第4章 环

§4.1 子环

1. 证明：(1) ~~$\forall a,b \in H \cap S$~~ 由 $e \in H \cap S$，故 $H \cap S$ 非空，e：环的单元

$\forall a, b \in H \cap S$，有 $a, b \in H$，$a, b \in S$ 有 $a-b \in H$，$a-b \in S$

故 $a-b \in H \cap S$.

又 $\forall a, b \in H \cap S$，有 $a \cdot b \in H \cap S$.

故 $H \cap S$ 为 R 的子环

(2) 同(1)，对数乘运算的法.

□

2. 证明：由 $\mathbb{Z}[i]^{\times}$ 为 $\mathbb{Z}[i]$ 的所有乘法的逆元组成的集合

由命题 4.1.2(3) 即求 $\alpha \in \mathbb{Z}[i]$，有 $N(\alpha)=1$ 的所有 α.

令 $\alpha = a+bi$，则 $N(\alpha) = (a+bi)(a-bi) = a^2+b^2 = 1$，$a, b \in \mathbb{Z}$.

故有 $a=\pm 1$ 或 $b=\pm 1$ 即 $\alpha = \pm 1, \pm i$.

于是 $\mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\}$

□

3. 证明：类似于例 4.1.2，高斯整环的证明.

① 先证 $\mathbb{Z}[\sqrt{d}]$ 是 $\mathbb{C}$ 的子环，由 $0 \in \mathbb{Z}[\sqrt{d}]$，故 $\mathbb{Z}[\sqrt{d}]$ 非空.

对于给的 $\alpha = a+b\sqrt{d}$，$\beta = c+h\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$，$a, b, c, h \in \mathbb{Z}$.

有 $\alpha - \beta = (a-c) + (b-h)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

$\alpha\beta = (ac+bhd) + (ah+bc)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

故 $\mathbb{Z}[\sqrt{d}]$ 是 $\mathbb{C}$ 的子环. 由

② 由 $\mathbb{C}$ 中乘法可交换，且 $1 \in \mathbb{Z}[\sqrt{d}]$ 故 $\mathbb{Z}[\sqrt{d}]$ 是有单位元交换环.

由 $\mathbb{C}$ 中无零因子，故 $\mathbb{Z}[\sqrt{d}]$ 中也无零因子.

于是 $\mathbb{Z}[\sqrt{d}]$ 是整环.

□

4. (1). 由 $R \subseteq M_2(C)$ 且 $\begin{pmatrix}0&0\\0&0\end{pmatrix} \in R$ 故 R 非空.

$\forall A=\begin{pmatrix}a&b\\0&0\end{pmatrix}, B=\begin{pmatrix}c&d\\0&0\end{pmatrix} \in R$, $a,b,c,d \in C$

有 $A-B=\begin{pmatrix}a-c&b-d\\0&0\end{pmatrix} \in R$ $A \cdot B=\begin{pmatrix}ac&ad\\0&0\end{pmatrix} \in R$.

故 R 是 $M_2(C)$ 的子环.

同理 S 为 R 的子环.

(2). $\forall \begin{pmatrix}a&b\\0&0\end{pmatrix} \in R$, $c \neq 0$. $c \in C$.

$$\begin{pmatrix}0&c\\0&0\end{pmatrix}\begin{pmatrix}a&b\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix} \neq \begin{pmatrix}0&c\\0&0\end{pmatrix}$$

故 R 无乘法单位元.

$\forall \begin{pmatrix}a&0\\0&0\end{pmatrix} \in S$. $\begin{pmatrix}b&0\\0&0\end{pmatrix} \in S$ 由 $\begin{pmatrix}a&0\\0&0\end{pmatrix}\begin{pmatrix}b&0\\0&0\end{pmatrix}=\begin{pmatrix}ab&0\\0&0\end{pmatrix}=\begin{pmatrix}b&0\\0&0\end{pmatrix}$

$\Rightarrow a=1$ 故 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ 为 S 的乘法单位元.

5. (1). 上一题中 $R \subseteq M_2(C)$ $R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix} \middle| a,b \in C\right\}$

成整数环 $\mathbb{Z}$, 单位元 1. 子环 $M_2(\mathbb{Z})$ 无单位元.

(2). 上一题中. $R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix} \middle| a,b \in C\right\}$ 无单位元

$S=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix} \middle| a \in C\right\}$ 有单位元, 且 S 是 R 的子环.

(3). $\mathbb{Q} \subseteq R$ 有理数域, 与实数域.

上一题中. $M(2,\mathbb{R})$ 有单位元 $\begin{pmatrix}1&0\\0&1\end{pmatrix}$. 子环 $S=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix} \middle| a \in C\right\}$

有单位元 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$.

(4). 上一题中. $M_2(C)$ 不是交换环, 但子环

$S=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix} \middle| a \in C\right\}$ 是交换环.

6. 证明: 由幂零元的定义 $a^n=0$.

故由 $a^n-1=(a-1)(a^{n-1}+\cdots+1)$

$\Rightarrow 1-a^n=(1-a)(a^{n-1}+a^{n-2}+\cdots+1)=1$

于是 $(1-a)$ 可逆, 逆元为 $(1+a^0+\cdots+a^{n-1})$

7. 证明:

$\Rightarrow$ 由 $\bar{z} \in \mathbb{Z}/n\mathbb{Z}$ 是幂零元. 设 $(\bar{z})^k = \bar{0}$ $\quad \overline{z^k} = \bar{0}$.

于是 $n \mid z^k$ 于是对任意 n 的素因子 p, $p \mid n$ 有 $p \mid z^k$

p 是素数 故 $p \mid z$, 即 p 是 z 的素因子

$\Leftarrow$ 由算术基本定理, 设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, $p_1, p_2 \cdots p_m$ 为不同的素数.

$\alpha_j > 0$. $\quad j \le m$.

由 $p_j \mid z$. $(\forall j \le m)$ 于是令 $k = \max\{\alpha_1, \alpha_2, \cdots \alpha_m\}$

有 $n \mid (p_1 p_2 \cdots p_m)^k$, 且 $(p_1 p_2 \cdots p_m)^k \mid z^k$.

于是 $n \mid z^k$ 于是 $(\bar{z})^k = \overline{z^k} = \bar{0}$. 于是 $\bar{z}$ 是 $\mathbb{Z}/n\mathbb{Z}$ 中的幂零元. □

8. 证明: 由 $Z(R) = \{a \in R \mid ra = ar \ \forall r \in R\}$

显然 $0 \in Z(R)$ 故 $Z(R)$ 非空.

(1) $\forall a, b \in Z(R)$ $\quad \forall r \in R$ $\quad r(a-b) = ra - rb = ar - br = (a-b)r$

故 $a - b \in Z(R)$

(2) $\forall a, b \in Z(R)$ $\quad \forall r \in R$ $\quad rab = arb = abr$

故 $ab \in Z(R)$

于是 $Z(R)$ 是 R 的子环. □

9. 证明 由 R 为有限环, S 为 R 的子环, 故作为加群, 于是 R 的加法子群.

即 $S \le R$ 由 拉格朗日定理 有 ~~$|S| \le |R|$~~

$|S| \mid |R|$

□

10. 证明: $\Rightarrow$ 若 K 为 F 的子域 (子体), 则. (1). (2) 显然成立.

$\Leftarrow$. 由 $0, 1 \in K$. 非空子集 K 关于加法成子群, 且又对乘法 (非零元) 成子群.

则 K 上的加法与乘法 自然满足乘法结合律, 以及加法和乘法之间的结合律

且对加法是交换群. 又由 $1 \in K$, 有乘法单位元, 故 K 为域 (子体)

于是 K 是 F 的子域 (子体) □

4.2 理想及商环

1. 证明命题4.2.1,

(1) 也见习题4.1.1.

由 $0 \in H \cap S$. 故 $H \cap S$ 非空.

对 $\forall a, b \in H \cap S$, 有 $a, b \in H$, $a, b \in S$, 有 $a-b \in H$, $a-b \in S$. 故 $a-b \in H \cap S$.

对 $\forall a, b \in H \cap S$, 有 $a \cdot b \in H \cap S$.

故 $H \cap S$ 为 R 的子环.

一般地, 同理应用数学归纳法可证: 若干子环的交是子环 □

(2). ~~由(1)可得, $H \cap S$ 为 S 的子环.~~

由 $0 \in H \cap S$, $H \cap S$ 非空. 且 $H \cap S \subseteq S$.

① 对 $\forall a, b \in H \cap S$, 由 H 为理想 故有 $a-b \in H$. $\left.\begin{matrix}\\ \\ \end{matrix}\right\} \Rightarrow a-b \in H \cap S$

由 S 为子环, 故有 $a-b \in S$. $\left.\begin{matrix}\\ \\ \end{matrix}\right\}$

② 对 $\forall r \in S$, $\forall a \in H \cap S$. 有 $a \in H$. 由于 H 为 R 的理想 $r \in S \subseteq R$.

~~故 $ra, ar \in H$. 且 $ra = ar$~~ 故 $ra \in H$, $ar \in H$

又由 $a, r \in S$, 故 $ar \in S$, $ra \in S$.

因此 ~~ar~~ $ar \in H \cap S$, $ra \in H \cap S$ 因此 $H \cap S$ 为 S 的理想. □

(3). 由 $0 \in H \cap S$ 故 $H \cap S$ 非空.

① 对 $\forall a, b \in H \cap S$. 由 H, S 均为理想 故 $a-b \in H \cap S$.

② 对 $\forall r \in R$, $\forall a \in H \cap S$. $ra \in H \cap S$, $ar \in H \cap S$ (因为 H, S 为理想)

故 $H \cap S$ 为 R 的理想

一般地, 同理可得, 若干理想的交是理想 □

2. 证明: $0 \in \bigcup_{k=1}^{\infty} H_k$ 故其显然非空.

$\forall a, b \in \bigcup_{k=1}^{\infty} H_k$, $\forall r \in R$, 不妨设 $a \in H_{k_1}$ $b \in H_{k_2}$ $k_1 \le k_2$.

则 $a \in H_{k_1} \subseteq H_{k_2}$ 故 $a-b \in H_{k_2} \subseteq \bigcup_{k=1}^{\infty} H_k$ $ar, ra \in H_{k_1} \subseteq \bigcup_{k=1}^{\infty} H_k$

故 $\bigcup_{k=1}^{\infty} H_k$ 是 R 的理想 □

3. $\Leftarrow$ 显然

$\Rightarrow$ 由于 $a\in R$ 的乘法可逆元，故存在 $a^{-1}\in R$，$a^{-1}\cdot a=e$（R 的乘法单位元）

由于 I 是理想 故 $a\in I$，$a^{-1}\in R$，有 $a\cdot a^{-1}=e\in I$.

故对 $\forall b\in R$ 有 $b=e\cdot b\in I$. 故 $I=R$ □

4. 证明：若 $I\neq\{0\}$

则 I 中有非零元 a，~~且 a 在 R 中是可逆的（在是主张~~

且 a 在 F 中是可逆的 由第3题 知 $I=F$ □

5. 证明例 4.2.1 (2)

由于 $\mathbb{Z}/m\mathbb{Z}$ 的理想 H 是其子环. 由 例4.1.1. 知

所有可能的~~理想~~是 $\{d\mathbb{Z}/m\mathbb{Z} \mid d|m,\ 1\le d\le m\}$.

下面引证. 即它们均是理想

首环 $\{d\mathbb{Z}/m\mathbb{Z} \mid d|m,\ 1\le d\le m\}$ 是 $\mathbb{Z}/m\mathbb{Z}$ 的子环.

现证对 $\forall\ \bar{r}\in\mathbb{Z}/m\mathbb{Z}$，~~对~~ 对 $\forall\ \overline{k_1 d}$，~~$\in$~~ $\in d\mathbb{Z}/m\mathbb{Z}$ 有

$\bar{r}\cdot\overline{k_1 d}=\overline{rk_1 d}\in d\mathbb{Z}/m\mathbb{Z}$　　$\overline{k_2 d}\cdot\bar{r}=\overline{k_2 r\cdot d}\in d\mathbb{Z}/m\mathbb{Z}$.

故 $\mathbb{Z}/m\mathbb{Z}$ 的所有理想是 $\{d\mathbb{Z}/m\mathbb{Z} \mid d|m,\ 1\le d\le m\}$ □

6. 证明命题 4.2.2 (2) (3)

(2) 由(1)知 $H+N$ 为 R 的子环. 故只需证明

对 $\forall r\in R$，$\forall a\in H+N$.（则存在 $h_1\in H$，$n\in N$. 有 $a=h+n$）

故 $r\cdot a=r(h+n)=rh+rn$ 由 H,N 为 R 的理想 故 $r\cdot R=rh+rn\in H+N$.

同理 $a\cdot r\in H+N$. 故 $H+N$ 为 R 的理想

(3) 由(2)与数学归纳法可证. "证毕"

□

7. 证明：A B. C 都是R的子环（由定义可立证即可）

对 $\forall \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \in R$. $\forall \begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix} \in A$.

$$\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix} = \begin{pmatrix} r_1a_1+r_2a_2 & 0 \\ r_3a_1+r_4a_2 & 0 \end{pmatrix} \in A.$$

$$\begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} = \begin{pmatrix} a_1r_1 & a_1r_2 \\ a_2r_1 & a_2r_2 \end{pmatrix} \notin A \ (\text{若 } a_1, a_2 \neq 0 \text{ 时}, r_2 \neq 0)$$

故 A 是R的右理想 但不是R的理想

$\forall \begin{pmatrix} b_1 & b_2 \\ 0 & 0 \end{pmatrix} \in B$，有

$$\begin{pmatrix} b_1 & b_2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} r_1 & r_3 \\ r_3 & r_4 \end{pmatrix} = \begin{pmatrix} b_1r_1+b_2r_3 & b_1r_2+b_2r_4 \\ 0 & 0 \end{pmatrix} \in B$$

$$\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} r_1b_1 & r_2b_2 \\ r_3b_1 & r_3b_2 \end{pmatrix} \notin B \ (\text{若 } r_3 \neq 0, b_1 b_2 \neq 0)$$

故 B是R的左理想 但不是R的理想.

$\forall \begin{pmatrix} c_1 & c_2 \\ 0 & c_3 \end{pmatrix} \in C$ 有

$$\begin{pmatrix} c_1 & c_2 \\ 0 & c_3 \end{pmatrix} \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} = \begin{pmatrix} c_1r_1+c_2r_3 & c_1r_2+c_2r_4 \\ c_3r_3 & c_3r_4 \end{pmatrix} \notin C \quad (c_3, r_3 \neq 0 \text{ 时})$$

$$\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ 0 & c_3 \end{pmatrix} = \begin{pmatrix} r_1c_1 & r_1c_2+r_2c_3 \\ r_3c_1 & r_3c_2+r_4c_3 \end{pmatrix} \notin C \quad (\text{当 } r_3, c_1 \neq 0 \text{ 时})$$

故 C即不是R的左理想，也不是R的右理想 □

8. 证明：由定理 4.2.1. 只需证 R/P 为交换环.

由R是交换环，故对 $\forall \bar{a}, \bar{b} \in R/P$ 有

$$\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}.$$

由R有单位元1，故有 $\bar{a}\bar{1} = \overline{a \cdot 1} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a} = \bar{a}$.

故 R/P 是有单位元交换环，单位元为 $\bar{1}$. □

9. $\mathbb{Z}/12\mathbb{Z}$ 的所有子环 $\mathbb{Z}/12\mathbb{Z}$, $2\mathbb{Z}/12\mathbb{Z}$, $3\mathbb{Z}/12\mathbb{Z}$, $4\mathbb{Z}/12\mathbb{Z}$, $6\mathbb{Z}/12\mathbb{Z}$, $12\mathbb{Z}/12\mathbb{Z}$. (见例 4.1.1)

$\mathbb{Z}/12\mathbb{Z}$ 的所有理想 $\mathbb{Z}/12\mathbb{Z}$, $2\mathbb{Z}/12\mathbb{Z}$, $3\mathbb{Z}/12\mathbb{Z}$, $4\mathbb{Z}/12\mathbb{Z}$, $6\mathbb{Z}/12\mathbb{Z}$, $12\mathbb{Z}/12\mathbb{Z}$ (见例 4.2.2)

□

10. 证明：令 $I=\{a \mid a^n=0, \exists\, n\in\mathbb{Z}_{>0}\}=\{a \mid \exists n\in\mathbb{Z}_{>0}, s.t.\ a^n=0\}$

首先由 $0\in I$，故 I 非空.

对 $\forall a,b\in I$，则存在 $m,n\in\mathbb{Z}_{>0}$，s.t. $a^m=0$，$b^n=0$.

故 $(a-b)^{m+n}=\sum_{k=0}^{m+n}\binom{m+n}{k}a^k b^{m+n-k}(-1)^{m+n-k}=0$.

故 $a-b\in I$

对 $\forall r\in R$，有 $(ra)^m=r^m\cdot a^m=0$（想交换环），$(ar)^m=a^m r^m=0$.

故 $ar\in I$，$ra\in I$.

故 $I\triangleleft R$（I 是 R 的一个理想） □

11：证明：类似10题.

由 $I\subseteq \mathrm{rad}I$，故 $\mathrm{rad}I$ 非空.

① 对 $\forall a,b\in \mathrm{rad}I$，存在 $m,n\in\mathbb{Z}_{>0}$，使得 $a^m, b^n\in I$.

故 $(a-b)^{m+n}=\sum_{k=0}^{m+n}(-1)^k\binom{m+n}{k}a^{m+n-k}b^k$

若 $n\geq k$，由 $a^{m+n-k}b^k=a^m(a^{n-k}b^k)\in IR\subseteq I$

若 $n<k$ 则 $a^{m+n-k}b^k=(a^{m+n-k}b^{k-n})b^n\in RI\subseteq I$

故 $(a-b)^{m+n}\in I$，故 $a-b\in \mathrm{rad}I$.

② 对 $\forall r\in R$ $(ra)^m=(ar)^m=a^m r^m\in IR\subseteq I$.（交换环.）

故 $ra\in \mathrm{rad}I$，$ar\in \mathrm{rad}I$.

即 $\mathrm{rad}I$ 是 R 的一个理想 □

4.3 一元多项式环

1. (1) 证明：设 $f(x)=\sum_{i=0}^{n} a_i x^i$ $a_n\neq 0$ $g(x)=\sum_{j=0}^{m} b_j x^j$ $b_m\neq 0$

不妨设 $n\geq m$

则 $f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i$ 若 $i>m$ 则 $b_i=0$

故 $\deg(f(x)+g(x))\leq n=\max\{\deg f(x),\deg g(x)\}$

若 $f(x)=0$ 或 $g(x)=0$，结果显然成立 □

(2) 同理 $f(x)\cdot g(x)=\sum_{i=0}^{m+n} c_i x^i$，$c_i=\sum_{k_1+k_2=i} a_{k_1}b_{k_2}$

故 $\deg f(x)\cdot g(x)\leq m+n=\deg f(x)+\deg g(x)$

若 $f(x)=0$ 或 $g(x)=0$，结论成立. □

2. (1) $p(x)+q(x)=9x^3-3x^2+37x-9$

$p(x)\cdot q(x)=14x^6-21x^5+94x^4-142x^3+144x^2-181x+20$

(2) $p(x)+q(x)=x^3+x^2+x+1$

$p(x)\cdot q(x)=x^5+x$

(3) $p(x)+q(x)=x$

$p(x)\cdot q(x)=2x^6+x^4+2x^3+2x+2$ □

3. (1) 证明：① $\Rightarrow$ 由 $(u(x))\subseteq(v(x))$ 故 $u(x)\in(v(x))$ 故存在 $f(x)\in F[x]$ 使得 $u(x)=v(x)\cdot f(x)$ 于是 $v(x)\mid f(x)$.

$\Leftarrow$ 若 $v(x)\mid u(x)$，则存在 $f(x)\in F[x]$，使得 $u(x)=v(x)\cdot f(x)$. 故 $u(x)\in(v(x))$ 于是 $(u(x))\subseteq(v(x))$ □

② $\Rightarrow$ 由 $u(x)\in(v(x))$ 于是存在 $f(x)\in F[x]$，使得 $u(x)=v(x)\cdot f(x)$.

由 $v(x)\in(u(x))$ 于是存在 $g(x)\in F[x]$ 使得 $v(x)=u(x)\cdot g(x)$

于是 $v(x)=u(x)g(x)=v(x)\cdot f(x)\cdot g(x)$ 故 $f(x)\cdot g(x)=1$ 由于是域，$F[x]$ 为整环

故无零因子. 于是 $\deg f(x)=\deg g(x)=0$ 故存在 $k\in F^*$ 使得 $v(x)=ku(x)$.

⇐ 由 $v(x)=ku(x)$ $k\in F^*$. 故 $v(x)\in(u(x))$ $\Rightarrow (v(x))\subseteq(u(x))$

由 $u(x)=k^{-1}v(x)$ 故 $u(x)\in(v(x))$ $\Rightarrow (u(x))\subseteq(v(x))$

得 $(u(x))=(v(x))$ □

(2). 由 $d(x)=\gcd(u(x),v(x))$ 故 $d(x)\mid u(x)$. $d(x)\mid v(x)$

① 得 $(u(x))\subseteq(d(x))$ $(v(x))\subseteq(d(x))$

从而 $(u(x))+(v(x))\subseteq(d(x))$

② 由 $d(x)=\gcd(u(x),v(x))$ 故存在 $f(x),g(x)\in F[x]$

使得 $f(x)u(x)+v(x)\cdot g(x)=d(x)$.

故 $d(x)\in(u(x))+(v(x))$ $\Rightarrow (d(x))\subseteq(u(x))+(v(x))$ □

③ 对任意 $f(x)\in(u(x))\cap(v(x))$ 故 $u(x)\mid f(x)$, $v(x)\mid f(x)$

得由 $m(x)=\operatorname{lcm}[u(x),v(x)]$ 得 $m(x)\mid f(x)$.

得存在 $g(x)\in F(x)$, 使得 $f(x)=m(x)\cdot g(x)$, 故 $f(x)\in(m(x))$

得 $(u(x))\cap(v(x))\subseteq(m(x))$

另现在对任意 $h(x)\in(m(x))$ 存在 $a(x)\in F(x)$. 使得 $h(x)=m(x)\cdot a(x)$

故 $h(x)\in(u(x))$, $h(x)\in(v(x))$ 因此 $h(x)\in(u(x))\cap(v(x))$

得 $(m(x))\subseteq(u(x))\cap(v(x))$

得证 □

4. (1). 不是. $f(x)\in I$, $f(x)-f(x)=0\notin I$.

(2). 是: $0\in I$. 故 I 非空, $\forall f(x),g(x)\in I$, 则 $f(x)-g(x)\in I$. 其系数次为若干个偶数

或者, 仍是偶数. 对 $\forall r(x)\in\mathbb{Z}[x]$, $f(x)r(x)=r(x)f(x)\in I$.

故 I 是理想

(3). 不是 $8x^5\in I$. $-8x^5+3\in I$ $8x^5-8x^5+3=3\notin I$. □

5. 证明：① 对 $\forall\ a+b\sqrt{d} \in \{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\}$

令 $f(x)=a+bx \in \mathbb{Q}[x]$ 则 $f(\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$

故 $\{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\} \subseteq \mathbb{Q}[\sqrt{d}]$.

② 对任意 $g(\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$. $g(x) \in \mathbb{Q}[x]$

由带余除法，存在 $q(x)$，$r(x)$ 使得 $g(x)=q(x)\cdot(x^2-d)+r(x)$

其中 $r(x)=0$ 或 $\deg r(x)\le 1$. 令 $r(x)=cx+h$. (c,h 可能为0)

故 $g(\sqrt{d})=c\sqrt{d}+h \in \{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\}$

因此 $\mathbb{Q}[\sqrt{d}] \subseteq \{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\}$

故 $\mathbb{Q}[\sqrt{d}]=\{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\}$ □

6. 证明：由 $\mathbb{R}[i]$ 的定义及 $i^2=-1\in\mathbb{R}$ 得

$\mathbb{R}[i]=\{a+bi \mid a,b\in\mathbb{R}\}$

且 $\{a+bi \mid a,b\in\mathbb{R}\}=\mathbb{C}$ 故得证 □

7. 证明：由例题3.4.4得 $R/I=\{\overline{a+bx} \mid a,b\in\mathbb{Q}\}$.

令 $\varphi: R/I \longrightarrow \mathbb{Q}[i]$

$\overline{a+bx} \longmapsto a+bi$

由 $\overline{a+bx}=\overline{c+dx} \Leftrightarrow a+bx=c+dx \Leftrightarrow a=c,\ b=d$

$\Leftrightarrow a+bi=c+di$

$\Leftrightarrow \varphi(\overline{a+bx})=\varphi(\overline{c+dx})$

因此 φ 是良定义的，且 φ 是单射，又显然 φ 是满射，故 φ 是双射.

对 $\forall\ \overline{a+bx},\ \overline{c+dx} \in R/I$.

有 $\varphi(\overline{a+bx})+\varphi(\overline{c+dx})=(a+bi)+(c+di)=(a+c)+(b+d)i=\varphi(\overline{a+bx}+\overline{c+dx})$

$\varphi(\overline{a+bx})\varphi(\overline{c+dx})=(a+bi)(c+di)=(ac-bd)+(ad+bc)i$

$=\varphi(\overline{(ac-bd)+(ad+bc)x})=\varphi(\overline{ac-bd+(ad+bc)x+bd(x^2+1)})$

$=\varphi(\overline{ac+(ad+bc)x+bdx^2})=\varphi(\overline{(a+bx)(c+dx)})$

故 φ 保持运算，故 $R/I\cong\mathbb{Q}[i]$ □

8. 证明：

(1) 由 $1 \in R \subset R[[x]]$ 且对 $\forall f(x) = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$

有 $1 \cdot f(x) = f(x) \cdot 1 = f(x) \in R[[x]]$

故 $R[[x]]$ 是有单位元环，单位元为 1.

对 $\forall f(x) = \sum_{n=0}^{\infty} a_n x^n$, $g(x) = \sum_{n=0}^{\infty} b_n x^n$.

则 $f(x) \cdot g(x) = \sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) x^n$

$= \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} b_i a_{n-i} \right) x^n$ [R可交换]

$= \sum_{n=0}^{\infty} b_n x^n \cdot \sum_{n=0}^{\infty} a_n x^n = g(x) f(x)$.

故 $R[[x]]$ 是交换环

□

(2): 由 $(1-x) \cdot f(x) = 1 \Rightarrow f(x) = \frac{1}{1-x} = 1 + x + x^2 + \cdots$ 且 $f(x) \cdot (1-x) = 1$

故 $1-x$ 是 $R[[x]]$ 中的可逆元，逆元为 $\frac{1}{1-x}$.

□

(3) 若存在 $g(x) = \sum_{n=0}^{\infty} b_n x^n$ 使得 $\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = 1$.

则 $\sum_{i=0}^{n} a_i b_{n-i} = C_n = (1, 0, 0, \cdots 0, \cdots)$ $n \geq 0$

$$\begin{cases} a_0 b_0 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \\ \vdots \end{cases}$$

故若 $\sum_{n=0}^{\infty} a_n x^n$ 为 $R[[x]]$ 中可逆元 则有 $a_0 b_0 = 1$ 故 a_0 为 R 中的可逆元.

若 a_0 是 R 中的可逆元，则 $b_0 = a_0^{-1}$,

则可得 $a_0 b_1 + a_0 b_0 = 0 \Rightarrow b_1 = a_0^{-1}(-a_0 b_0)$

同理可得 $b_2, b_3 \cdots$

即存在 $g(x) = \sum_{n=0}^{\infty} b_n x^n$, 使得 $\sum_{n=0}^{\infty} a_n x^n \cdot g(x) = g(x) \cdot \sum_{n=0}^{\infty} a_n x^n = 1$.

故 $\sum_{n=0}^{\infty} a_n x^n$ 是 $R[[x]]$ 中的可逆元

□

9. 证明：若 $f(x)=0$，则 $\deg f(x)<\deg g(x)$，则令 $q(x)=0$，$r(x)=f(x)$，即可。

现在 $\deg f(x)\geq \deg g(x)$，对 $\deg f(x)$ 做数学归纳法。

若 $\deg f(x)=0$，则 $\deg g(x)=0$，$g(x)=\pm 1$。令 $q(x)=\frac{f(x)}{g(x)}$，$r(x)=0$，即可。

假设对小于 n 次的多项式 $f(x)$ 均成立，则

令 $f(x)=a_nx^n+\cdots+a_1x+a_0 \quad a_n\neq 0,\ a_i\in\mathbb{Z}$

$g(x)=b_mx^m+\cdots+b_1x+b_0 \quad b_m=\pm 1,\ b_i\in\mathbb{Z}$.

由 $n\geq m$，令 $f_1(x)=f(x)-\frac{a_n}{b_m}x^{n-m}g(x)$，则 $\deg f_1(x)<n$.

由归纳假设 存在 $q_1(x),r(x)\in\mathbb{Z}[x]$，使得

$f_1(x)=f(x)-\frac{a_n}{a_m}x^{n-m}g(x)=g(x)q_1(x)+r(x)$. 其中 $r(x)=0$ 或 $r(x)\neq 0$ $\deg r(x)<\deg g(x)$.

令 $q(x)=q_1(x)+\frac{a_n}{a_m}x^{n-m}$

即：$f(x)=q(x)g(x)+r(x)$. 即可。

下证：唯一性。

设另有 $f(x)=q_1(x)g(x)+r_1(x)$，$q_1(x),r_1(x)\in\mathbb{Z}[x]$.

其中 $r_1(x)=0$ 或 $r_1(x)\neq 0$，$\deg r_1(x)<\deg g(x)$，则

$$(q(x)-q_1(x))g(x)=r(x)-r_1(x)$$

若 $q(x)-q_1(x)\neq 0$，则

$$\deg\left(q(x)-q_1(x)\right)g(x)\geq \deg g(x)>\deg(r(x)-r_1(x)) \text{ 矛盾.}$$

故 $q(x)-q_1(x)=0$ 即 $q(x)=q_1(x)$，亦得 $r(x)=r_1(x)$ □.

4.4 环的同态与同构.

1. ① 证明：由于 φ 满，故存在 $a \in R$, s.t. $\varphi(a) = 1'$.

由于 φ 是同态，故 $\varphi(1) = \varphi(1) \cdot 1' = \varphi(1) \cdot \varphi(a) = \varphi(1 \cdot a) = \varphi(a) = 1'$

② 由 $\varphi(1)(\varphi(1) - 1') = \varphi(1 \cdot 1) - \varphi(1) = 0$

由于 R 无零因子，故且 $\varphi(1) \neq 0$，因此 $\varphi(1) - 1' = 0$ 即：$\varphi(1) = 1'$ □

2. 证明：由整数环 $(\mathbb{Z}; +, \cdot)$ 有单位元 1，但偶数环 $(2\mathbb{Z}; +, \cdot)$ 不存在单位元

故不同构

3. ~~$\mathbb{Z}_{2\mathbb{Z}} = \{\bar{0}, \bar{1}\}$~~

~~$\mathbb{Z}_{3\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}\}$~~

~~$2\mathbb{Z} \not\cong 3\mathbb{Z}$~~

反证，设存在映射 $\varphi: 2\mathbb{Z} \to 3\mathbb{Z}$，为环同构 □

且 $\varphi(2) = 3m$, $m \in \mathbb{Z}$

$\varphi(2n) = 3 \quad n \in \mathbb{Z}$

$\varphi(2n) = \varphi(2) \cdot n = 3mn = 3$ □

故 $mn = 1$，故 $m = n = 1$ 或 $m = n = -1$.

$\varphi(2) = 3$ 或 -3，$\varphi(2)^2 = \varphi(4) = 2\varphi(2)$ 矛盾 ↓

4. 参考 P87 页命题 3.6.1 的证明即可.

5. 证明：由 $F[\alpha] = \{f(\alpha) \mid f(x) = F[x]\}$ 的定义

知 σ 一定是满射.

且 $\sigma(f(x) + g(x)) = f(\alpha) + g(\alpha) = \sigma(f(x)) + \sigma(g(x))$

$\sigma(f(x) \cdot g(x)) = f(\alpha) g(\alpha) = \sigma(f(\alpha)) \cdot \sigma(g(\alpha))$. □

6. 参考例 4.4.3

令 $\varphi: \mathbb{Q}[x] \to \mathbb{Q}$

$f(x) \mapsto f(0), \quad \forall f(x) \in \mathbb{Q}[x]$

则 $\varphi(f(x) + g(x)) = f(0) + g(0) = \varphi(f(x)) + \varphi(g(x))$

$\varphi(f(x) \cdot g(x)) = f(0) \cdot g(0) = \varphi(f(x)) \cdot \varphi(g(x))$

故 φ 是环同态，且显然是环满同态 $\forall m \in \mathbb{Q}$，$\exists f(x) + m \in \mathbb{Q}[x]$

下证 $\ker\varphi = (x)$ 显然 $(x) \subseteq \ker\varphi$. 反过来 $\forall f(x) \in \ker\varphi$. $\deg g(x) = 1$

由带余除法：存在 $q(x), r(x) \in \mathbb{Q}[x]$ 使得 $f(x) = g(x)q(x) + r(x)$ $r(x) = 0$ 或 $\deg r(x) < 1$

~~不妨设~~ 若 $r(x)\neq 0$，则 $\deg r(x)=0$，令 $r(x)=m\in\mathbb{Q}$.

代入 $x=0$，有 $0=f(0)=r(0)=m$

故 $r(x)=0$. 即此 $x\mid f(x)$. 由 $f(x)$ 的任意性. $\ker\varphi\subseteq(x)$

故 $\mathbb{Q}[x]/(x)\cong\mathbb{Q}$.

(2). 令 $\varphi:\mathbb{Q}[x]\to\mathbb{C}$.

$f(x)\mapsto f(i)$. $\forall f(x)\in\mathbb{Q}[x]$

则 $\varphi(f(x)+g(x))=f(i)+g(i)=\varphi(f(x))+\varphi(g(x))$.

$\varphi(f(x)g(x))=f(i)g(i)=\varphi(f(x))\varphi(g(x))$.

故 φ 是环同态.

下证 $\ker\varphi=(x^2+1)$. 显然 $(x^2+1)\subseteq\ker\varphi$.

反之，$\forall f(x)\in\ker\varphi$. 由带余除法，存在 $g(x),r(x)\in\mathbb{Q}[x]$，使得.

$f(x)=(x^2+1)g(x)+r(x)$. $r(x)=0$ 或 $r(x)\neq 0$ 且 $\deg r(x)<2$.

① 若 $r(x)\neq 0$，则令 $r(x)=a+bx$. 其中 $a,b\in\mathbb{Q}$ 代入 $x=i$，有

$0=f(i)=r(i)=a+bi$ 由 $a,b\in\mathbb{Q}$，故 $a=b=0$，即 $r(x)=0$.

即此 $(x^2+1)\mid f(x)$ 由 $f(x)$ 的任意性 有 $\ker\varphi\subseteq(x^2+1)$.

故 $\ker\varphi=(x^2+1)$.

由 $\varphi(\mathbb{Q}[x])=\{f(i)\mid f(x)\in\mathbb{Q}[x]\}=\mathbb{Q}[i]$.

由环的基本定理得 $\mathbb{Q}[x]/(x^2+1)\cong\mathbb{Q}[i]$

7: 证明：同习题 4.4.6 (2). 将 i 换成 $\sqrt{d}$ 即可

8: 证明：参考定理 3.6.3

9: $\mathbb{Z}/n\mathbb{Z}$ 的子环：$m\mathbb{Z}/n\mathbb{Z}$. $m\mid n$. 且 $m\leq n$

$\mathbb{Z}/n\mathbb{Z}$ 的理想：$m\mathbb{Z}/n\mathbb{Z}$. $m\mid n$. 且 $m\leq n$.

10: $\mathbb{Z}/18\mathbb{Z}$ 的所有理想：$m\mathbb{Z}/18\mathbb{Z}$, $m=1,2,3,6,9,18$.

$\mathbb{Z}/18\mathbb{Z}$ 的所有商环为：$(\mathbb{Z}/18\mathbb{Z})/(m\mathbb{Z}/18\mathbb{Z})$. $m=1,2,3,6,9,18$

4.5 素理想、极大理想

1. (1) R 为整环 $\Leftrightarrow ab=0 \Rightarrow a=0$ 或 $b=0$ ($\forall a,b\in R$)

$\Leftrightarrow \forall a,b\in R,\ ab\in(0) \Rightarrow a\in(0)$ 或 $b\in(0)$.

$\Leftrightarrow$ (0) 为素理想

$R\cong R/(0)$ 由定理 4.5.1 可得 (1),(2) 得证.

(2) R 为域 $\Leftrightarrow$ R 的理想为 (0) 或 R. $\Leftrightarrow$ (0) 是极大理想 □

2. 证明:

$\Rightarrow$ 若存在理想 P $(0)\subsetneq P\subseteq R$ 中.

由 R 是域, 故对 $\forall x\in P$. $x\cdot x^{-1}=1\in P$ 故 $P=R$

因此 R 仅有理想 R 和 (0).

$\Leftarrow$ 若 R 仅有两个理想 R 和 (0) 故 (0) 为 R 的极大理想

因为 $R\cong R/(0)$ 由定理 4.5.1 得: R 为域. □

3. (1) 证明:

$(x,2)=(x)+(2)=\{xf(x)+2g(x) \mid f(x),g(x)\in Z[x]\}$

因此, $(x,2)$ 是 $Z[x]$ 中常数项环为偶数的多项式组成的集合.

而 (x) 是其中所有常数项为 0 的多项式构成的集合

故显然 $(x)\subsetneq(x,2)\subsetneq Z[x]$. 故 (x) 不是 $Z[x]$ 的极大理想 □

(2). 设 I 是 $Z[x]$ 的极大理想, 且 $(x,2)\subsetneq I\subseteq Z[x]$, 则 $\exists f(x)\in I\setminus(x,2)$.

即 $f(x)$ 为 I 中常数项为奇数的多项式 设 $f(x)=g(x)+1$ 其中 $g(x)\in(x,2)\subsetneq I$.

故 $1=f(x)-g(x)\in I$, 因此 I 为单位理想 $I=Z[x]$.

故 $(x,2)$ 是 $Z[x]$ 的极大理想 □

4. 证明: 由习题 4.4.6.(1) $Q[x]/(x)\cong Q$ 故 $Q[x]/(x)$ 是域, 又 $Q[x]\neq(x)$.

于是 (x) 是 $Q[x]$ 的极大理想 亦是素理想 □

5. 证明: 由习题 2.3.1, 知 $Q[\sqrt{d}]$ 是域. 由习题 4.4.7 知 $Q[x]/(x^2-d)\cong Q[\sqrt{d}]$.

由定理 4.5.1 知 (x^2-d) 是 $Q[x]$ 的极大理想

~~直接证明: 若存在 J, $(x^2-d)\subsetneq J\subsetneq Q[x]$, ... 存在 ... 一定在 J 中, 且与 x^2-d 在 Q 中互质 ...~~

6. 由例 4.2.1 (2) $\mathbb{Z}/18\mathbb{Z}$ 的全部理想为 $\{d\mathbb{Z}/18\mathbb{Z} \mid d=1,2,3,6,9,18\}$

由第一同构定理 $(\mathbb{Z}/18\mathbb{Z})/(d\mathbb{Z}/18\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$.

由推论 2.2.2 和例 2.3.2，$\mathbb{Z}/d\mathbb{Z}$ 是整环和域 $\Leftrightarrow$ d 是素数.

故 $\mathbb{Z}/d\mathbb{Z}$ 的所有素理想与极大理想为 $\{2\mathbb{Z}/18\mathbb{Z}, 3\mathbb{Z}/18\mathbb{Z}\}$. □

7. 证明：设有限单位交换环为 R，I 为 R 的非单位素理想

R/I 是有限整环，由命题 2.3.1，R/I 是域，故 I 是 R 的极大理想. □

8. 证明：

(1). 由例 4.2.2(4) $R = \mathbb{Z}/p^n\mathbb{Z}$.

由例 2.2.7. $(\mathbb{Z}/p^n\mathbb{Z})^\times = \{\bar{i} \mid (i,p^n)=1, 0 \le i < p^n\} \xrightarrow{\text{限制映}} \{\bar{i} \mid p \nmid i, 0 \le i < p^n\}$

于是 R 中非可逆元构成的集合为 $R \setminus (\mathbb{Z}/p^n\mathbb{Z})^\times = \{\bar{i} \mid p \mid i, 0 \le i < p^n\}$

对于其中任一元素 $\bar{x}$，有 $p^n \mid x^n$，故 $(\bar{x})^n = \bar{0}$. 因此 R 的元素不是可逆元就是零因子. □

(2). 由例 4.2.1 (2) R 的所有理想为

$\{d\mathbb{Z}/p^n\mathbb{Z} \mid d$ 是 p^n 的正因数$\} = \{d\mathbb{Z}/p^n\mathbb{Z} \mid d = 1, p, p^2 \cdots p^n\}$

其中 $d\mathbb{Z}/p^n\mathbb{Z}$ 为素理想 $\Leftrightarrow$ $(\mathbb{Z}/p^n\mathbb{Z})/(d\mathbb{Z}/p^n\mathbb{Z})$ 是整环. 由同构定理知

$(\mathbb{Z}/p^n\mathbb{Z})/(d\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$

而由推论 2.2.2，$\mathbb{Z}/d\mathbb{Z}$ 是整环 $\Leftrightarrow$ d 是素数，故 R 只有一个素理想 $p\mathbb{Z}/p^n\mathbb{Z}$. □

(3)：由(2)，显然 R 的理想中除了 R 本身外，均包含于 P，故 P 也是 R 的极大理想.

又 R 是有单位交换环，因此商环 R/P 是域 □

9. 在习题 4.4.4 (3) 中，加入素理想与极大理想的条件 □