odot (b \oplus c) = a \odot (bc) = a + bc$$

$$(a \odot b) \oplus (a \odot c) = (a + b) \oplus (a + c) = (a + b)(b + c)$$

所以, $a \odot (b \oplus c) \neq (a \odot b) \oplus (a \odot c)$ 。

3. 设 L 为一具有单位元素的交换环, 在 L 中定义:

$$a \oplus b = a + b - 1, a \odot b = a + b - ab$$

证明在新定义的运算下, L 仍成一具有单位元素的交换环, 并且与原来的环同构。

证明:

(1) 加法, 显然所定义的加法是一个二元运算:

1) 满足结合律, 因为:

$$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 2$$

$$(a \oplus b) \oplus c = (a + b - 1) \oplus c = a + b + c - 2$$

2) 有零元为 1:

$$a \oplus 1 = 1 \oplus a = a + 1 - 1 = a$$

3) a 有负元为 $2 - a$:

$$a \oplus (2 - a) = (2 - a) \oplus a = a + 2 - a - 1 = 1$$

4) 交换律:

$$a \oplus b = b \oplus a = a + b - 1$$

所以 L 对新定义加法构成加法交换群。

(2) 乘法, 显然新定义的乘法是二元运算:

1) 满足结合律:

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

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

2) 有单位元 0 :

$$a \odot 0 = 0 \odot a = a$$

3) 满足交换律:

$$a \odot b = b \odot a = a + b - ab$$

(3) 乘法对加法的分配律:

$$\begin{aligned} a \odot (b \oplus c) &= a \odot (b + c - 1) \\ &= a + (b + c - 1) - a(b + c - 1) \\ &= a + b + c - ab - ac \end{aligned}$$

$$\begin{aligned} (a \odot b) \oplus (a \odot c) &= (a + b - ab) \oplus (a + c - ac) \\ &= (a + b - ab) + (a + c - ac) - 1 \\ &= 2a + b + c - ab - ac - 1 \end{aligned}$$

综上所述, L 对新定义的加法和乘法构成有单位元的交换环。

记新运算下的环为 L' 。令 $\varphi: L \rightarrow L'$ 为

$$\varphi(a) = 1 - a$$

很容易验证该映射为同态映射。

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

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

4. 给出环 L 与它的一个子环 S 的例子, 它们分别具有下列性质:

- (1) L 具有单位元素, 但 S 无单位元素;
- (2) L 没有单位元素, 但 S 有单位元素;
- (3) L 、 S 都有单位元素, 但不相同;
- (4) L 不交换, 但 S 交换。

解: (1) 取 L 为 \mathbb{Z} , S 为 $2\mathbb{Z}$ 。 \mathbb{Z} 有单位元 1 , 而 $2\mathbb{Z}$ 无单位元。

(2) 取 \mathbb{Z}_{12} 的子环 $2\mathbb{Z}_{12} = \{0, 2, 4, 6, 8, 10\}_{mod 12}$ 和 $4\mathbb{Z}_{12} = \{0, 4, 8\}_{mod 12}$ 。可以验证 $4\mathbb{Z}_{12}$ 是 $2\mathbb{Z}_{12}$ 的子环, 满足 $2\mathbb{Z}_{12}$ 无单位元, 而 $4\mathbb{Z}_{12}$ 有单位元 4 。

(3) \mathbb{Z}_{12} 的子环 $4\mathbb{Z}_{12} = \{0, 4, 8\}_{mod 12}$ 。可以验证 \mathbb{Z}_{12} 的单位元是 1, 而 $4\mathbb{Z}_{12}$ 的单位元为 4。

(4) 取 L 为 n 阶矩阵环, S 为 n 阶对角矩阵环, 则 L 不交换而 S 交换。

5. 设 L 是一个至少有两个元素的环。如果对于每个非零元素 $a \in L$ 都有唯一的元素 b 使得

$$aba = a.$$

证明:

- (1) L 无零因子;
- (2) $bab = b$;
- (3) L 有单位元素;
- (4) L 是一个除环。

证明: (1) 先证 L 无左零因子。假设 a 是 L 的左零因子, 则 $a \neq 0$, 而且存在 $c \neq 0$ 满足 $ac = 0$ 。又根据已知条件, 存在唯一元素 b , 使得 $aba = a$, 则有 $a(b+c)a = a$, 且 $b+c \neq b$, 与条件中的唯一性矛盾。因此, L 无左零因子。类似地, 可以证明 L 无右零因子。

(2) L 无零因子, 因而满足消去律, 则

$$aba = a \Rightarrow abab = ab \Rightarrow bab = a,$$

(3) 首先, $ab = ba$, 因为 $a(a^2b - a + b)a = a$, 所以 $a^2b - a + b = b$, 即有 $a^2b = a = aba$, 由消去律可得 $ab = ba$ 。

任取 $c \in L$, 则 $ac = abac$, 故此 $c = (ba)c = (ab)c$; 另一方面, $ca = caba \Rightarrow c = c(ab)$ 。综上, 有 $c = (ab)c = c(ab)$, 所以 ab 就是单位元, 记 $ab = ba = 1$ 。

(4) 由 (3) 可知任意 $a(\neq 0) \in L$, $ab = ba = 1$, 即任意非零元都可逆。因此 L 是一个除环。

6. 设 $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$, 证明: $\mathbb{Z}[i]$ 关于复数的加法和乘法构成一个环。

证明思路: 类似于习题 1 的证明, 零元为 0, $a+bi$ 的负元为 $-a-bi$; 单位元为 1, $a+bi$ 的逆元为 $\frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}$ 。证明过程略。

7. 设 R 是特征 p 的无零因子交换环, 证明: $(a+b)^p = a^p + b^p$ 对任意 $a, b \in R$ 都成立。

证明: 见例题 5.1.9。

8. 环 R 中元 a 称为幂零的, 如果有正整数 n , 使得 $a^n = 0$ 。证明在交换环 R 中, 如果 a, b 都是幂零的, 那么 $a+b$ 也是幂零的; 证明有单位元的交换环 R 中所有幂零元构成 R 的一个理想。

证明: 第一部分: 如果 a, b 都是幂零的, 那么 $a+b$ 也是幂零的

不妨设 $a^n = 0$, $b^k = 0$, $n > k$, 则有

$$(a+b)^{n+k} = a^{n+k} + C_{n+k}^1 a^{n+k-1}b + \cdots + C_{n+k}^{n+k-1} ab^{n+k-1} + b^{n+k}$$

上式中的前 k 项中都有 $n+k-i \geq n$, $i = 1, 2, \dots, k$, 因此这 k 项中都等于 0, 同理后 n 项也都等于 0。因此, $a+b$ 也是幂零的。

第二部分: 证明 R 中所有幂零元构成 R 的一个理想。

首先对于任意 $a \in I$, $a^n = 0$, 有 $-a \in I$, 因为 $(-a)^n = ((-1)^n e)(a^n) = 0$, 其中 e 是 R 的单位元。根据第一部分证明可知, 对于任意 $a, b \in I$, 有 $a-b$ 也是幂零元, 因此, $a-b \in I$ 。又对于任意 $r \in R$, $a \in I$, $a^n = 0$, 又 $(ra)^n = r^n a^n = 0$, 即 $ra \in I$ 。

综上所述, 根据理想的定义, 所有的幂零元构成 R 的一个理想。

9. 设 $F[x]$ 是数域 F 上的一元多项式集合, 现对 $F[x]$ 定义乘法 “ \circ ” 为

$$f(x) \circ g(x) = f(g(x)).$$

问 $F[x]$ 关于多项式的加法和如上定义的乘法 “ \circ ” 是否构成环?

答: 不构成环, 因为乘法对加法不满足分配律。例如:

$$\begin{aligned} f(x) &= x+1, g(x) = 2x+1, h(x) = 3x+1 \\ f(x) \circ (g(x) + h(x)) &= f(x) \circ (5x+2) = 5x+3 \\ f(x) \circ g(x) + f(x) \circ h(x) &= 2x+2 + 3x+2 = 5x+4 \end{aligned}$$

10. 如果环 R 的加法群是循环群, 证明: R 是交换环。

证明: 设 $a \in R$ 是环 R 加法群的生成元, 因此 $R = \{na | n \in \mathbb{Z}\}$ 。

对于任意 $b, c \neq 0 \in R$, 有 $b = n_1a, c = n_2a, n_1, n_2 \in \mathbb{Z}$, 则

$$bc = (n_1a)(n_2a) = n_1n_2a^2 = (n_2a)(n_1a) = cb$$

所以, R 是交换环。

11. 设 a 是环 R 中的可逆元, 证明: a 的逆元惟一。

证明: 设存在 $b, c \in R$, 使得 $ab = ba = 1, ac = ca = 1$, 则有 $bac = b \cdot 1 = b$, $bac = 1 \cdot c = c$, 因此有 $b = c$, 即 a 的逆元惟一。

12. 设 $F = \{a+bi | a, b \in \mathbb{Q}, i^2 = -1\}$, 证明: F 关于数的加法和乘法构成一个域。

证明思路: 根据定义一一验证: 加法交换群, 乘法交换群, 乘法对加法的分配律。

加法: 零元为 0 , $a+bi$ 的负元为 $-a-bi$;

乘法: 单位元为 1 , $a+bi$ 的逆元为 $\frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}$

13. 证明: 一个至少有两个元但没有零因子的有限环是一个除环。

证明: 见定理 5.2.1。

14. 证明: $(\mathbb{Z}_n, +, \cdot)$ 是域的充分必要条件是 n 为素数。

证明: 见例 5.2.3。

15. 设 F 是一个有 4 的元素的域, 证明:

(1) F 的特征为 2;

(2) F 的不等于 0, 1 的两个元素都是方程 $x^2 = x+1$ 的解。

证明: 设 $F = \{0, 1, a, b\}$ 。

(1) 根据定理 5.1.3, 域的特征一定是某一个素数 p , 则非零元 a 生成的加法子群为 p 阶群 $\{a, \dots, pa=0\}$, 又 F 的加法群的阶为 4, 子群的阶一定整除群的阶, 所以 $p|4$ 。因此 $p=2$ 。

(2) 设 $a \neq 0, a \neq 1$, 由 (1) 可知, $a+a=0$ 。若 $a+1=0$, 则 $a=1$, 矛盾; 若 $a+1=a$, 则, 矛盾; 若 $a+1=1$, 则 $a=0$, 矛盾。所以 $a+1=b$ 。

对于乘法, 有 $a^2 \neq 0$, 又 F^* 的阶为 3, 所以 $a^2 \neq 1$ 。因此有 $a^2 = b$ 。

综上所述, $a^2 = a+1$ 。同理可证 $b^2 = b+1$ 。

16. 设 R 是特征为 p 的交换环, $a, b \in R$, 证明: $(a-b)^p = a^p - b^p$ 。

证明: $(a-b)^p = a^p - \binom{p}{1}a^{p-1}b + \cdots + (-1)^{p-1}\binom{p}{p-1}ab^{p-1} + (-1)^pb^p$

由于 $p \mid \binom{p}{k}, 1 \leq k \leq p-1$, 所以上式可变为

$$(a-b)^p = a^p + (-1)^pb^p$$

(1) 当 $p=2$ 时, 对于任意 $a \in R$, 有 $a = -a$, 所以

$$(a-b)^p = a^p + (-1)^pb^p = a^p + b^p = a^p - b^p$$

(2) 当 p 是奇素数时, 显然有

$$(a-b)^p = a^p + (-1)^pb^p = a^p - b^p$$

17. 找出 \mathbb{Z}_6 的所有理想。

解: 理想首先是子环。 \mathbb{Z}_6 的子环有 $0, 2\mathbb{Z}_6 = \{0, 2, 4\}, 3\mathbb{Z}_6 = \{0, 3\}$ 和 \mathbb{Z}_6 。

根据理想的定义, 容易验证这些都是 \mathbb{Z}_6 的理想。

18. 设 F 是域, 问 $F[x]$ 中的主理想 $\langle x^2 \rangle$ 含有哪些元? $F[x]/\langle x^2 \rangle$ 含有哪些元?

答: 由于 F 是域, 所以 $F[x]$ 是有单位元的交换环。因此

$$\begin{aligned}\langle x^2 \rangle &= \{x^2 f(x) \mid f(x) \in F[x]\} \\ F[x]/\langle x^2 \rangle &= \{[a + bx] \mid a, b \in F\}\end{aligned}$$

19. 设 $\mathbb{Z}[x]$ 为整数环上的一元多项式环, 问理想 $\langle 2, x \rangle$ 由哪些元素组成? $\langle 2, x \rangle$ 是否是主理想?

答: (1) 因为 $\mathbb{Z}[x]$ 为有单位元 1 的交换环, 故 $\langle 2, x \rangle$ 中每个元素有形状

$$2f(x) + xg(x), \text{ 其中 } f(x), g(x) \in \mathbb{Z}[x]$$

由此可见, $\langle 2, x \rangle$ 中每个元素的常数项为偶数。

(2) 由 (1) 可知, $1 \notin \langle 2, x \rangle$, 则 $\mathbb{Z}[x] \neq \langle 2, x \rangle$ 。如果 $\langle 2, x \rangle$ 是主理想, 则 $\exists p(x) \in \mathbb{Z}[x]$, 使得 $\langle 2, x \rangle = \langle p(x) \rangle = \{h(x)p(x) \mid h(x) \in \mathbb{Z}[x]\}$ 。另一方面, $2, x \in \langle 2, x \rangle$, 则有 $\exists r_1(x), r_2(x) \in \mathbb{Z}[x]$, 使得 $2 = r_1(x)p(x), x = r_2(x)p(x)$, 因此有 $p(x) \in \mathbb{Z}$, 即 $p(x) = \pm 1$, 从而有 $\langle p(x) \rangle = \mathbb{Z}[x]$, 矛盾。所以 $\langle 2, x \rangle$ 不是主理想。

20. 设 p, q 是两个不同的素数, 试求 $\langle p \rangle \cap \langle q \rangle$ 是 \mathbb{Z} 的怎样一个理想?

答: 对于任意 $k \in \langle p \rangle \cap \langle q \rangle$, 则有 $p \mid k$ 和 $q \mid k$, 因而有 $pq \mid k$, 所以 $k \in \langle pq \rangle$, 即 $\langle p \rangle \cap \langle q \rangle \subseteq \langle pq \rangle$ 。反之, 根据例 5.3.7 的结论, 有 $\langle pq \rangle \subseteq \langle p \rangle \cap \langle q \rangle$ 。因此 $\langle p \rangle \cap \langle q \rangle = \langle pq \rangle$ 。

21. 设 $R = \{a + bi \mid a, b \in \mathbb{Z}\}, I = \langle 1 + i \rangle$, 求商环 R/I 。

解: (1) 首先证明 I 中任意元素的实部和虚部奇偶性相同, 而且任何实部和虚部奇偶性相同的元素都属于 I

I 中元素都具有 $(a+bi)(1+i) = a-b+(a+b)i$ 的形式, 因此实部虚部的奇偶性相同

假设 $a+bi$ 实部虚部奇偶性相同, 则取 $c=(a+b)/2, d=(b-a)/2$,

则有 $a+bi=(c+di)(1+i) \in I$

(2) 其次证明任何 $a+bi$ (a, b 奇偶性不同) 都有

$$a+bi+I=1+I$$

任意 $a+bi+c+di \in a+bi+I$, 其中 c, d 奇偶性相同

$$\text{有 } a+bi+c+di=a+c+(b+d)i$$

当 a, b 奇偶性不同时

$a+c$ 与 $b+d$ 的奇偶性也不同。

因此 $a+c+(b+c+d)i=1+a-1+c+(b+d)i$

由于 $a-1+c$ 与 $b+d$ 奇偶性相同

所以属于 I ，因此上式：

$a+bi+c+di=1+(a-1+c)+(b+d)i \in 1+I$

反之，若任意 $1+c+di$ 属于 $1+I$ （其中 c, d 奇偶性相同）

则有 $1+c+di=a+bi+(1-a+c)+(d-b)i$

c, d 奇偶性相同， a, b 奇偶性不同

所以 $1-a+c, d-b$ 奇偶性相同

所以 $a+bi+(1-a+c)+(d-b)i \in a+bi+I$

由此得证。

所以 $R/I=\{I, 1+I\}$

22. 设 $f: R \rightarrow S$ 是环的满同态，证明：

- (1) 若 T 是 R 的一个子环，则 $f(T)$ 是 S 的一个子环；
- (2) 若 I 是 R 的一个理想，则 $f(I)$ 是 S 的一个理想；
- (3) 若 T' 是 S 的一个子环，则 $f^{-1}(T')=\{a \in R \mid f(a) \in T'\}$ 是 R 的一个子环；
- (4) 若 I' 是 S 的一个理想，则 $f^{-1}(I')=\{a \in R \mid f(a) \in I'\}$ 是 R 的一个理想。

证明思路：（1）根据子环的充要条件直接验证。

$$f(a) - f(b) = f(a - b) \in f(T)$$

$$f(a)f(b) = f(ab) \in f(T)$$

（2）根据理想的定义直接验证。

$$f(a) - f(b) = f(a - b) \in f(I)$$

$$f(a)f(r) = f(ar) \in f(I)$$

$$f(r)f(a) = f(ra) \in f(I)$$

（3）根据子环的充要条件直接验证。

$$f(a) - f(b) = f(a - b) \in T' \Rightarrow a - b \in f^{-1}(T')$$

$$f(a)f(b) = f(ab) \in T' \Rightarrow ab \in f^{-1}(T')$$

（4）根据理想的定义直接验证。

$$f(a) - f(b) = f(a - b) \in I' \Rightarrow a - b \in f^{-1}(I')$$

$$f(a)f(r) = f(ar) \in I' \Rightarrow ar \in f^{-1}(I')$$

$$f(r)f(a) = f(ra) \in I' \Rightarrow ra \in f^{-1}(I')$$

23. 设 $f: R \rightarrow S$ 是环的满同态，其核为 K ，证明：

- (1) 如果 P 是 R 的包含 K 的一个素理想，则 $f(P)$ 是 S 的素理想；
- (2) 如果 Q 是 S 的素理想，则 $f^{-1}(Q)=\{a \in R \mid f(a) \in Q\}$ 是 R 的素理想，且包含 K 。

证明思路：（1）根据 22 题的结论， $f(P)$ 是 S 的理想。设 $f(a)f(b) \in f(P)$ ，则有

$f(ab) \in f(P)$, 因而有 $ab \in P$, \mathfrak{p} 是素理想则有 $a \in P$ 或 $b \in P$, 因此有 $f(a) \in f(P)$ 或 $f(b) \in f(P)$ 。根据素理想的定义有 $f(P)$ 是 S 的素理想。

(2) 根据 22 题的结论, $f^{-1}(Q)$ 是 R 的理想。若 $ab \in f^{-1}(Q)$, 则有 $f(ab) \in Q$, 即有 $f(a)f(b) \in Q$, 由于 Q 是素理想, 有 $f(a) \in Q$ 或 $f(b) \in Q$, 即有 $a \in f^{-1}(Q)$ 或 $b \in f^{-1}(Q)$ 。因此 $f^{-1}(Q)$ 是 R 的素理想。又 Q 是 S 的素理想, 所以 $0 \in Q$, 则有 $K \subseteq f^{-1}(Q)$ 。

24. 证明定理 5.3.3。

证明: $R \cong R'$, 设该同构映射为 $\varphi: R \rightarrow R'$, 设 $a, b \in R, a', b' \in R'$ 。

(1) 整环: $ab = ba$, 有单位元 1 , 无零因子。

交换律: $\forall a', b' \in R', \exists a, b \in R$, 使得 $\varphi(a) = a', \varphi(b) = b'$, 因而有

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = b'a'$$

单位元: $\varphi(1)a' = \varphi(1)\varphi(a) = \varphi(1 \cdot a) = \varphi(a) = a'$, 同理 $a'\varphi(1) = a'$, 所以 $\varphi(1)$ 为 R' 的单位元。

无零因子: 设 $a'b' = 0$, 则 $a'b' = \varphi(a)\varphi(b) = \varphi(ab) = 0$, 因而有 $ab = 0$, 而 R 无零因子, 所以有 $a = 0$ 或 $b = 0$, 从而有 $a' = 0$ 或 $b' = 0$ 。

(2) 除环: 非零元构成乘法群。

单位元: $\varphi(1)a' = \varphi(1)\varphi(a) = \varphi(1 \cdot a) = \varphi(a) = a'$, 同理 $a'\varphi(1) = a'$, 所以 $\varphi(1)$ 为 R' 的单位元。

逆元: $\varphi(a^{-1})a' = \varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1)$, 同理有 $a'\varphi(a^{-1}) = \varphi(1)$, 所 a' 的逆元为 $\varphi(a^{-1})$ 。

(3) 域: R 是域, 交换除环是域。

首先 R 是除环, 所以 R' 也是除环, 其次由 (1) 中的交换律证明可知, R' 是交换环, 所以是域 R' 。

25. 设 I 是环 R 的一个理想, 证明: 从 R 到 R/I 有一个满同态映射。

证明思路: 参考定理 5.3.5, 直接根据同态的定义验证。

26. 设 I, J 是环 R 的理想, 定义 $I+J = \{a+b \mid a \in I, b \in J\}$, 证明: $I+J$ 是 R 的理想。

证明: 根据理想的定义直接验证。

$\forall a_1 + b_1, a_2 + b_2 \in I+J, r \in R$ 有

$$a_1 + b_1 - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I+J$$

$$r(a_1 + b_1) = ra_1 + rb_1 \in I+J$$

$$(a_1 + b_1)r = a_1r + b_1r \in I+J$$

所以 $I+J$ 是 R 的理想。

27. 设 I, J 是环 R 的理想, 定义 $I \cdot J = \{\sum_{i=1}^t a_i b_i \mid a_i \in I, b_i \in J, t \text{ 是正整数}\}$, 证明: $I \cdot J$ 是

R 的一个理想。

证明: 根据理想的定义直接验证。

$$\forall \sum_{i=1}^t a_i b_i, \sum_{i=1}^{t'} a'_i b'_i \in I \cdot J, \text{ 显然有 } \sum_{i=1}^t a_i b_i - \sum_{i=1}^{t'} a'_i b'_i \in I \cdot J.$$

$\forall r \in R$, 有

$$r \sum_{i=1}^t a_i b_i = \sum_{i=1}^t r a_i b_i = \sum_{i=1}^t (r a_i) b_i \in I \cdot J$$

$$(\sum_{i=1}^t a_i b_i) r = \sum_{i=1}^t a_i b_i r = \sum_{i=1}^t a_i (b_i r) \in I \cdot J$$

所以 $I \cdot J$ 是 R 的一个理想。

28. 设 $R = 2\mathbb{Z}$ 为偶数环,

(1) 证明: $I = \{4k | k \in R\}$ 是 R 的理想。 $I = \langle 4 \rangle$ 对吗?

(2) 证明: $\langle 4 \rangle$ 是 R 的一个极大理想。 $R/\langle 4 \rangle$ 是不是域?

证明: (1) 根据理想的定义直接验证。

$\forall 4k_1, 4k_2 \in I, n \in R$ 有

$$4k_1 - 4k_2 = 4(k_1 - k_2) \in I$$

$$n \cdot (4k_1) = (4k_1) \cdot n = 4nk_1 = 4 \cdot (nk_1) \in I$$

所以 $I = \{4k | k \in R\}$ 是 $R = 2\mathbb{Z}$ 的理想。

$I = \langle 4 \rangle$ 不对, 因为 $4 \in \langle 4 \rangle$, 但是 $4 \notin I$ 。

(2) 取 $M = \langle 4 \rangle, 2 \notin M$, 所以 M 是真理想。设 T 为 R 的理想, 且 $M \subseteq T \subseteq R$ 。设 $M \neq T$, 则 $\exists t \in T, t \notin M \Rightarrow 4 \nmid t \Rightarrow t$ 与 4 的最大公因子为 $2 \Rightarrow \exists a, b \in \mathbb{Z}$, 使得 $4a + tb = 2$ 。令 $a = 2k + r, b = 2l + r_1, r, r_1 \in \{0, 1\}$, 则有 $2 = 4(2k) + t(2l) + 4r + tr_1 \in T \Rightarrow T = R$ 。因此, $\langle 4 \rangle$ 是 R 的一个极大理想。

因为 $[2] \in R/\langle 4 \rangle, [2] \neq 0, [2]^2 = 0$, 故 $R/\langle 4 \rangle$ 有零因子, 不是域。