第三章　环

§3.1　基础知识 - 环与域

概要: 环; 整系数运算; 幺环的可逆元, 域, 可除代数; 单位元生成的子环, 特征.

3.1.1 定义. 设 R 是非空集合, 有两个运算, 一般记作加法 "$+$" 和乘法 "$\cdot$". 如果

(R1). $(R,+)$ 是一个交换群;

(R2). $(R,\cdot)$ 是一个半群 (即运算 "$\cdot$" 满足结合律);

(R3). 乘法对加法满足左、右分配律;

就称 $(R,+,\cdot)$ 是一个 环, 简称 R 是一个环.

如果环 R 满足:

(R4). $|R|>1$ 且 $(R,\cdot)$ 是一个幺半群, 即运算 "$\cdot$" 满足结合律以外还有 单位元, 一般记作 1_R, 或更简单地记作 1 ;

就称 $(R,+,\cdot)$ 是一个 幺环, 简称 R 是一个 幺环.

如果环 R 满足:

(R5). $(R,\cdot)$ 是一个交换半群, 即运算 "$\cdot$" 满足结合律以外还满足交换律;

就称 $(R,+,\cdot)$ 是一个 交换环, 简称 R 是一个 交换环.

对一般的环 R, 令 $Z(R)=\{\,z\in R\mid za=az,\ \forall\ a\in R\,\}$, 称为 R 的 中心.

显然, R 是交换环当且仅当 $Z(R)=R$.

例 1. $(\mathbb{Z},+,\cdot)$ 是交换幺环.

$(\mathbb{Z}_m,+,\cdot)$ 是交换幺环.

复多项式环 $\mathbb{C}[x]$ 是交换幺环.

例 2. $(\mathrm{M}_n(\mathbb{C}),+,\cdot)$ 在 $n>1$ 时是非交换幺环, 零矩阵 0 是零元, 单位矩阵 E 是单位元, 所以也记单位矩阵为 1. $Z(\mathrm{M}_n(\mathbb{C}))=\{\,c\cdot 1\mid c\in\mathbb{C}\,\}$, 这里 1 是单位矩阵.

设 R 是一个环. 如同第一章已使用的符号 (见 2.3.3), 对 $a \in R$ 和 $n \in \mathbb{Z}$:

$$na = \begin{cases} a + \cdots + a \ (n \text{ 个 } a \text{ 相加}), & \text{若 } n > 0; \\ 0, & \text{若 } n = 0; \\ (-a) + \cdots + (-a) \ (-n \text{ 个 } -a \text{ 相加}), & \text{若 } n < 0; \end{cases}$$

特别是, 按定义有 $(-1)a = -a$. "整系数" 运算满足

3.1.2

$$\begin{aligned} &(m+n)a = ma + na\,, \\ &m(na) = (mn)a\,, \\ &n(a+b) = na + nb\,, \\ &1a = a\,. \end{aligned}$$

在环 R 中定义减法 $a - b = a + (-b)$. 如同群论中已证明的: $-(-a) = a$.

命题. (1). $0a = 0 = a0$; (这里的 0 都是零元)

(2). $(-a)b = -ab = a(-b)$;

(3). $(-a)(-b) = ab$;

(4). $a(b-c) = ab - ac$; $(b-c)a = ba - ca$;

(5). $(ma)(nb) = (mn)(ab)$, $\quad \forall \ a, b \in R,\ m, n \in \mathbb{Z}$.

证. (1). $0a = (0+0)a = 0a + 0a$; 两边加上 $-0a$ 得: $0a = 0$.

(2). $(-a)b + ab = ((-a) + a)b = 0b = 0$; 所以 $(-a)b = -ab$.

(3). $(-a)(-b) = -a(-b) = -(-ab) = ab$.

(4). $a(b-c) = a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab - ac$.

(5). 对 m, n 为正整数, 为负整数, 一正一负分别予以证明. $\square$

又, 对 $a \in R$ 和正整数 n: $a^n = a \cdots a$ (n 个 a 相乘) ; "幂" 运算满足

3.1.3

$$\begin{aligned} &\text{对 } a \in R,\ m, n > 0 \text{ 有:} \quad && a^{m+n} = a^m a^n\,, \\ &&& (a^m)^n = a^{mn}\,, \\ &\text{在 } ab = ba \text{ 时还有:} && (ab)^n = a^n b^n\,. \\ &&& (a+b)^n = \sum_{k=0}^{n} \tbinom{n}{k} a^k b^{n-k} \end{aligned}$$

其中 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ 表示组合数.

定义. 幺环 R 的元素 a 称为 可逆元 如果存在 $a' \in R$ 使得 $aa' = 1 = a'a$; 此时 a' 称为 a 的 逆元, 记作 $a' = a^{-1}$. R 的所有可逆元的集合记作 $R^\times$.

3.1.4 命题. (1). 幺环 R 的单位元是唯一的, 记此唯一单位元为 1.

(2). 幺环 R 的元素 a 如果是可逆的, 则 a 的逆元是唯一的, 记此唯一逆元为 a^{-1}.

(3). 幺环 R 的所有可逆元的集合 $R^\times$ 在乘法运算下构成一个群, 称为环 R 的可逆元乘群. $\square$

当 R 是幺环时还定义： $a^0 = 1$. 当幺环 R 的元 a 可逆时，对负整数 n 定义 $a^n = a^{-1}\cdots a^{-1}$ ($-n$ 个 a^{-1} 相乘). 上面的幂运算公式 3.1.3 同样成立.

例 3. $\mathbb{Z}^\times = \{\pm 1\}$.

$\mathbb{Z}_m^\times$ 就是既约剩余类乘群.

$\mathbb{C}[x]^\times = \mathbb{C}^\times$.

$\mathrm{M}_n(\mathbb{C})^\times = \mathrm{GL}_n(\mathbb{C})$.

3.1.5 定义. (1). 如果幺环 $\mathbb{D}$ 的每个非零元都可逆，即 $\mathbb{D}^\times = \mathbb{D} - \{0\}$，则称 $\mathbb{D}$ 为**除环** .

(2). 交换的除环 $\mathbb{F}$ 称为**域** .

例 4. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是域.

$\{\, a + b\sqrt{2} \mid a, b \in \mathbb{Q} \,\}$ 是域.

3.1.6 例. 设 p 是素数. 则模 p 的剩余类环 $\mathbb{Z}_p$ 是域.

证. 设剩余类 $[a] \in \mathbb{Z}_p$, $[a] \neq [0]$; 则 $p \nmid a$, 那么存在整数 b, c 使得 $ab + pc = 1$; 于是 $ab = 1 - pc$, 即在剩余类环 $\mathbb{Z}_p$ 中有 $[ab] = [1]$, 就是 $[a][b] = [1]$. 故 $[a]$ 可逆. 所以 $\mathbb{Z}_p$ 是域. □

定义. 只含有限个元的域称为**有限域**.

注. 对一个域 $\mathbb{F}$, 几乎所有的线性代数一样做.

3.1.7 例. 对 $a \in \mathbb{C}$ 记 $\bar{a}$ 是共轭复数. 令

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; a, b \in \mathbb{C} \right\}$$

则在矩阵加法和矩阵乘法之下 $\mathbb{H}$ 是一个非交换除环.

证. 易验证 $\mathbb{H}$ 在矩阵加法和矩阵乘法之下是封闭的，从而易验证 $\mathbb{H}$ 构成一个环. 对任 $0 \neq A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, 有 $\det A = a\bar{a} + b\bar{b}$ 为非零实数，故

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \in \mathbb{H}\,;$$

因此 $\mathbb{H}$ 的每个非零元可逆; 所以 $\mathbb{H}$ 是一个除环. $\mathbb{H}$ 非交换，如 (其中 $\mathrm{i} = \sqrt{-1}$ 是虚数单位):

$$\begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}\,. \qquad \square$$

定义. 如果一个幺环 A 的中心包含实数域，那么用实数左乘就使得 A 成为实向量空间，这时也称 A 为一个**实代数**; A 作为实向量空间的维数也称为这个实代数的维数. 如果实代数 A 作为环是可除的，就称 A 是**实可除代数**.

注意：交换的实可除代数是域.

例 5. $\mathbb{R}$ 是实可除代数， $\dim_{\mathbb{R}} \mathbb{R} = 1$.

$\mathbb{C}$ 是实可除代数， $\dim_{\mathbb{R}} \mathbb{C} = 2$.

上述 $\mathbb{H}$ 是 4 维实可除代数，称为 *四元数代数*; 下述四个元素构成 $\mathbb{H}$ 的实向量空间基底：

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

与群类似，有子环概念.

定义. 设 R 是环.

(1). 如果非空子集 $S \subseteq R$ 在 R 的运算 "+" 和 "·" 也构成环，就称 S 是 R 的 *子环*.

(2). 如果 R 是幺环， S 是幺子环而且 S 的单位元与 R 的单位元一致，就称 S 是 *幺子环*. 如果幺子环构成域就称 *子域*.

例 6. (1) $2\mathbb{Z} = \{\, 2n \mid n \in \mathbb{Z} \,\}$ 是 $\mathbb{Z}$ 的子环但不是幺子环，因为 $2\mathbb{Z}$ 没有单位元.

(2) 设 $n > 1$, $R = \mathrm{M}_n(\mathbb{C})$, $e = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}$. 则

$$eRe = \left\{ \left. \begin{pmatrix} c & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} \right| \, c \in \mathbb{C} \right\}$$

是 R 的有单位元的子环，实际上易见 $eRe \cong \mathbb{C}$, 这也说明不是域的环可以有子域. 但 S 不是 R 的幺子环因为 S 的单位元 e 不等于 R 的单位元.

(3) $R = \mathrm{M}_n(\mathbb{C})$ 同上， $S = \{\, c \cdot 1 \mid c \in \mathbb{C} \,\}$ 其中 1 为恒等矩阵，即 S 是所有相似矩阵的集合；则 S 是 R 的幺子环，且是子域.

(4) 取 $R = \mathbb{Q}$, 是有理数域；令 $S = \{\, a/b \mid a, b \in \mathbb{Z},\ p \nmid b \,\}$, 则 S 为 R 的幺子环. 这个例子说明一个域可以有不是域的子环.

命题. *设 R 是环， $\emptyset \neq S \subseteq R$.*

(1). *S 是子环当且仅当对任 $a, b \in S$ 有 $a - b \in S$ 和 $ab \in S$.*

(2). *S 是子环当且仅当 $1 \in S$ 且对任 $a, b \in S$ 有 $a - b \in S$ 和 $ab \in S$.* □

由此易验证：

命题. *设 R 是环.*

(1). *如果 S_i, $i \in I$, 都是 R 的子环，则 $\bigcap\limits_{i \in I} S_i$ 是 R 的子环.*

(2). *如果 S_i, $i \in I$, 都是 R 的幺子环，则 $\bigcap\limits_{i \in I} S_i$ 是 R 的幺子环.* □

定义. (1). 设 R 是环, $T \subseteq R$ 为子集; 令 Σ 是 R 中所有包含 T 的子环的集合. 则称 $\bigcap\limits_{S\in\Sigma} S$ 为由子集 T 生成的子环.

(2). 设 R 是幺环, $T \subseteq R$ 为子集; 令 Σ 是 R 中所有包含 T 的幺子环的集合. 则称 $\bigcap\limits_{S\in\Sigma} S$ 为由子集 T 生成的幺子环.

注. 按定义, 环 R 的子集 T 生成的子环就是 R 中包含 T 的最小子环. 子集 T 生成的幺子环就是 R 中包含 T 的最小幺子环.

例. 取 $R = \mathbb{C}[\lambda], T = \{\, x^2 \,\}$.

(1). T 生成的子环为 $\{\, \sum_{i=1}^{k} a_i x^{2i} \mid k > 0, a_i \in \mathbb{Z} \,\} \bigcup \{0\}$.

(2). T 生成的幺子环为 $\{\, c + \sum_{i=1}^{k} a_i x^{2i} \mid c \in \mathbb{Z},\ k > 0,\ a_i \in \mathbb{Z} \,\}$.

例. 环 R 的中心 $Z(R)$ 是子环. 一般地, 如果子环 $S \subseteq Z(R)$, 则称 S 是 R 的 **中心子环**.

3.1.8 命题. *设 R 是幺环. 则单位元 1_R 生成的子环为 $\mathbb{Z}1_R := \{\, n\,1_R \mid n \in \mathbb{Z} \,\}$ 是单位元 1_R 的所有整系数倍的集合, 它是 R 的中心幺子环, 且下列之一成立:*

(1). 存在正整数 h 使得 $h\,1_R = 0$ 但 $k\,1_R \neq 0$ 对任 $0 < k < h$, 此时 $\mathbb{Z}1_R = \{\, 0,\ 1_R,\ 2\,1_R,\ \cdots,\ (h-1)\,1_R \,\}$, 括号中恰是 $\mathbb{Z}1_R$ 的全部互不相等的元.

(2). 任何正整数 k 使 $k\,1_R \neq 0$ (从而只有 $0\,1_R = 0$), 此时 $\mathbb{Z}1_R = \{\cdots,\ (-2)\,1_R,\ (-1)\,1_R,\ 0,\ 1_R,\ 2\,1_R,\ \cdots\}$, 括号中恰是 $\mathbb{Z}1_R$ 的全部互不相等的元.

证. $1_R = 1\,1_R \in \mathbb{Z}1_R$; 特别, $\mathbb{Z}1_R \neq \emptyset$. 对任 $n\,1_R, n'\,1_R \in \mathbb{Z}1_R$, 其中 $n, n' \in \mathbb{Z}$, 有

$$\begin{aligned} n\,1_R - n'\,1_R &= (n-n')\,1_R \in \mathbb{Z}1_R\,; \\ (n\,1_R)(n'\,1_R) &= (nn')\,1_R \in \mathbb{Z}1_R\,. \end{aligned}$$

所以 $\mathbb{Z}1_R$ 是子环, 且它包含 1_R. 为证明 $\mathbb{Z}1_R$ 是由 1_R 生成的子环, 只需证明: 只要子环 S 包含 1_R 就一定包含 $\mathbb{Z}1_R$; 这是因为: 如果 $1_R \in S$, 则对任整数 n, $n \cdot 1_R$ 都有 $n\,1_R \in S$.

在只考虑加群 $(R, +)$ 时, 或者 1_R 是有限阶元, 设 1_R 的阶为 h, 那么 (1) 成立; 或者 1_R 是无限阶元, 此时 (2) 成立. □

3.1.9 定义. 设 R 是幺环. 如果上命题的 (1) 成立就称幺环 R 的 **特征** 是 h, 记作 $\mathrm{char}R = h$. 否则上命题的 (2) 成立, 就称幺环 R 的 **特征** 是 0, 记作 $\mathrm{char}R = 0$.

例. $\mathrm{char}\,\mathbb{Z} = 0$.

$\mathrm{char}\,\mathbb{Z}_m = m$.

$\mathrm{char}\,\mathbb{Q} = 0$.

习题 3.1

1. 设 R 是环. 证明:

(1). 中心 $Z(R)$ 是交换子环.

(2). 如果 R 是除环, 则中心 $Z(R)$ 是域.

2. 环 R 的元素 a 称为 **幂零元** *(nilpotent element)* 如果存在正整数 n 使得 $a^n = 0$. 证明交换环的幂零元之和仍为幂零元. 这结论对非交换环对码?

3. 环 R 的元素 a 称为 **幂等元** *(idempotent)* 如果 $a^2 = a$. 如果 R 的所有元都是幂等元, 就称 R 是 **布尔环** *(Boolean ring)*. 证明: 布尔环恒是交换环, 而且所有元满足 $2a = 0$.

4. 下面哪些环是域, 哪些环不是域, 并说明理由:

(1). $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, 数的加法和数的乘法.

(2). $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, 数的加法和数的乘法.

(3). 模 m 剩余类换 $\mathbb{Z}_m$, 其中 m 是正整数但不是素数.

(4). 复多项式环 $\mathbb{C}[x] := \{ f(x) \mid f(x)$ 是复多项式$\}$.

(5). 复分式环 $\mathbb{C}(x) := \{ f(x)/g(x) \mid f(x), g(x) \in \mathbb{C}[x],\ g(x) \neq 0 \}$.

5. 设幺环 R 的特征是 $h > 0$. 证明: 对任 $a \in R$ 有 $h\,a = 0$. 举例说明: 可以存在 $0 \neq a \in R$ 和 $0 < k < h$ 使得 $k\,a = 0$.

§3.2 基础知识 - 同态与理想

概要: 环同态; 理想; 主理想整环; 商环与同态基本定理; 整环的特征; 极大理想与素理想.

环论中与群的正规子群相应的概念是 **理想**, 它与环的同态相联系.

环同态

3.2.1 定义. 设 R, R' 是环.

(1). 如果映射 $f : R \to R'$ 满足

$$f(a + b) = f(a) + f(b)\ , \quad \forall\ a, b \in R\ ;$$
$$f(ab) = f(a)f(b)\ , \qquad \forall\ a, b \in R\ ;$$

则称 f **为环的同态**.

(2). 单射的 (满射的, 双射的) 环同态 f 称为 **单同态**(**满同态**, **同构**).

如果 $f : R \to R'$ 是同构, 则称环 R 与环 R' 同构, 记作 $R \cong R'$.

(3) 如果 R, R' 都是幺环而且同态 f 还满足: $f(1_R) = 1_{R'}$, 则称 f 是 **幺同态**.

注意, 环同态 f 满足的第一个条件说: f 是从加群 $(R, +)$ 到加群 $(R', +)$ 的群同态. 所以 f 具备加群同态的一切性质, 如 $f(na) = nf(a)$; $f(a - b) = f(a) - f(b)$ 等.

例 1. (1). $\mathbb{Z} \to \mathbb{Z}_m$, $z \mapsto [z]$, 是满的环同态.

(2). $\mathbb{C} \to \mathrm{M}_n(\mathbb{C})$, $c \mapsto cI$, 是单的环同态.

(3). 设 V 是 n 维实向量空间， $\mathrm{End}(V)$ 是所有线性变换的集合，在线性变换加法和乘法之下是环. 取 V 的基底，则任一线性变换 $\alpha \in \mathrm{End}(V)$ 对应唯一矩阵 $A_\alpha \in \mathrm{M}_n()\mathbb{R})$. 那么 $\mathrm{End}(V) \longrightarrow \mathrm{M}_n()\mathbb{R})$, $\alpha \longmapsto A_\alpha$, 是环同构.

命题. 设 $f : R \to R'$ 是环同态.

(1). 同态像 $\mathrm{Im}(f) = \{\, r' \in R' \mid$ 存在 $r \in R$ 使得 $f(r) = r' \,\}$ 是 R' 的子环； σ 是满同态当且仅当 $\mathrm{Im}(\sigma) = R'$.

(2). 同态核 $K = \mathrm{Ker}(f) = \{\, r \in R \mid f(r) = 0 \,\}$ 满足两条：

(I1). $(K, +)$ 是 $(R, +)$ 的子群；

(I2). 对任 $a \in K$ 和 $r \in R$ 有 $ra \in K$ 和 $ar \in K$;

σ 是单同态当且仅当 $\mathrm{Ker}(\sigma) = 0$.

证. (1). 略.

(2). 对任 $a, b \in K$, $f(a-b) = f(a) - f(b) = 0 - 0 = 0$, 所以 $a - b \in K$; 即 $(K, +)$ 是 $(R, +)$ 的子群. 此即 (i). 又对 $a \in K$ 和 $r \in R$, $f(ra) = f(r)f(a) = f(r)0 = 0$, 即 $ra \in K$; 同理 $ar \in K$.

因为环同态首先是加群同态, 由群论已证明的结论，σ 是单同态当且仅当 $\mathrm{Ker}(\sigma) = 0$. □

理想

3.2.2 定义. 环 R 的非空子集 I 如果满足以下两条就称为 R 的一个 理想:

(I1). $(I, +)$ 是 $(R, +)$ 的子群;

(I2). 对任 $a \in I$ 和 $r \in R$ 有 $ra \in I$ 和 $ar \in I$.

所以环同态 $f : R \to R'$ 的同态核 $\mathrm{Ker}(f)$ 是 R 的理想. 一个环 R 至少有两个理想: 0 和 R, 分别称为 零理想 和 单位理想; 这两个都称为平凡理想.

例 2. (1). $f : \mathbb{Z} \to \mathbb{Z}_m$, $a \mapsto [a]$, 是环同态. $\mathrm{Ker}(f) = m\mathbb{Z}$.

(2). $\mathbb{C}[x]$ 是所有复多项式构成的幺环. 给定 $c_0 \in \mathbb{C}$. 则 $\nu_{c_0} : \mathbb{C}[x] \to \mathbb{C}$, $f(x) \mapsto f(c_0)$, 是环同态，同态核

$$\mathrm{Ker}(\nu_{c_0}) = \mathbb{C}[x](x - c_0) := \{\, g(x)(x - c_0) \mid g(x) \in \mathbb{C}[x] \,\}$$

(3). 设 V 是 n 维复向量空间, $\mathrm{End}(V)$ 是所有线性变换构成的幺环. 取定 $\alpha \in \mathrm{End}(V)$. 则 $\nu_\alpha : \mathbb{C}[x] \to \mathrm{End}(V)$, $f(x) \mapsto f(\alpha)$, 是环同态，同态核恰是 α 的所有零化多项式的集合，所以构成 $\mathbb{C}[x]$ 的理想，称为 α 的 零化理想.

命题. 设 R 是环， $\emptyset \neq I \subseteq R$. 则 I 是理想当且仅当以下两条成立：

(i). 对任 $a, b \in I$ 有 $a - b \in I$.

(ii). 对任 $a \in I$ 和 $r \in R$ 有 $ra \in I$ 和 $ar \in I$. □

那么容易验证:

命题. 设 I, J, K 是环 R 的理想.

(1) $I + J := \{ a + b \mid a \in I,\ b \in J \}$ 是 R 的理想, 称为理想 I 与 J 的和; 且 $(I + J) + K = I + (J + K)$.

(2) $IJ := \{ \sum_{k=1}^{\ell} a_k b_k \mid a_k \in I,\ b_k \in J,\ \ell \in \mathbb{Z}^+ \}$ 是 R 的理想, 称为理想 I 与 J 的积; 且 $(IJ)K = I(JK)$.

(3) $I(J + K) = IJ + IK$; $(J + K)I = JI + KI$.

证. 练习 □

特别地, 若 I 是环 R 的理想, 则 $I^2 = II$, I^3, $\cdots$, 都是 R 的理想. 如果存在 $n \in \mathbb{Z}^+$ 使得 $I^n = 0$ 就称 I 为 R 的 幂零理想.

例 3. $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{C} \right\}$ 是一个幺环, $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \;\middle|\; b \in \mathbb{C} \right\}$ 是 R 的一个幂零理想, 因为 $I^2 = 0$.

命题. 设 R 是环, I_j, $j \in J$, 都是 R 的理想; 则 $\bigcap\limits_{j \in J} I_j$ 是 R 的理想.

证. 练习. □

定义. (1) 设 R 是环, $T \subseteq R$ 为子集; 令 Σ 是 R 中所有包含 T 的理想的集合. 则称 $\bigcap\limits_{I \in \Sigma} I$ 为由子集 T 生成的理想, 记作 $\langle T \rangle$.

(2) 由一个元 $a \in R$ 生成的理想称为 R 的 主理想.

(3) 如果环 R 的任何理想是主理想, 则称 R 为 主理想环.

有单位元的交换环 R 的主理想比较容易表达, $a \in R$ 生成的理想是

$$Ra = \{ ra \mid r \in R \} .$$

主理想整环与欧氏环整环

有一类重要的主理想环, 与下述概念有关.

3.2.3 定义. 设 R 是环.

(1). $0 \neq a \in R$ 称为 左零因子 如果存在 $0 \neq b \in R$ 使得 $ab = 0$. 显然, 此时 b 是 右零因子. 如果 R 是交换环, 零因子就没有左右之分.

(2). 交换的无零因子的有单位元的环称为 整环 (*domain* 或 *integral domain*).

(3). 交换的无零因子的有单位元的主理想环称为 主理想整环 (*principal ideal domain*, 简写为 *p.i.d.*).

3.2.4 定义. 整环 R 称为 欧氏整环 如果有非负整函数 $\delta : R - \{0\} \to \mathbb{Z}^+$ 满足:

(E1). 对任 $a, b \in R - \{0\}$ 有: $\delta(a) \leq \delta(ab)$;

(E2). 对任 $a, b \in R$ 其 $b \neq 0$, 存在 $q, r \in R$ 使得: $a = bq + r$, $r = 0$ 或 $\delta(r) < \delta(b)$.

3.2.5 命题. 欧氏整环是主理想整环.

证. 设 R 是欧氏整环. 设 I 是 R 的理想. 如果 $I=0$, 则 $I=R0$ 为主理想. 再设 $I\neq 0$. 取 $a\in I-\{0\}$ 使得 $\delta(a)$ 最小. 首先, 由理想的定义马上有 $Ra\subseteq I$. 反过来, 对任 $b\in I$, 因 $a\neq 0$, 存在 $q,r\in R$ 使得

$$b=aq+r\ ,\qquad r=0\ \text{ 或 }\delta(r)<\delta(a)\ ;$$

如果 $r\neq 0$, 则 $\delta(r)<\delta(a)$, 且 $r=b-aq\in I$, $\delta(r)<\delta(a)$, 这与 a 是 $I-\{0\}$ 中使得 $\delta(a)$ 最小的元相矛盾. 所以 $r=0$, 从而 $b=aq\in Ra$. 故 $I=Ra$ 是主理想. □

下面是重要例子.

例 4. (1). $\mathbb{Z}$ 是欧氏整环从而是主理想整环, $\delta(z)=|z|$; .

(2). 一元复多项式环 $\mathbb{C}[x]$ 从而是欧氏整环是主理想整环, $\delta(f(x))=\deg f(x)$.

(3). $\mathbb{Z}[\mathrm{i}]=\{\,a+b\mathrm{i}\mid a,b\in\mathbb{Z}\,\}$ 是欧氏整环, $\delta(a+b\mathrm{i})=a^2+b^2$. (习题 5.)

例 5. 设 $\mathrm{End}(V)$ 是复向量空间 V 的所有线性变换构成的幺环. 取定 $\alpha\in\mathrm{End}(V)$. 则幺环同态

$$\nu_\alpha:\quad \mathbb{C}[x]\longrightarrow \mathrm{End}(V)\ ,\quad f(x)\longmapsto f(\alpha)\ ,$$

的同态核是 α 的所有零化多项式构成的 $\mathbb{C}[x]$ 的理想 (即 α 的零化理想), 由一个元素 $m(x)$ 生成, 它是 α 的零化理想中次数最小的非零多项式, 就是 α 的 *极小多项式*.

3.2.6 例. 一元有理多项式环 $\mathbb{Q}[x]$ 是欧氏整环, 从而是主理想整环. 任取 $\alpha\in\mathbb{C}$, 有 *赋值映射*:

$$\nu_\alpha:\quad \mathbb{Q}[x]\longrightarrow \mathbb{C}\ ,\quad f(x)\longmapsto f(\alpha)\ ;$$

易验证赋值映射 ν_α 是幺环同态, 同态核 $\mathrm{Ker}(\nu_\alpha)$ 称为 α 的零化理想, 其中的多项式称为 α 在有理数域 $\mathbb{Q}$ 上的 *零化多项式*. 有两种情形.

- $\mathrm{Ker}(\nu_\alpha)\neq 0$, 即有非零有理多项式 $f(x)$ 零化 α: $f(\alpha)=0$; 此时称 α 是有理数域 $\mathbb{Q}$ 上的 *代数元* (数论中称 *代数数*), $\mathrm{Ker}(\nu_\alpha)$ 中的次数最低的非零多项式 $g(x)$ 可以生成该零化理想: $\mathrm{Ker}(\nu_\alpha)=\mathbb{Q}[x]\cdot g(x)$; $g(x)$ 称为 α 在 $\mathbb{Q}$ 上的 *极小多项式*.
- 另一种情形, $\mathrm{Ker}(\nu_\alpha)=0$, 即任何非零有理多项式 $f(x)$ 不零化 α; 此时称 α 是有理数域 $\mathbb{Q}$ 上的 *超越元*(数论中称 *超越数*).

例. $\sqrt{2}$, $\mathrm{i}=\sqrt{-1}$ 都是有理数域 $\mathbb{Q}$ 上的代数元, 因为有理多项式 x^2-2 零化 $\sqrt{2}$, 有理多项式 x^2+1 零化 i.

圆周率 π, 自然对数的底数 e, 都是有理数域 $\mathbb{Q}$ 上的超越元; 但是证明非常不简单.

商环, 同态基本定理

以下的构造和定理都与群论情形类似.

设 R 是环, I 是 R 的理想. 对 $a,b\in R$, 如果 $a-b\in I$ 就称 a 模 I 同余于 b, 记作 $a\equiv b\pmod I$. 那么 $\equiv\pmod{\ }$ 是 R 上的等价关系, 元素 a 所在的等价类为 I 作为

$(R,+)$ 的子群的陪集 $a+I=\{\,a+h\mid h\in I\,\}$. 商集记作 R/I. 在商集 R/I 上定义运算

$$(a+I)+(b+I)=(a+b)+I\ ,\qquad (a+I)(b+I)=(ab)+I\ ;$$

则易验证它们是合理定义的 (与代表元选取无关的) 运算, 使得 R/I 构成环, 称为 R 模理想 I 的 **商环**(或称 **剩余环**). 而且 **商映射**(或称 **剩余映射**)

$$\rho:\quad R\longrightarrow R/I\ ,\quad a\longmapsto a+I\ ,$$

是环的满同态, 称为 **自然同态**, 其同态核是 I. 表示为正合序列:

$$0\ \longrightarrow\ I\ \longrightarrow\ R\ \longrightarrow\ R/I\ \longrightarrow\ 0\ .$$

3.2.7 环同态基本定理. 设 $f:R\to R'$ 是从环 R 到环 R' 的同态, 记同态核 $K=\mathrm{Ker}(f)$. 则存在唯一环同态 $\bar f:R/K\to R'$ 使得 $f=\bar f\cdot\rho$, 其中 $\rho:R\to R/I$ 是自然同态. 而且, $\bar f$ 恒为单同态; $\bar f$ 是同构当且仅当 f 是满同态. □

$$\begin{array}{ccc} R & \longrightarrow^{f} & R' \\ {\scriptstyle\rho}\big\downarrow & \nearrow_{\bar f} & \\ R/I & & \end{array}$$

引理. 设 $f:R\to R'$ 是环同态.

(1). 如果 I' 是 R' 的理想则 $f^{-1}(I')$ 是 R 的理想.

(2). 如果 f 是满同态, I 是 R 的理想, 则 $f(I)$ 是 R' 的理想. □

注. 如果环同态 $f:R\to R'$ 不是满同态, 则理想的像不一定是理想. 例如

$$f:\quad \mathbb{Q}\longrightarrow\mathbb{Q}[x]\,,\quad q\longmapsto q\,,$$

是环同态, 但单位理想 $\mathbb{Q}$ 的像是 $\mathbb{Q}[x]$ 中常数多项式的集合, 不是 $\mathbb{Q}[x]$ 的理想.

3.2.8 理想对应定理. 设 $f:R\to R'$ 是从环 R 到环 R' 的满同态, 记 $K:=\mathrm{Ker}(f)$. 令 $L(R')=\{\,I'\mid I'\text{是 }R'\text{ 的理想}\,\}$, 令 $L(R,K)=\{\,I\mid I\text{ 是 }R\text{ 的理想且 }I\supseteq K\,\}$. 则映射

$$f^*:\quad L(R,K)\longrightarrow L(R'),\quad I\longmapsto f(I)$$

是双射; 而且对 $I,J\in L(R,K)$ 有

(1). $I\subseteq J$ 当且仅当 $f(I)\subseteq f(J)$;

(2). $f_I:\ R/I\cong R'/f(I),\ \ a+I\ \mapsto\ f(a)+f(I)$.

证. 由上述引理, 对 $I\in L(R,K)$ 有 $f(I)\in L(R')$, 即 f^* 定义合理. 对 $I'\in L(R')$, 从子群对应定理 (同态 f 的核首先是加群同态的核) 知道 $f^{-1}(I')\supseteq K$, 而且, 仍由上述引理, $f^{-1}(I')$ 是 R 的理想. 所以有合理定义的映射:

$$g^*:\quad L(R')\longrightarrow L(R,K),\quad I'\longrightarrow f^{-1}(I')\ .$$

由子群对应定理已知， g^* 与 f^* 互逆，故 f^* 是双射.

结论 (1) 可以直接从子群对应定理得出.

(2). 子群对应定理已指出，映射 f_I 是加群同构；对 $a+I, b+I \in R/I$ 有：

$$\begin{aligned} f_I\Big((a+I)(b+I)\Big) &= f_I\Big((ab)+I\Big) = f(ab)+f(I) = f(a)f(b)+f(I) \\ &= \Big(f(a)+f(I)\Big)\Big(f(b)+f(I)\Big) = f_I(a+I)f_I(b+I)\ . \end{aligned}$$

所以 f_I 是环同构. □

同样地，还有子环对应定理.

极大理想，素理想

3.2.9 定义. (1). 环 R 的理想 I 称为 *极大理想* 如果 $I \neq R$ 而且对 R 的任何理想 J 只要 $I \subseteq J \subseteq R$ 那么或者 $I = J$ 或者 $J = R$ (也就是说在理想 I 与 R 之间只有两个理想 I, R).

(2). 称交换幺环 R 的理想 I 是 *素理想*, 如果 $I \neq R$ 而且对任 $a, b \in R$ 只要 $ab \in I$ 那么或者 $a \in I$ 或者 $b \in I$ (也就是说差集 $R - I$ 是对乘法封闭的).

引理. *交换幺环 R 是域当且仅当 R 只有两个平凡理想.*

证. 设 R 是域. 如果 I 是 $\bar{R}$ 的非零理想, 则任取 $0 \neq \bar{a} \in I$, 那么 $1 = \bar{a}^{-1}\bar{a} \in I$, 从而对任何 $\bar{r} \in \bar{R}$ 有 $\bar{r} = \bar{r}1 \in I$; 即 $I = R$.

设 R 只有两个平凡理想. 设 $0 \neq a \in R$; 则 Ra 是 R 的非零理想, 故 $Ra = R$; 那么 $1 \in R = Ra$, 所以有 $a' \in R$ 使得 $a'a = 1$. 即 a 是可逆元. □

3.2.10 命题. *设 I 是交环幺环 R 的理想.*

(1). *商环 R/I 是整环 当且仅当 I 是素理想.*

(2). *商环 R/I 是域 当且仅当 I 是 R 的极大理想.*

证. (1). R/I 是整环 当且仅当 只要 $(a+I)(b+I) = I$ 那么 $a+I = I$ 或者 $b+I = I$, 由于 $(a+I)(b+I) = ab+I$, 所以这等价于说：只要 $ab \in I$ 那么 a, b 中至少一个在 I 中.

(2). 商环 R/I 是域, 当且仅当 R/I 只有平凡理想, 由理想对应定理, 当且仅当在 I 与 R 之间只有两个理想： I 与 R, 即, 当且仅当 I 是极大理想. □

推论. *交换幺环的极大理想是素理想.* □

整环的特征

设 R 是幺环. 那么中心 $Z(R)$ 是幺子环. 易验证：下述映射

$$\zeta: \quad \mathbb{Z} \longrightarrow Z(R)\ , \quad n \longmapsto n\,1_R\ ;$$

是环同态. 与命题 3.1.8 对照, 知道 $\mathrm{Im}(\zeta) = \mathbb{Z}1_R$. 另一方面, 因为 $\mathbb{Z}$ 是主理想整环, $\mathrm{Ker}(\zeta) = \mathbb{Z}h$ 由一个元生成, 可设生成元 $h \in \mathbb{Z}^+$. 由同态基本定理,

$$\mathbb{Z}/\mathbb{Z}h \cong \mathrm{Im}(\zeta) = \mathbb{Z}1_R \ .$$

这里 h 就是 3.1.9 定义的幺 R 的 特征 $h = \mathrm{char}\, R$.

3.2.11 命题. *设 R 是整环, 记 $\mathrm{char}\, R = h$. 则或者 $h = 0$ 或者 $h = p$ 是个素数, 且:*

(1) 如果 $h = p$ 为素数, 则 R 的任何非零元 a 在加群 $(R, +)$ 的阶等于 p, 而且 R 的子环 $\mathbb{Z}1_R$ 同构于 $\mathbb{Z}_p$.

(2) 如果 $h = 0$, 则 R 的任何非零元 a 在加群 $(R, +)$ 的阶等于 ∞, 而且 R 的子环 $\mathbb{Z}1_R$ 同构于 $\mathbb{Z}$.

证. 设 $h \neq 0$ 且 h 不是素数, 则 $h = h_1h_2$ 且 $h_1 < h$, $h_2 < h$, 由特征的定义, $0 = h \cdot 1 = (h_1h_2) \cdot (11) = (h_1 \cdot 1)(h_2 \cdot 1)$; 但 R 是整环, 故: 或者 $(h_1 \cdot 1) = 0$, 或者 $(h_2 \cdot 1) = 0$; 都与 $\mathrm{char}\, R = h$ 相矛盾.

(1). 由于 $pa = 0$, 故 a 的阶整除 p 从而只能是 p. 由于 $\mathrm{char}\, R = p$, 由同态基本定理, 同态 $\zeta : \mathbb{Z} \to R$ 诱导单同态 $\mathbb{Z}/p\mathbb{Z} \to R$; 即 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}\,1_R$.

(2). 类似于 (1). □

域是特殊的整环. 域的特征有进一步性质.

3.2.12 命题. *(1) 域 $\mathbb{F}$ 的特征或者为 0 或者为素数 p.*

(2) 如果域 $\mathbb{F}$ 的特征为素数 p, 则 $\mathbb{F}$ 包含一个子域同构于 $\mathbb{Z}_p$.

(3) 如果域 $\mathbb{F}$ 的特征为 0, 则 $\mathbb{F}$ 包含一个子域同构于 $\mathbb{Q}$.

证. (1), (2) 已包含在在上面的命题中.

(3). 由于 $\mathrm{char}\, \mathbb{F} = 0$, 故 $\mathbb{Z} \to \mathbb{F}$, $n \mapsto n \cdot 1_{\mathbb{F}}$, 是单同态; 通过它可认为 $\mathbb{Z} \subseteq \mathbb{F}$ (即把 $n \cdot 1_{\mathbb{F}}$ 看作整数 n). 由于 $\mathbb{F}$ 是域, 对任 $0 \neq n \in \mathbb{Z}$, 在 $\mathbb{F}$ 中 n 可逆: $n^{-1} \in \mathbb{F}$. 易验证:

$$\mathbb{Q} \ \longrightarrow \ \mathbb{F} \ , \quad \frac{m}{n} \ \longmapsto \ mn^{-1} \ ,$$

是从 $\mathbb{Q}$ 到 $\mathbb{F}$ 的幺同态从而是单同态 (因为域 $\mathbb{Q}$ 只有平凡理想所以同态核只能是零理想), 同态象是 $\{\, mn^{-1} \mid m, n \in \mathbb{Z},\ n \neq 0 \,\} \subseteq \mathbb{F}$. 所以 $\mathbb{F}$ 的子集 $\{\, mn^{-1} \mid m, n \in \mathbb{Z},\ n \neq 0 \,\}$ 是一个与 $\mathbb{Q}$ 同构的子域. □

习题 3.2

1. 设 R 是没有单位元的环. 令 $S = \{\, (r, z) \mid r \in R,\ z \in \mathbb{Z} \,\}$, 定义运算:

$$(r,\, z) + (r',\, z') = (r + r',\ z + z') \ ;$$

$$(r,\, z) \cdot (r',\, z') = (rr' + zr' + z'r,\ zz') \ ;$$

证明 S 是幺环，而 $R \longrightarrow S,\ r \longmapsto (r,0)$ 是单同态.

2. 证明：除环只有平凡理想.

3. 证明： $\mathrm{M}_n(\mathbb{R})$ 只有平凡理想.

4. 设 I, J 是环 R 的理想，证明： $IJ \subseteq I \cap J$. 举例说明等号不必成立.

5. 证明： $\mathbb{Z}[\mathrm{i}]$ 是欧氏整环.

6. 如果 $\alpha \in \mathbb{C}$ 是 $\mathbb{Q}$ 上的代数元，则 α 的极小多项式是不可约多项式.

7*. 证明 $\mathbb{C}$ 中所有代数数的集合是可数集；特别，超越数存在 (而且比代数数 "多出很多").

8. 叙述并证明子环对应定理.

9. 设幺环 R 的特征 $\operatorname{char} R = h$. 证明： $ha = 0,\ \forall a \in R$.

10. 设 R 是交换幺环，设特征 $\operatorname{char} R = p$ 是个素数. 证明：对任 $a, b \in R$ 和任正整数 n 有 $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

11. 令 $p \in \mathbb{Z}$ 是素数，那么 $\mathbb{Z}p$ 是 $\mathbb{Z}$ 的素理想，也是极大理想.

12. 记 $\mathbb{Z}[x]$ 是所有整系数多项式构成的环. 证明：一个元素 x 生成的循环理想 $\mathbb{Z}[x]x = \{$常数项为 0 的多项式$\} \cup \{0\}$; 并证明它是素理想但不是极大理想.

13. 令 $C[0,1]$ 是定义在闭区间 $[0,1]$ 上的所有连续实函数的集合；定义运算：对任 $f, g \in C[0,1]$,

$$(f+g)(x) = f(x) + g(x)\ , \qquad \forall\ x \in [0,1]\ ;$$

$$(f \cdot g)(x) = f(x)g(x)\ , \qquad \forall\ x \in [0,1]\ .$$

(1). 在上述运算下 $C[0,1]$ 是交换环，但 $C[0,1]$ 不是整环.

(2). 设 $r \in [0,1]$. 则 $\nu_r :\ C[0,1] \to \mathbb{R},\ f \mapsto f(r)$, 是环的满同态；求同态核 $\operatorname{Ker}(\nu_r)$.

(3). 证明： $\operatorname{Ker}(\nu_r)$ 不是 $C[0,1]$ 的主理想.

§3.3 直和

概要: 直和；外直和；直和的可逆元；中国剩余定理；数论中的中国剩余定理.

环的直和

3.3.1 定义. 设 R 是环. 如果理想 $I_1, \cdots, I_k$ 使得：

(1) $R = I_1 + \cdots + I_n$, 即对任 $r \in R$ 存在 $r_j \in I_j,\ j = 1, \cdots, n$, 使得 $a = a_1 + \cdots + a_n$;

(2) 对任 $a \in R$, 如果 $a_j, a'_j \in I_j,\ j = 1, \cdots, n$, 使得 $a = a_1 + \cdots + a_n = a'_1 + \cdots + a'_n$, 则 $a_j = a'_j,\ j = 1, \cdots, n$;

就称环 R 是理想 $I_1, \cdots, I_n$ 的 直和, 记作 $R = I_1 \oplus \cdots \oplus I_n$.

3.3.2 命题. 设幺环 R 是理想 $I_1, \cdots, I_n$ 的直和，设 $1 = e_1 + \cdots + e_n$ 其中 $e_j \in I_j$. 则

(1). $e_j^2 = e_j$, $j = 1, \cdots, n$;

(2). $e_i e_j = 0$, $1 \le i \ne j \le n$;

而且对任 $j = 1, \cdots, n$ 有： $e_j \in Z(R)$, 而 $I_j = Re_j$ 它是一个以 e_j 为单位元的环.

证. 一方面 $e_j = 1e_j = (e_1 + \cdots + e_n)e_j$, 即

$$e_j = e_1e_j + \cdots + e_{j-1}e_j + e_j^2 + e_{j+1}e_j + \cdots + e_ne_j \ ;$$

其中 $e_ie_j \in I_i$; 而

$$e_j = 0 + \cdots + 0 + e_j + 0 + \cdots + 0 \ ;$$

由于直和表写的唯一性 (3.3.1) 之 (2), 得本命题 (1), (2) 两条成立.

又对任 $a \in R$, 有

$$\begin{aligned} ae_1 + \cdots + ae_n &= a(e_1 + \cdots + e_n) = a1 = 1a \\ &= (e_1 + \cdots + e_n)a = e_1a + \cdots + e_na \end{aligned}$$

但 $ae_i, e_ia \in I_i$; 仍由直和表写的唯一性，得 $ae_j = e_ja$; 即 $e_j \in Z(R)$.

最后，按理想的定义， $Re_j \subseteq I_j$; 反之，对任 $a_j \in I_j$ 有

$$\begin{aligned} a_j &= a_je_1 + \cdots + a_je_{j-1} + a_je_j + a_je_{j+1} + \cdots + +a_je_n \\ &= 0 + \cdots + 0 + a_j + 0 + \cdots + 0 \end{aligned}$$

还是由直和表写的唯一性知：当 $i \ne j$ 时 $a_je_i = 0$, 而 $a_j = a_je_j \in Re_j$. □

推论. 记号如上. 如果 $a = a_1 + \cdots + a_n$, $b = b_1 + \cdots + b_n$, 其中各 $a_j, b_j \in I_j$; 则

$$(a_1 + \cdots + a_n) + (b_1 + \cdots + b_n) = (a_1 + b_1) + \cdots + (a_n + b_n) \ ;$$

$$(a_1 + \cdots + a_n)\,(b_1 + \cdots + b_n) = (a_1b_1) + \cdots + (a_nb_n) \ .$$

证. (1). 显然.

(2). 由上面的证明，每 $a_j = a_je_j$, $b_j = b_je_j$; 所以

$$\Big(\sum_{i=1}^n a_i\Big)\Big(\sum_{j=1}^n b_j\Big) = \Big(\sum_{i=1}^n a_ie_i\Big)\Big(\sum_{j=1}^n b_je_j\Big) = \sum_{i=1}^n\sum_{j=1}^n a_ie_ib_je_j = \sum_{i=1}^n\sum_{j=1}^n a_ib_je_ie_j$$

由于 $i \ne j$ 时 $e_ie_j = 0$, 所以

$$\Big(\sum_{i=1}^n a_i\Big)\Big(\sum_{j=1}^n b_j\Big) = \sum_{j=1}^n a_jb_je_je_j = \sum_{j=1}^n a_je_jb_je_j = \sum_{j=1}^n a_jb_j \ .$$

定义. 如果环 R 的元素 e 满足 $e^2=e$, 称 e 为 幂等元 . 如果幂等元 $e\in Z(R)$, 则称 e 为 R 的 中心幂等元.

如果环 R 的一组幂等元 $e_1,\cdots,e_n$ 满足对任 $1\le i\ne j\le n$ 有 $e_ie_j=0$, 就称 $e_1,\cdots,e_n$ 为 正交幂等元系.

如果幺环 R 的正交幂等元系 $e_1,\cdots,e_n$ 使得 $1=e_1+\cdots+e_n$, 就称 $e_1,\cdots,e_n$ 为 完全正交幂等元系.

上命题就是说幺环 R 的理想直和分解给出一个 完全正交中心幂等元系.

3.3.3 命题. 设 $e_1,\cdots,e_n$ 是幺环 R 的完全正交中心幂等元系, 那么 $Re_j=\{ae_j\mid a\in R\}$ 是 R 的理想, 而 $R=Re_1\oplus\cdots\oplus Re_n$.

证. 对任 $ae_j,be_j\in Re_j$, 有 $ae_j-be_j=(a-b)e_j\in Re_j$; 又若 $c\in R$, 有 $c(ae_j)=(ca)e_j\in Re_j$; 因 e_j 是中心元, 还有 $(ae_j)c=(ac)e_j\in Re_j$. 所以 Re_j 是理想.

任 $a\in R$, 有 $a=a1=a(e_1+\cdots+e_n)=ae_1+\cdots+ae_n$; 又若 $a=a_1+\cdots+a_n$ 其中 $a_j\in Re_j$, 那么可写 $a_j=b_je_j$ 其中 $b_j\in R$, 所以

$$a_j=b_je_j=(b_1e_1+\cdots+b_je_j+\cdots+b_ne_n)e_j=ae_j\ .$$

即 3.3.1 的两条都成立, 所以 $R=Re_1\oplus\cdots\oplus Re_n$. □

例. 设 $R=\mathbb{Z}_6$. 设 $e_1=[3],\ e_2=[4]$. 则

$$e_1^2=[3]^2=[3]=e_1\ ;\quad e_2^2=[4]^2=[4]=e_2\ ;\quad e_1e_2=[3][4]=[0]\ ;\quad [3]+[4]=[1]\ .$$

所以 e_1, e_2 构成 R 的完全正交幂等元系 ($\mathbb{Z}_6$ 是交换环所以幂等元都是中心幂等元).

$$Re_1=\left\{\,[n][3]\;\middle|\;[n]\in R\,\right\}=\left\{\,[0],\ [3]\,\right\}\ ;$$

$$Re_2=\left\{\,[n][4]\;\middle|\;[n]\in R\,\right\}=\left\{\,[0],\ [2],\ [4]\,\right\}\ ;$$

都是 R 的理想. 实际上, 这两个理想本身都是幺环 (但不是 R 的幺子环因为它们的单位元不是 R 的单位元), 而且

$$\begin{aligned}\mathbb{Z}_2&\cong Re_1\ ,\quad [0]_2\mapsto[0]_6\ ,\ \ [1]_2\mapsto[3]_6\ ;\\ \mathbb{Z}_3&\cong Re_2\ ,\quad [0]_3\mapsto[0]_6\ ,\ \ [1]_3\mapsto[4]_6\ ,\ \ [2]_3\mapsto[2]_6\ .\end{aligned}$$

而 $R=Re_1\oplus Re_2$, 即

$$\mathbb{Z}_6=\left\{\,[0],\ [3]\,\right\}\bigoplus\left\{\,[0],\ [2],\ [4]\,\right\}\ ;$$

每个元素的表写:

$$\begin{aligned}&[0]=[0]+[0]\ ,\quad [1]=[3]+[4]\ ,\quad [2]=[0]+[2]\ ,\\ &[3]=[3]+[0]\ ,\quad [4]=[0]+[4]\ ,\quad [5]=[3]+[2]\ .\end{aligned}$$

外在地构造环的直和的办法

设 $R_1, \cdots, R_n$ 都是幺环. 作集合积 (即卡氏积)

$$R = R_1 \times \cdots \times R_n = \{\, (a_1, \cdots, a_n) \mid a_j \in R_j,\ \jmath = 1, \cdots, n \,\}$$

再定义运算:

$$(a_1, \cdots, a_n) + (a'_1, \cdots, a'_n) = (a_1 + a'_1,\ \cdots,\ a_n + a'_n)\ ,$$

$$(a_1,\ \cdots,\ a_n) \cdot (a'_1,\ \cdots,\ a'_n) \ \ = \ \ (a_1 a'_1,\ \ \cdots,\ \ a_n a'_n)\ ;$$

那么容易验证 R 是一个幺环 (单位元是 $(1, \cdots, 1)$); 而且, 令

$$I_j = \{\, (0, \cdots, 0, a_j, 0, \cdots, 0) \mid a_j \in R_j \,\}\ , \qquad j = 1, \cdots, n\ ;$$

则 I_j 都是 R 的理想, 作为环 $I_j \cong R_j$, 而 $R = I_1 \oplus \cdots \oplus I_n$. 所以称 R 为环 R_1, $\cdots$, R_n 的外直和. 有时也记作 $R = R_1 \oplus \cdots \oplus R_n$.

例. 设 $R_1 = \mathbb{Z}_2$, $R_2 = \mathbb{Z}_3$. 直和

$$\begin{aligned} \mathbb{Z}_2 \bigoplus \mathbb{Z}_3 \ \ = \ \ \Big\{ & \Big([0]_2,\, [0]_3\Big)\ , \quad \Big([1]_2,\, [1]_3\Big)\ , \quad \Big([0]_2,\, [2]_3\Big)\ , \\ & \Big([1]_2,\, [0]_3\Big)\ , \quad \Big([0]_2,\, [1]_3\Big)\ , \quad \Big([1]_2,\, [2]_3\Big) \Big\}\ . \end{aligned}$$

对群有完全类似的构造, 作为习题 5, 习题 6.

直和的可逆元乘群

3.3.4 命题. 设 $R_1, \cdots, R_n$ 都是幺环, $R_1^\times, \cdots, R_n^\times$ 是相应的可逆元乘群. 则

$$(R_1 \oplus \cdots \oplus R_n)^\times = R_1^\times \times \cdots \times R_n^\times\ .$$

证. $R_1 \oplus \cdots \oplus R_n$ 的单位元为 $(1_1, \cdots, 1_n)$ 其中位置 j 上的 1_j 是 R_j 的单位元. 如果 $(a_1, \cdots, a_n)$, $(a'_1, \cdots, a'_n) \in R_1 \oplus \cdots \oplus R_n$ 使得

$$(a_1, \cdots, a_n)\,(a'_1, \cdots, a'_n) = (a_1 a'_1, \cdots, a_n a'_n) = (1, \cdots, 1)\ ,$$

则 $a_j a'_j = 1_j$, $j = 1, \cdots, n$. 由此可知

$$(a_1, \cdots, a_n) \in (R_1 \oplus \cdots \oplus R_n)^\times \quad \Longleftrightarrow \quad a_j \in R_j^\times\ ,\ \forall\, j = 1, \cdots, n\ . \qquad \square$$

中国剩余定理

3.3.5 命题. 设 I_1, $\cdots$, I_n 是环 R 的理想, 记 $I = I_1 \cap \cdots \cap I_n$. 那么有单同态

$$\bar\gamma : \quad R/I \ \longrightarrow\ R/I_1 \oplus \cdots \oplus R/I_n\ , \quad a + I \ \longmapsto\ (a + I_1,\ \cdots,\ a + I_n)\ .$$

证. 易验证下述映射是环同态

$$\gamma: \quad R \longrightarrow R/I_1 \oplus \cdots \oplus R/I_n\,, \quad a \longmapsto (a+I_1,\ \cdots,\ a+I_n)\,.$$

而且

$$\begin{aligned}\mathrm{Ker}(\gamma) &= \{\, a \in R \mid a + I_j = I_j\,,\ \ j = 1, \cdots, n \,\} \\ &= \{\, a \in R \mid a \in I_j\,,\ \ j = 1, \cdots, n \,\} \\ &= I_1 \cap \cdots \cap I_n = I\,;\end{aligned}$$

由同态基本定理，得本命题. □

定义. 幺环 R 的两个理想 I_1 和 I_2 称为 *互素的 (coprime)* 如果 $I_1 + I_2 = R$.

例. $\mathbb{Z}$ 的理想 $\mathbb{Z}a_1$ 和 $\mathbb{Z}a_2$ 互素当且仅当 $\gcd(a_1,\ a_2) = 1$.

证. $\mathbb{Z}a_1 + \mathbb{Z}a_2 = \mathbb{Z}$, 当且仅当存在 $b_1,\ b_2 \in \mathbb{Z}$ 使得 $b_1a_1 + b_2a_2 = 1$, 当且仅当 $\gcd(a_1,\ a_2) = 1$. □

如果整数 $a_1, \cdots, a_n$ 两两互素，则任 a_j 与 $a_1 \cdots a_{j-1}a_{j+1} \cdots a_n$ 互素. 对理想有同样结论.

引理. *设幺环 R 的理想 $I_1, \cdots, I_n$ 两两互素. 那么对任 $1 \le j \le n$, 积理想 $I_1 \cdots I_{j-1}I_{j+1} \cdots I_n$ 与理想 I_j 互素.*

证. 注意，由于 R 有单位元 1, 所以 $RR = R$.
不妨对 $j = 1$ 给出证明. 对任 $k > 1$ 有 $I_1 + I_k = R$, 所以

$$(I_1 + I_2)(I_1 + I_3) \cdots (I_1 + I_n) = R\,;$$

左边按分配律展开，共 2^{n-1} 项，除一项 $I_2I_3 \cdots I_n$ 外，其他均含 I_1 为因子，因此都包含在 I_1 中，那么它们的和，记作 I, 也包含在 I_1 中，即

$$R = I_1^n + \cdots + (I_2I_3 \cdots I_n) \subseteq I_1 + I_2I_3 \cdots I_n\,.$$

所以 I_1 与 $I_2I_3 \cdots I_n$ 互素. □

3.3.6 中国剩余定理. *设幺环 R 的理想 $I_1, \cdots, I_n$ 两两互素，记 $I = I_1 \cap \cdots \cap I_n$. 那么有环同构：*

$$\bar{\gamma}: \quad R/I \xrightarrow{\ \cong\ } R/I_1 \oplus \cdots \oplus R/I_n\,, \quad a + I \longmapsto (a+I_1,\ \cdots,\ a+I_n)\,.$$

证. 由命题 3.3.5, 只需证明下述环同态是满射：

$$\gamma: \quad R \longrightarrow R/I_1 \oplus \cdots \oplus R/I_n\,, \quad a \longmapsto (a+I_1,\ \cdots,\ a+I_n)\,.$$

由上述引理, 对任何指标 j, $1 \le j \le n$, 都有 $I_j + I_1 \cdots I_{j-1} I_{j+1} \cdots I_n = R$, 因此存在 $s_j \in I_j$ 和 $\ell_j \in I_1 \cdots I_{j-1} I_{j+1} \cdots I_n$ 使得 $s_j + \ell_j = 1$; 因此

$$\ell_j + I_k = \begin{cases} 1 + I_k\,, & \text{若 } k = j, \\ I_k\,, & \text{若 } k \ne j. \end{cases} \qquad \text{或写作} \quad \ell_j \equiv \begin{cases} 1 \pmod{I_k}, & \text{若 } k = j, \\ 0 \pmod{I_k}, & \text{若 } k \ne j. \end{cases} \tag{$*$}$$

那么对任 $(a_1 + I_1,\ \cdots,\ a_n + I_n) \in R/I_1 \oplus \cdots \oplus R/I_n$, 令

$$a = a_1 \ell_1 + \cdots + a_n \ell_n\,, \tag{$**$}$$

则

$$a = a_1 \ell_1 + \cdots + a_n \ell_n \equiv 0 + \cdots + 0 + a_k \cdot 1 + 0 + \cdots + 0 \equiv a_k \pmod{I_k}$$

所以

$$\gamma(a) = (a + I_1,\ \cdots,\ a + I_n) = (a_1 + I_1,\ \cdots,\ a_n + I_n)\,.$$

即 γ 是满射. □

注. 证明中的 $(*)$ 和 $(**)$ 给出了满射 γ 的原像的构造方法.

3.3.7 推论. *如果 $m_1, \cdots, m_n \in \mathbb{Z}$ 两两互素, 记 $m = m_1 \cdots m_n$. 那么有环同构:*

$$\mathbb{Z}_m \xrightarrow{\cong} \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}\,, \quad [a]_m \longmapsto ([a]_{m_1},\ \cdots,\ [a]_{m_n})\,.$$

推论. *如果 $m = p_1^{n_1} \cdots p_k^{n_k}$ 是正整数 m 的标准分解式, 则*

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}\,, \quad [a]_m \mapsto ([a]_{p_1^{n_1}},\ \cdots,\ [a]_{p_k^{n_k}})\,. \qquad \square$$

3.3.8 推论. *Euler 函数 $\varphi(p_1^{n_1} \cdots p_k^{n_k}) = p_1^{n_1 - 1}(p_1 - 1) \cdots p_k^{n_k - 1}(p_k - 1)$.*

证. 记 $m = p_1^{n_1} \cdots p_k^{n_k}$. 由上述推论, $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$. 再由命题 3.3.4, 得

$$\mathbb{Z}_m^\times \cong \mathbb{Z}_{p_1^{n_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{n_k}}^\times\,;$$

所以 $\varphi(m) = \varphi(p_1^{n_1}) \cdots \varphi(p_k^{n_k})$.

那么只需证明 $\varphi(p^n) = p^{n-1}(p-1)$ 其中 p 是素数. 任何 $< p^n$ 的非负整数可写成

$$ap + b\,, \qquad a = 0, 1, \cdots, p^{n-1} - 1,\ \ b = 0, 1, \cdots, p - 1\,;$$

它与 p 互素当且仅当 $b = 1, \cdots, p-1$, 这样的整数共 $p^{n-1}(p-1)$ 个. □

注. "孙子算经", 作者和写作年代不详, 出现于四、五世纪. 下卷第 26 题:

今有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何? 答曰: "二十三".

韩信点兵的故事： 韩信点兵，约数十人. 汉王问，有多少兵？韩信说，三人三人一列，余一人；五人五人一列，余二人；七人七人一列，余四人. 问兵多少？

这里 $3\cdot 5\cdot 7=105$, 要求 $a\in\mathbb{Z}_{105}$ 使得 $(a,a,a)=(1,2,4)\in\mathbb{Z}_3\oplus\mathbb{Z}_5\oplus\mathbb{Z}_7$. 按照 $(*)$ 和 $(**)$, 先要求出 ℓ_1,ℓ_2,ℓ_3 使得

$$\ell_1\equiv\begin{cases}1, & (\mathrm{mod}\ 3)\\ 0, & (\mathrm{mod}\ 5)\\ 0, & (\mathrm{mod}\ 7)\end{cases}\qquad \ell_2\equiv\begin{cases}0, & (\mathrm{mod}\ 3)\\ 1, & (\mathrm{mod}\ 5)\\ 0, & (\mathrm{mod}\ 7)\end{cases}\qquad \ell_3\equiv\begin{cases}0, & (\mathrm{mod}\ 3)\\ 0, & (\mathrm{mod}\ 5)\\ 1, & (\mathrm{mod}\ 7)\end{cases}$$

然后知道 $(a_1,a_2,a_3)\in\mathbb{Z}_3\oplus\mathbb{Z}_5\oplus\mathbb{Z}_7$ 在 $\mathbb{Z}_{105}$ 中的原像是 $a=a_1\ell_1+a_2\ell_2+a_3\ell_3$.

可以通过辗转相除求出：

$$\ell_1=70\,,\qquad \ell_2=21\,,\qquad \ell_1=15\,;$$

所以韩信点兵的答案是： $1\cdot 70+2\cdot 21+4\cdot 15=172$; 模 105, 得 67 人.

宋朝数学家秦九韶把这种算法叫做“大衍求一术”. 对上述韩信点兵的算法歌诀曰：

三人同行七十稀,
五树梅花廿一枝,
七子团圆正半月,
除百零五便得知.

习题 3.3

1. 设 I_1, I_2 是环 R 两个理想. 则 $R=I_2\oplus I_2$ 当且仅当 $R=I_1+I_2$ 且 $I_1\cap I_2=0$.

2. 设环 R 是两个理想 I_1, I_2 的之和. 证明： $R/I_1\cong I_2$.

2. 幺环 R 的非空子集 L 称为 *左理想* 如果 L 在加法下构成子群, 而且对任 $a\in L$ 和 $r\in R$ 有 $ra\in L$. 左理想的直和按 2.3.1 类似地定义. 证明

(1). 对任 $a\in R$, 子集 $Ra=\{\,ra\mid r\in R\,\}$ 是 R 的左理想.

(2). R 是左理想的直和 $R=L_1\oplus\cdots\oplus L_n$, 当且仅当 R 有完全正交幂等元系 $e_1,\cdots,e_n$ 使得 $L_j=Re_j$, $j=1,\cdots,n$.

3. 设实向量空间 V 分解为子空间的直和 $V=V_1\oplus\cdots\oplus V_n$, 即任 $v\in V$ 有唯一表达式 $v=v_1+\cdots+v_n$ 其中 $v_j\in V_j$; 定义 $\pi_j:V\to V$ 为 $\pi_j(v)=v_j$. 证明：

(1). $\pi_1,\cdots,\pi_n$ 是幺环 $E=\mathrm{End}(V)$ 的完全正交幂等元系, 从而有左理想直和分解: $E=E\pi_1\oplus\cdots\oplus E\pi_n$.

(2). $\alpha\in E\pi_j$, 当且仅当 $\alpha\pi_j=\alpha$, 当且仅当 $\mathrm{Ker}(\alpha)\supseteq V_1\oplus\cdots V_{j-1}\oplus V_{j+1}\oplus\cdot\oplus V_n$.

4. 设 G_1, $\cdots$, G_n 是群. 作集合积

$$G=G_1\times\cdots\times G_n=\{\,(g_1,\cdots,g_n)\mid g_j\in G_j,\ j=1,\cdots,n\,\}$$

定义运算：

$$(g_1, \cdots, g_n)\cdot(g_1', \cdots, g_n') \;=\; (g_1g_1',\ \cdots,\ g_ng_n')\,;$$

证明：

(1). G 是群 (称为群 $G_1, \cdots, G_n$ 的 外直积).

(2). $H_j = \{\,(1,\cdots,1,g_j,1,\cdots,1) \mid g_j \in G_j\,\}$, $j = 1,\cdots,n$, 都是正规子群，而且 $H_j \cong G_j$; 又，对 $1 \le i \ne j \le n$, H_i 与 H_j 的元素相乘可交换.

5. 设 G 为群，设 $H_1, \cdots, H_n$ 是 G 的正规子群，而且对 $1 \le i \ne j \le n$, H_i 与 H_j 的元素相乘可交换.

如果 G 的任何元 g 可以唯一的写成 $g = g_1\cdots g_n$ 其中 $g_j \in H_j$, 就称群 G 是正规子群 $H_1, \cdots, H_n$ 的 *(内) 直积*, 记作 $G = H_1 \times \cdots \times H_n$. 证明以下两条等价：

(i). $G = H_1 \times \cdots \times H_n$.

(ii). $G = H_1\cdots H_n$, 且 $(H_1\cdots H_j)\cap H_{j+1} = 1$, $j = 1, \cdots, n_1$.

6. 设 H 和 K 是群 G 的正规子群，且 $G = HK$. 证明 $G/H\cap K \cong G/H \times G/K$.

7. 设 $H_1, \cdots, H_n$ 是群 G 的正规子群，记 $H = H_1 \cap \cdots \cap H_n$. 那么有单同态

$$\bar\gamma:\quad G/H \;\longrightarrow\; G/H_1 \times \cdots \times G/H_n\,,\quad xH \;\longmapsto\; (xH_1,\ \cdots,\ xH_n)\,.$$

§3.4 多项式环

概要: 多项式环；基本性质；多项式取值；插值定理；多项式函数；多元多项式，对称多项式.

在复数域中讨论多项式时，往往把一个多项式 $f(x) = a_0 + a_1x + \cdots + a_nx^n$ 作为一个复函数， $\mathbb{C} \to \mathbb{C}$, $c \mapsto f(c)$. 在实数域、或在有理数域上讨论多项式时也常常是这样的观点.

但在任意交换幺环 R 中讨论多项式时这种看法有很大局限性. 例如在 $R = \mathbb{Z}_2 = \{0, 1\}$ 上，多项式 $x^2 - x$ 与零多项式 0 作为 R 到 R 的函数是一样的.

所以我们从一种形式化的观点出发来讨论多项式. 然后再来看看形式化的多项式与多项式作为函数有什么关系.

多项式环

以下恒设 R 是交换幺环. 我们说表达式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n\,,\qquad a_i \in R\,,\ \ a_n \ne 0\,,$$

是 R- 系数的多项式 (简称 R- 多项式) 时，是把其中的 x 作为一个形式符号，称为 不定元 (而不称为未知数); 称这个多项式的次数为 n, 记作 $\deg f = n$; 为方便也沿用数字系数多项式的说法，称 $a_0 \in R$ 为 常数多项式; 约定零多项式 0 的次数为 $-\infty$. 称两个 R- 多项式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n\,,\qquad a_n \ne 0\,,$$

和

$$g(x) = b_0 + b_1x + \cdots + b_mx^m\ , \qquad b_m \neq 0\ ,$$

相等，记作 $f(x) = g(x)$, 如果 $m = n$ 且 $a_i = b_i$, $i = 1, \cdots, n$. 这样我们就构建了集合

$$R[x] = \{\, a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R\ ,\ \ a_n \neq 0\ ,\ \ n \geq 0\ ,\ 或\ n = -\infty \,\}$$

完全与数字系数多项式一样地定义加法和乘法运算. 加法运算：

$$\sum_{i=0}^{n} a_ix^i + \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{n} (a_i + b_i)x^i\ ;$$

这里两多项式次数不相同时，例如后一多项式次数 $m < n$ 时把它的高于 m 次的项看作零系数的项. 乘法运算：

$$\left(\sum_{i=0}^{n} a_ix^i\right)\left(\sum_{j=0}^{m} b_jx^j\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_ib_j\right)x^k\ .$$

按常规计算就可验证 $R[x]$ 是一个交换幺环.

定义. 称 $R[x]$ 为交换环 R 上的 *一元多项式环*.

基本性质

首先，如果 R 是整环，则次数公式成立. 更一般的，有：

3.4.1 次数公式. *设 $f(x), g(x) \in R[x]$, 设 $g(x)$ 的首项系数不是零因子. 则*

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)\ .$$

证. 如果 $f(x) = 0$, 则两边都是 $-\infty$, 故等式成立. 否则 $f(x) = a_mx^m + \cdots + a_1x + a_0$ 其中 $a_m \neq 0$, $g(x) = b_nx^n + \cdots + b_1x + b_0$ 其中 b_n 不是零因子. 那么

$$f(x)g(x) = a_mb_nx^{m+n} + (a_mb_{n-1} + a_{m-1}b_n)x^{m+n-1} + \cdots + (a_1b_0 + a_0b_1)x + a_0b_0$$

其中 $a_mb_n \neq 0$ 因为 b_n 不是零因子而 $a_m \neq 0$. 即 $\deg(f(x)g(x)) = m + n = \deg f(x) + \deg g(x)$. □

但若 R 不是整环，则次数公式不一定成立；例如：在 $\mathbb{Z}_6[x]$ 中： $([2]x) \cdot ([3]x) = 0$.

3.4.2 带余除法. *设 R 是交换环；设 $f(x), g(x) \in R[x]$, 其中 $g(x)$ 的首项系数是 R 的可逆元. 则存在唯一 $q(x) \in R[x]$ 和唯一 $r(x) \in R[x]$ 满足 $\deg r(x) < \deg g(x)$ 使得 $f(x) = g(x)q(x) + r(x)$.*

证. 设 $f(x) = a_mx^m + a_{m-1}x^{m-1} + \cdots + a_0$; 设 $g(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_0$ 其中 b_n 可逆.

先证存在性. 若 $m < n$, 则

$$f(x) = 0 \cdot g(x) + f(x)\ , \qquad \deg f(x) < \deg g(x)$$

否则 $m \geq n$, 令

$$h(x) = f(x) - (a_m b_n^{-1} x^{m-n}) g(x)\ ;$$

则 $\deg h(x) < \deg f(x)$. 按对次数的归纳法, 即

$$h(x) = q_1(x)g(x) + r(x)\ , \qquad \deg r(x) < \deg g(x)\ ,$$

就有 $f(x) = (a_m b_n^{-1} x^{m-n}) g(x) + h(x)$; 令 $q(x) = a_m b_n^{-1} x^{m-n} + q_1(x)$, 则

$$f(x) = q(x)g(x) + r(x)\ , \qquad \deg r(x) < \deg g(x)\ .$$

再证唯一性. 如果还有 $f(x) = g(x)q'(x) + r'(x)$, $\deg r'(x) < \deg g(x)$; 那么从 $g(x)q'(x) + r'(x) = f(x) = g(x)q(x) + r(x)$, 就得出

$$g(x)(q'(x) - q(x)) = r(x) - r'(x)\ ;$$

若 $q'(x) - q(x) \neq 0$, 由于 $g(x)$ 的首项系数可逆, 由 3.4.1, 知: 左端次数 $= \deg g(x) + \deg(q'(x) - q(x)) > \deg(r(x) - r'(x))$, 这是矛盾; 所以 $q'(x) - q(x) = 0$ 随之 $r'(x) - r(x) = 0$; 即 $q'(x) = q(x)$ 且 $r'(x) = r(x)$. □

这个带余除法需要条件: "除式" $g(x)$ 的首项系数是 R 的可逆元; 这条件一般无法保证满足. 所以 3.4.2 并不意味一般整环上的多项式环是欧氏整环. 但是如果 R 是域, 则只要是非零多项式则首项系数就是可逆元. 所以得下述定理.

3.4.3 定理. *域上的多项式环是欧氏整环, 从而是主理想整环.* □

注. 一般整环上的多项式环不一定是主理想整环. 例如 $\mathbb{Z}[x]$ 中 3 和 x 两个元素生成的理想

$$I = \langle 3, x \rangle = \mathbb{Z}[x] \cdot 3 + \mathbb{Z}[x] \cdot x = \{\, a_n x^n + \cdots + a_1 x + a_0 \mid n \geq 0,\ \ a_i \in \mathbb{Z},\ \ 3 | a_0 \,\}\ ,$$

不是主理想. 因为: 如果 $I = \mathbb{Z}[x] \cdot g(x)$ 是由一个 $g(x)$ 生成的理想, 则存在 $f(x)$ 使得 $3 = f(x)g(x)$, 所以 $f(x)$, $g(x)$ 都得是常数多项式, 而 $g(x) \in I$, 故只能是 $g(x) = 3$; 但是 $x \in I$, 即 $x = h(x) \cdot 3$; 但这是不可能的. □

多项式取值

对 $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$, 对 $r \in R$, 记 $f(r) := a_0 + a_1 r + \cdots + a_n r^n$, 称为 $f(x)$ 在点 r 处的值. 如果 $f(r) = 0$ 就称 r 是多项式 $f(x)$ 的 *零点*, 或称 $f(x)$ 的 *根*.

对任一多项式 $f(x)\in R[x]$, 映射 $r\mapsto f(r)$, 就是由多项式 $f(x)$ 决定的 R 到 R 的一个函数; 为了加以区别, 把这个函数记作 $f^*(x)$. 这种有多项式决定的 R 到 R 的函数称为多项式函数. 把 R 到 R 的所有函数的集合记作 $\mathrm{Fun}(R,R)$; 就有映射

3.4.4 $$R[x]\longrightarrow \mathrm{Fun}(R,R)\ ,\quad f(x)\longmapsto f^*(x)\ ;$$

注意, $\mathrm{Fun}(R,R)$ 也是一个交换幺环: 对 $\alpha,\beta\in \mathrm{Fun(R,R)}$, 它们的和 $\alpha+\beta$ 定义为

$$(\alpha+\beta)(r)=\alpha(r)+\beta(r)\ ,\qquad \forall\, r\in R\ ;$$

它们的积 $\alpha\beta$ 定义为

$$(\alpha\beta)(r)=\alpha(r)\beta(r)\ ,\qquad \forall\, r\in R\ .$$

这种乘法一般称为 "点积"; 它与函数 (也就是 R 的变换) 合成是完全不同的运算.

按常规计算就可证明映射 3.4.4 是幺环同态. 将从两个方面考查同态 3.4.4 的性质.

这里先看看多项式取值带来的多项式的性质.

3.4.5 余式定理. *设 R 是交换幺环. 设 $f(x)\in R[x]$, $r\in R$. 则存在唯一 $q(x)\in R[x]$ 使得 $f(x)=(x-r)q(x)+f(r)$.*

证. 由于 $x-r$ 是首一的多项式, 由带余除法 3.4.2, 存在唯一 $q(x)\in R[x]$ 和 $s\in R$ 使得 $f(x)=(x-r)q(x)+s$. 带入 $x=r$, 得 $f(r)=s$. □

以下是一系列推论.

3.4.6 推论. *设 R 是整环. 设 $f(x),g(x)\in R[x]$, 设 $\deg f(x)=n\geq 0$, $\deg g(x)\leq n$.*

(1) *如果 $r_1,\cdots,r_k\in R$ 是 $f(x)$ 的两两不同的根, 则有 $g(x)\in R[x]$ 使得 $f(x)=(x-r_1)\cdots(x-r_k)g(x)$.*

(2) *$f(x)$ 在 R 中最多有 n 个互不相同的根.*

(3) *如果有 $n+1$ 个互不相同的 $r_1,\cdots,r_n,r_{n+1}\in R$ 使得 $f(r_i)=g(r_i)$, $i=1,\cdots,n,n+1$, 则在 $R[x]$ 中 $f(x)=g(x)$.*

证. (1). 对 k 归纳. $k=1$ 时, 就是上述余式定理. 设 $k>1$. 由余式定理, $f(x)=(x-r_1)q(x)$; 对 $j\neq 1$, 在 R 中有: $(r_j-r_1)q(r_j)=f(r_j)=0$, 但是 R 没有零因子, 而 $r_j-r_1\neq 0$, 所以

$$q(r_j)=0\ ,\qquad j=2,\cdots,k\ ;$$

由归纳法, $q(x)=(x-r_2)\cdots(x-r_k)g(x)$; 所以 $f(x)=(x-r_1)(x-r_2)\cdots(x-r_k)g(x)$.

(2). 若 $f(x)$ 在 R 中有 $n+1$ 个互不相同的根 $r_1,\cdots,r_n,r_{n+1}$, 由上面证明的 (1), $f(x)=(x-r_1)\cdots(x-r_n)(x-r_{n+1})g(x)$; 那么按次数公式有 $\deg f(x)\geq n+1$; 与假设矛盾. □

(3). 令 $h(x)=f(x)-g(x)\in R[x]$, 则 $\deg h(x)\leq n$; 按条件,

$$h(r_j)=0\ ,\qquad j=1,\cdots,n,n+1\ ;$$

由上面证明的 (2), 只能是 $h(x)=0$ 为零多项式. 所以 $f(x)=g(x)$. □

插值定理

3.4.7 牛顿 - 拉格朗日插值定理. 设 $\mathbb{F}$ 是域, $a_1,\cdots,a_k\in\mathbb{F}$ 两两不等; 令 $t(x)=\prod_{i=1}^{k}(x-a_i)$. 那么对任 $b_1,\cdots,b_k\in\mathbb{F}$ 存在唯一次数 $<k$ 的多项式 $h(x)\in\mathbb{F}[x]$ 使得:

(1) $h(a_i)=b_i\ ,\quad i=1,\cdots,k.$

(2) 如果 $f(x)\in\mathbb{F}[x]$ 使得 $f(a_i)=b_i,\ i=1,\cdots,k,$ 则存在唯一 $g(x)\in\mathbb{F}[x]$ 使 $f(x)=h(x)+g(x)t(x)$.

证. 对 $i\neq j$, 有 $(x-a_i)-(x-a_j)=a_j-a_i\neq 0$; 那么

$$1=(a_j-a_i)^{-1}(a_j-a_i)\in\mathbb{F}[x](x-a_i)+\mathbb{F}[x](x-a_j)\ ;$$

所以 $\mathbb{F}[x](x-a_i)+\mathbb{F}[x](x-a_j)=\mathbb{F}[x]$; 即理想 $\mathbb{F}[x](x-a_i)$ 与 $\mathbb{F}[x](x-a_j)$ 互素.

按 $t(x)$ 的定义, 它生成的理想 $\mathbb{F}[x]t(x)\subseteq\mathbb{F}[x](x-a_i),\ i=1,\cdots,k$; 故 $\mathbb{F}[x]t(x)\subseteq\bigcap_{i=1}^{k}\mathbb{F}[x](x-a_i)$. 反之, 设 $f(x)\in\bigcap_{i=1}^{k}\mathbb{F}[x](x-a_i)$, 则对 $1\leq i\leq k$, 有 $f(x)\in\mathbb{F}[x](x-a_i)$ 故可写 $f(x)=h(x)(x-a_i)$, 从而 $f(a_i)=0$; 由推论 3.4.6(1), 有 $g(x)\in\mathbb{F}[x]$ 使 $f(x)=g(x)t(x)$. 得 $f(x)\in\mathbb{F}[x]t(x)$. 综上得 $\mathbb{F}[x]t(x)=\bigcap_{i=1}^{k}\mathbb{F}[x](x-a_i)$.

由中国剩余定理得环同构:

$$\begin{array}{ccc}\mathbb{F}[x]/\mathbb{F}[x]t(x) & \xrightarrow{\cong} & \mathbb{F}/\mathbb{F}(x-a_1)\ \oplus\ \cdots\ \oplus\ \mathbb{F}/\mathbb{F}(x-a_k)\ ,\\ f(x)+\mathbb{F}[x]t(x) & \longmapsto & (f(x)+\mathbb{F}(x-a_1)\ ,\ \cdots\ ,\ f(x)+\mathbb{F}(x-a_k))\ .\end{array}$$

对每 a_i, 易验证下述映射是满的环同态

$$\nu_{a_i}:\quad \mathbb{F}[x]\longrightarrow\mathbb{F}\ ,\quad f(x)\longmapsto f(a_i)\ ; \tag{VL}$$

它的同态核是由 $x-a_i$ 生成的理想 $\mathbb{F}[x](x-a_i)$. 由同态基本定理, ν_{a_i} 诱导同构

$$\bar{\nu}_{a_i}:\quad \mathbb{F}[x]/\mathbb{F}[x](x-a_i)\ \xrightarrow{\cong}\ \mathbb{F}\ ,\quad f(x)+\mathbb{F}[x](x-a_i)\ \longmapsto\ f(a_i)\ .$$

那么得到环同构

$$\begin{array}{ccc}\mathbb{F}/\mathbb{F}(x-a_1)\ \oplus\ \cdots\ \oplus\ \mathbb{F}/\mathbb{F}(x-a_k) & \xrightarrow{\cong} & \overbrace{\mathbb{F}\ \oplus\ \cdots\ \oplus\ \mathbb{F}}^{k}\ ,\\ (f(x)+\mathbb{F}(x-a_1)\ ,\ \cdots\ ,\ f(x)+\mathbb{F}(x-a_k)) & \longmapsto & (f(a_1),\ \cdots,\ f(a_k))\ .\end{array}$$

把它与上述由中国剩余定理得到的同构合成, 就得到环同构

$$\begin{array}{ccc}\mathbb{F}[x]/\mathbb{F}[x]t(x) & \xrightarrow{\cong} & \overbrace{\mathbb{F}\ \oplus\ \cdots\ \oplus\ \mathbb{F}}^{k}\ ,\\ f(x)+\mathbb{F}[x]t(x) & \longmapsto & (f(a_1),\ \cdots,\ f(a_k))\ .\end{array}$$

因此, 对 $(b_1,\cdots,b_k)\in\mathbb{F}\oplus\cdots\oplus\mathbb{F}$ 有唯一一个剩余类其中任何多项式 $f(x)$ 都满足 $f(a_i)=b_i$, $i=1,\cdots,k$. 由习题 6, 此剩余类含有唯一一个次数 $<k$ 的多项式 $h(x)$. 那么此剩余类可写为 $h(x)+\mathbb{F}[x]t(x)$. 这样 (1),(2) 两条都获证. □

注. 对 $(b_1,\cdots,b_k)\in\mathbb{F}\oplus\cdots\oplus\mathbb{F}$, 如何具体找出 $h(x)$ 满足插值定理中 (1),(2) 两条? 由中国剩余定理中的 $(*)$ 式, 关键是要找多项式 $\ell_i(x)$ 使得

$$\ell_i(x)\equiv\begin{cases}1\pmod{x-a_j}, & \text{如 } i=j;\\ 0\pmod{x-a_j}, & \text{如 } i\neq j.\end{cases}$$

令 $t_i(x)=t(x)/(x-a_i)$, 其中 $t(x)$ 如定理所设; 则 $t_i(a_i)\neq 0$. 下述多项式即满足上述要求, 它们被称为 拉格朗日多项式:

$$\ell_i(x)=t(x)/t(a_i)=\prod_{j\neq i}(x-a_j)\Big/\prod_{j\neq i}(a_i-a_j)\ ,\qquad i=1,\cdots,k\ ;$$

那么 $h(x)=\sum_{i=1}^{k}b_i\ell_i(x)$.

多项式函数

3.4.8 定理. (1) 如果 R 是无限整环, 则同态 *3.4.4* 是单同态.

(2) 如果 R 是有限整环, 则同态 *3.4.4* 是满同态.

证. (1). 如果 $f^*(x)=g^*(x)$, 即对任 $r\in R$ 有 $f(r)=g(r)$, 这样的 r 有无数个, 由定理 3.6.8(2), 在 $R[x]$ 中得 $f(x)=g(x)$. 即映射 3.4.4 是单射.

(2). 有限整环一定是域, 见习题 5. 写 $R=\{a_0=0,\ a_1=1,\ a_2,\ \cdots,\ a_{n-1}\}$. 对任意函数 $\alpha\in\mathrm{Fun}(R)$, 记 $b_i=\alpha(a_i)$, $i=0,1,\cdots,n-1$. 由插值定理 3.6.10, 存在 $f(x)\in R[x]$ 使得 $f(a_i)=b_i=\alpha(a_i)$, $i=0,1,\cdots,n-1$. 所以作为 R 的函数有 $f^*(x)=\alpha$. 即同态 3.6.11 是满同态. □

多元多项式

显然, 容易递归地定义交换幺环 R 上的 n 个不定元 x_1, $\cdots$, x_n 的多元多项式环

$$R[x_1,\cdots,x_n]=R[x_1,\cdots,x_{n-1}][x_n]\ ;$$

交换幺环 R 上的 n 个不定元 x_1, $\cdots$, x_n 的多项式形如

$$f(x_1,\cdots,x_n)=\sum_{(i_1,\cdots,i_n)}a_{i_1,\cdots,i_n}x_1^{i_1}\cdots x_n^{i_n}\ ,\qquad a_{i_1,\cdots,i_n}\in R\ ,$$

其中幂指数序列 $(i_1,\cdots,i_n)$ 在一个有限集跑动其元素是长 n 的非负整数序列. 例如, 当 $n=3$ 时, 如果有限集为 $\{(1,2,0),\ (0,1,2),\ (2,0,1)\}$, 系数为 $a_{1,2,0}=a_{0,1,2}=a_{2,0,1}=1$, 则多项式为

$$x_1x_2^2+x_2x_3^2+x_3x_1^2\ .$$

对长 n 的非负整数序列按字典排列规则排序：

$$(i_1,\cdots,i_n)\succ(j_1\cdots j_n)\quad \text{如果}\quad i_1=j_1,\ \cdots,\ i_t=j_t\,,\ \text{但}\ i_{t+1}>j_{t+1}\,.$$

显然，字典顺序是所有长 n 的非负整数序列的集合

$$\left\{(i_1,\cdots,i_n)\ \middle|\ \text{所有 } i_k \text{ 是非负整数}\right\}$$

上的全序关系而且它的任意子集有唯一极小成员．这种全序集称为 良序集 *(well-ordered set)*; 对它们可以做数学归纳法.

设多项式 $f(x_1,\cdots,x_n)=\sum_{i_1,\cdots,i_n}a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}$. 为方便，把 $(i_1,\cdots,i_n)$ 也称为多项式 f 的单项 $a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}$ 的 “次数”. 把 f 的所有项按次数的字典顺序 “降幂” 排列，即：如果 $(i_1,\cdots,i_n)\succ(j_1\cdots j_n)$ 则把 $a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}$ 排在 $a_{j_1\cdots j_n}x_1^{j_1}\cdots x_n^{j_n}$ 之前，也说：项 $a_{j_1\cdots j_n}x_1^{j_1}\cdots x_n^{j_n}$ 在项 $a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}$ 之后.

如上面提到的多项式的降幂排列为：

$$x_1x_2^2+x_2x_3^2+x_3x_1^2=x_1^2x_3+x_1x_2^2+x_2x_3^2\,.$$

因为 $(2,0,1)\succ(1,2,0)\succ(0,1,2)$.

对称多项式

在第二章已提到，任意 n 次置换群 G 作用在 $R[x_1,\cdots,x_n]$ 上.

定义. 在 S_n 作用下不变的 n 元多项式称为 对称多项式.

例如，$n=3$ 时，上述多项式 $x_1x_2^2+x_2x_3^2+x_3x_1^2$ 不是对称多项式，因为置换 $\alpha=(12)$ 把它变为 $x_2x_1^2+x_1x_3^2+x_3x_2^2\neq x_1x_2^2+x_2x_3^2+x_3x_1^2$. 而以下都是对称多项式：

$$x_1+x_2+x_3\,,\qquad x_1x_2+x_2x_3+x_3x_1\,,\qquad x_1x_2x_3\,;$$

$$x_1+x_2+x_3\,,\qquad x_1^2+x_2^2+x_3^2\,,\qquad x_1^3+x_2^3+x_3^3\,.$$

显然，对称多项式的和，差，积仍然是对称多项式．也就是说对称多项式的集合构成 $R[x_1,\cdots,x_n]$ 的子环.

重要例子. 把下式按 x 展开

$$(x-x_1)(x-x_2)\cdots(x-x_n)=x^n-\sigma_1x^{n-1}+\sigma_2x^{n-2}+\cdots+(-1)^n\sigma_n$$

所得系数 σ_k 显然是 x_1, $\cdots$, x_n 的多项式，而且是对称多项式：

$$\sigma_1=\sum_{1\le i_1\le n}x_{i_1}\,,$$

$$\sigma_2=\sum_{1\le i_1<i_2\le n}x_{i_1}x_{i_2}\,,$$

$$\cdots$$

$$\sigma_k = \sum_{1\le i_1<\cdots<i_k\le n} x_{i_1}\cdots x_{i_k}\,,$$

$$\cdots$$

$$\sigma_n = x_1x_2\cdots x_n\,.$$

3.4.9 定义. 上述对称多项式 $\sigma_1,\cdots,\sigma_n$ 称为 $x_1,\cdots,x_n$ 的 *初等对称多项式 (elementary symmetric polynomials in $x_1,\cdots,x_n$).*

初等对称多项式具有基本重要性. 如: $n=3$ 时, $x_1^2+x_2^2+x_3^2=\sigma_1^2-2\sigma_2$.

一般地, 我们有:

3.4.10 对称多项式基本定理. *对 $x_1,\cdots,x_n$ 的任对称多项式 $f(x_1,\cdots,x_n)\in R[x_1,\cdots,x_n]$ 存在唯一多项式 $g(y_1,\cdots,y_n)\in R[y_1,\cdots,y_n]$ 使得*

$$f(x_1,\cdots,x_n)=g(\sigma_1,\cdots,\sigma_n)\,.$$

证. 如前所述, 多元单项式的 "次数" 按字典顺序是全序关系, 多元多项式各项可以按 "次数" 降幂排列. 我们对多元多项式的次数使用数学归纳法.

容易验证下述结论 (习题 8):

(3.4.10.1). *对称多项式 $\sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$ 的首项是 $x_1^{i_1+\cdots+i_n}x_2^{i_2+\cdots+i_n}\cdots x_n^{i_n}$.*

以下设 $f(x_1,\cdots,x_n)=\sum_{i_1,\cdots,i_n}a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}$ 是对称多项式.

现在证明存在性. 设 $a_{l_1\cdots l_n}x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$, 其中 $a_{l_1\cdots l_n}\neq 0$, 是 f 的首项. 首先断言 $l_1\ge l_2\ge\cdots\ge l_n$; 因为, 若不是这样, 则有指标 t 使得 $l_1=\cdots=l_t<l_{t+1}$; 那么, 取对换 $\alpha=(t,t+1)$, 由 f 的对称性知 $f=\alpha f$ 它有非零项 $a_{l_1\cdots l_n}x_1^{l_1}\cdots x_t^{l_{t+1}}x_{t+1}^{l_t}\cdots x_n^{l_n}$, 而 $(l_1,\cdots,l_{t+1},l_t,\cdots,l_n)\succ(l_1,\cdots,l_t,l_{t+1},\cdots,l_n)$, 这与 $a_{l_1\cdots l_n}x_1^{l_1}\cdots x_t^{l_t}x_{t+1}^{l_{t+1}}\cdots x_n^{l_n}$ 是 f 的首项相矛盾.

令 $f_1=f-a_{l_1\cdots l_n}\sigma_1^{j_1}\sigma_2^{j_2}\cdots\sigma_n^{j_n}$, 其中

$$j_k=l_k-l_{k+1}\,,\forall\ k<n\,;\quad j_n=l_n\,;$$

即: $(j_1,\cdots,j_n)$ 是非负整数序列, 且

$$j_1+j_2+\cdots+j_n=l_1\,,\quad j_2+\cdots+j_n=l_2\,,\quad\cdots,\quad j_n=l_n\,.$$

那么 f_1 仍然是对称多项式, 但是, 因为 $a_{l_1\cdots l_n}\sigma_1^{j_1}\sigma_2^{j_2}\cdots\sigma_n^{j_n}$ 的首项是

$$a_{l_1\cdots l_n}x_1^{j_1+\cdots+j_n}x_2^{j_2+\cdots+j_n}\cdots x_n^{j_n}=a_{l_1\cdots l_n}x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n},$$

所以, 只要 $f_1\neq 0$, 它的首项就真正在 f 的首项之后. 因此, 若 $f_1\neq 0$ 就可按归纳法, 存在 $g_1(y_1,\cdots,y_n)\in R[y_1,\cdots,y_n]$ 使得 $f_1=g_1(\sigma_1,\cdots,\sigma_n)$. 那么, 取 $g=g_1+a_{l_1\cdots l_n}y_1^{j_1}\cdots y_n^{j_n}$, 就得到 $f(x_1,\cdots,x_n)=g(\sigma_1,\cdots,\sigma_n)$.

唯一性. 设

$$g(y_1,\cdots,y_n)\neq g'(y_1,\cdots,y_n)\in R[y_1,\cdots,y_n]$$

都使得

$$g(\sigma_1,\cdots,\sigma_n)=g'(\sigma_1,\cdots,\sigma_n)\in R[x_1,\cdots,x_n]\,.$$

那么在 $R[x_1,\cdots,x_n]$ 中, $h(y_1,\cdots,y_n)=g(y_1,\cdots,y_n)-g'(y_1,\cdots,y_n)\neq 0$, 但是

$$h(\sigma_1,\cdots,\sigma_n)=0\,.$$

然而, 如果 $ay_1^{i_1}\cdots y_n^{i_n}$ 和 $by_1^{j_1}\cdots y_n^{j_n}$ 是 $h(y_1,\cdots,y_n)$ 的两个不同 "次数" 的项, 从 (3.4.10.1) 可以知道: 在 $R[x_1,\cdots,x_n]$ 中 $a\sigma_1^{i_1}\cdots\sigma_n^{i_n}$ 和 $b\sigma_1^{j_1}\cdots\sigma_n^{j_n}$ 的首项 "次数" 也不相同因而不可能合并; 因此, 只要 $h(y_1,\cdots,y_n)\neq 0$ 则 $h(\sigma_1,\cdots,\sigma_n)\neq 0$. 这个矛盾就完成了唯一性的证明. □

注. 以上证明同时提供了把对称多项式表达为初等对称多项式的多项式的方法.

例如: $n=3$, $f(x_1,x_2,x_3)=x_1^3+x_2^3+x_3^3$; 其首项是 x_1^3, 故

$$f_1=f-\sigma_1^{3-0}\sigma_2^{0-0}\sigma_3^0=3\sum_{i<j}x_i^2x_j+6x_1x_2x_3;$$

而 f_1 的首项是 $3x_1^2x_2$, 所以

$$f_2=f_1-3\sigma_1^{2-1}\sigma_2^1=6\sigma_3-9\sigma_3=-3\sigma_3;$$

最后得到: $f=\sigma_1^3+3\sigma_1\sigma_2-3\sigma_3$.

习题 3.4

1. 设 $R=\mathbb{Z}_6=\mathbb{Z}/6\mathbb{Z}$. 证明 R- 多项式 x^3-x 在 R 中有 6 个根.

2. 证明: $R[x]$ 是整环当且仅当 R 是整环.

3. 证明: 在 $\mathbb{Z}[x]$ 中由 $4, 2x, x^2$ 三个元素生成的理想 $I=\mathbb{Z}[x]\cdot 4+\mathbb{Z}[x]\cdot(2x)+\mathbb{Z}[x]\cdot x^2$ 不能由两个元素生成.

4. 整环 R 的乘法群 $R^\times$ 的有限子群一定是循环群.

5. 证明: 有限整环一定是域. (提示: 若 R 是有限整环, 则对任 $a\in R-\{0\}$, 映射 $R\to R$, $x\mapsto ax$, 是满射.)

6. 设 $g(x)\in R[x]$, 设 $g(x)$ 的首项系数是 R 的可逆元, $k=\deg g(x)$. 证明:

(1). $g(x)$ 生成的理想 $R[x]g(x)$ 的任一剩余类 $f(x)+R[x]g(x)$ 中有唯一一个次数 $<k$ 的多项式. (提示: 引理 3.4.2)

(2) 下述多项式是剩余类环 $R[x]/R[x]g(x)$ 的一个完全代表系:

$$\sum_{i=0}^{k-1}a_ix^i\,,\qquad a_i\in R\,,\quad i=0,1,\cdots,k-1\,.$$

7. 设 R 是有限整环. 试求同态 3.4.4 的核.

8. 证明：对称多项式 $\sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$ 的首项是 $x_1^{i_1+\cdots+i_n}x_2^{i_2+\cdots+i_n}\cdots x_n^{i_n}$.

9. 令 $s_k=\sum_{i=1}^n x_i^k$, $k=0,1,2,\cdots$. 证明 Newton 公式：

$$s_k-\sigma_1 s_{k-1}+\sigma_2 s_{k-2}+\cdots+(-1)^k\sigma_k s_0=0\ .$$

§3.5 局部化与完备化简介

概要: 局部化简介；从有理数构造实数.

为了使得环中的一些不可逆元素变得可逆，可以把环嵌入一个更大的环，这种思想方法称为 *局部化*; 最原始的重要模型就是从整数构造有理数.

为了使得在某种度量之下环 (域) 中 Cauchy 序列总有极限，也可以把环嵌入一个更大的环，这种思想方法称为 *完备化*; 最原始的重要模型就是从有理数构造实数.

本节简单介绍局部化的做法，简介从有理数构造实数的要点.

局部化简介

定义. 设 R 是整环. 如果子集 $S\subseteq R$ 满足：

(i) $1\in S$ 但 $0\notin S$; (ii) 若 $s_1,s_2\in S$ 则 $s_1s_2\in S$;

那么称 S 是整环 R 的一个 *乘闭子集*.

3.5.1 例. (1). 设 P 是整环 R 的理想. 则差集 $S=R-P$ 是乘闭子集当且仅当 P 是素理想. (习题 1.)

(2). 在 (1) 中取 $S=R-\{0\}$, 则 S 为乘闭子集.

设 R 是整环. 设 S 是 R 的乘闭子集.

令 $\mathcal{L}=\{\,(a,s)\mid a\in R,\ b\in S\,\}$. 在 $\mathcal{L}$ 上定义关系 (即是 "分数相等规则"):

$$(a,s)\sim(a',s')\qquad \text{如果}\quad as'=a's\ . \tag{$\sim$}$$

验证这是等价关系如下. 自反性、对称性显然成立. 若 $(a,s)\sim(a',a')$ 且 $(a',s')\sim(a'',s'')$, 即 $as'=a's$ 且 $a's''=a''s'$, 那么 $as's''=a'ss''=sa''s$, 即 $s'(as''-a''s)=0$. 由于 R 无零因子, $s'\neq 0$, 所以 $as''-a''s=0$, 即 $as''=a''s$; 得 $(a,s)\sim(a'',s'')$.

令 $S^{-1}R:=\mathcal{L}/\sim$, 是 $\mathcal{L}$ 关于等价关系 $\sim$ 的商集; 仿照 "分数"(fractions) 的记法，把 (a,s) 所在的等价类记作 $\dfrac{a}{s}$; 即

$$S^{-1}R:=\mathcal{L}/\sim=\left\{\frac{a}{s}\ \middle|\ (a,s)\in\mathcal{L}\right\}. \tag{L}$$

利用 R 的两个运算在集合 $S^{-1}R$ 上定义运算：

$$\frac{a}{s}+\frac{a'}{s'}\ =\ \frac{as'+a's}{ss'}\ ; \tag{$+$}$$

$$\frac{a}{s}\cdot\frac{a'}{s'} \;=\; \frac{aa'}{ss'}\,. \tag{$\bullet$}$$

需要验证运算定义与代表元选取无关. 设 $(a,b)\sim(b,t)$, $(a',s')\sim(b',t')$; 即 $\frac{a}{s}=\frac{b}{t}$, $\frac{a'}{s'}=\frac{b'}{t'}$, 那么 $at=bs$, $a't'=b's'$; 于是

$$\begin{aligned}(as'+a's)(tt') &= as'tt'+a'stt' = ats't'+a't'st = bss't'+b's'st\\ &= ss'bt'+ss'b't = ss'(bt'+b't)\,,\end{aligned}$$

即

$$\frac{as'+a's}{ss'}=\frac{bt'+b't}{tt'}\,;$$

加法的定义与代表元选取无关. 同理证明乘法的定义与代表元选取无关.

验证 $S^{-1}R$ 是一个交换幺环如下. $\frac{0}{1}$ 是 Q 的加法零元; 实际上 $\frac{a}{s}=\frac{0}{1}$ 当且仅当 $a=0$. 又 $-\frac{a}{b}=\frac{-a}{b}$. 而

$$\left(\frac{a}{s}+\frac{a'}{s'}\right)+\frac{a''}{s''}=\frac{as'+a's}{ss'}+\frac{a''}{s''}=\frac{as's''+a'ss''+a''ss'}{ss's''}$$

$$\frac{a}{s}+\left(\frac{a'}{s'}+\frac{a''}{s''}\right)=\frac{a}{s}+\frac{a's''+a''s'}{s's''}=\frac{as's''+a'ss''+a''ss'}{ss's''}$$

故

$$\left(\frac{a}{s}+\frac{a'}{s'}\right)+\frac{a''}{s''}=\frac{a}{s}+\left(\frac{a'}{s'}+\frac{a''}{s''}\right)\,;$$

即: 加法满足结合律. 类似地验证其他条件成立. 特别, $\frac{1}{1}$ 是乘法单位元. 如果 $\frac{a}{s}\cdot\frac{a'}{s'}=\frac{0}{1}$, 则 $aa'=0$; 由于 R 是整环, 故或者 $a=0$ 或者 $a'=0$; 即或者 $\frac{a}{s}=0$ 或者 $\frac{a'}{s'}=0$. 所以 $S^{-1}R$ 是整环.

最后, 把 R 嵌入 $S^{-1}R$ 作为 $S^{-1}R$ 的子环:

$$R\longrightarrow S^{-1}R,\quad a\longmapsto\frac{a}{1}\,,$$

由 $S^{-1}R$ 的运算定义, 易见这是幺环同态. 如果 $\frac{a}{1}=\frac{b}{1}$, 按等价关系定义 $(\sim)$, 得 $a=b$. 故这是单同态. 简记 $\frac{a}{1}=a$. 实际上对任 $s\in S$ 都有 $\frac{as}{s}=a$. 把 R 的元 a 等同于它在 $S^{-1}R$ 中的象 $a=\frac{a}{1}$, 可认为 $S^{-1}R$ 包含 R 为子环.

只要 $s\in S$, 在 $S^{-1}R$ 中有 $\frac{s}{1}\cdot\frac{1}{s}=1$. 即 s 在 $S^{-1}R$ 中可逆, $s^{-1}=\frac{1}{s}$.

3.5.2 结论. $(S^{-1}R,+,\cdot)$ 是一个包含 R 为子环而且 S 的每个元都可逆的整环. □

定义. 上述构造的整环 $S^{-1}R$ 称为整环 R 关于乘闭子集 S 的 局部化 *(localization)*.

3.5.3 定理 (局部化的泛性质). 设 R, S 和 $S^{-1}R$ 如上. 如果交换幺环 R' 和幺环同态 $f: R \to R'$ 使得任 $s \in S$ 的像 $f(s)$ 在 R' 中可逆, 则存在唯一幺环同态 $\tilde{f}: S^{-1}R \to S$ 使得 $\tilde{f}|_R = f$.

证明. 存在性：令

$$\tilde{f}: \quad S^{-1}R \longrightarrow R', \quad \frac{a}{s} \longmapsto f(a)f(s)^{-1};$$

若 $\dfrac{a'}{s'} = \dfrac{a}{s}$, 即 $as' = a's$, 那么 $f(a)f(s') = f(a')f(s)$, 故 $f(a')f(s')^{-1} = f(a)f(s)^{-1}$; 所以上述映射定义是合理的 (与代表元的选取无关). 易验证 $\tilde{f}$ 符合要求.

唯一性：设 $f': S^{-1}R \to R'$ 也是幺环同态且 $f'(a) = f(a)$, $\forall\, a \in R$. 那么

$$f'\left(\frac{a}{s}\right) f(s) = f'\left(\frac{a}{s}\right) f'(s) = f'\left(\frac{a}{s} \cdot s\right) = f'(a) = f(a)\,,$$

故 $f'\left(\dfrac{a}{s}\right) = f(a)f(s)^{-1} = \tilde{f}\left(\dfrac{a}{s}\right)$. 得 $f' = \tilde{f}$. □

取例 3.5.1(2) 中的 $S = R - \{0\}$, 则得推论如下.

3.5.4 推论. 设 R 是整环, $S = R - \{0\}$. 则 S 是乘闭子集, 且：

(1) 局部化 $S^{-1}R$ 是包含 R 为幺子环的域, 称为整环 R 的 商域 (quotient field). 或称整环 R 的 分式域 (fraction field).

(2) (分式域的泛性质). 如果交换幺环 R' 和幺环同态 $f: R \to R'$ 使得 R 的任何非零元 a 的像 $f(a)$ 在 R' 中可逆, 则存在唯一幺环同态 $\tilde{f}: S^{-1}R \to R'$ 使得 $\tilde{f}|_R = f$.

证. (1). 如果 $a/s \in S^{-1}R$, $a/s \neq 0$, 则 $a \neq 0$, 即 $a \in S$; 那么 $(a/s)\cdot(s/a) = 1$; 即 a/s 可逆. 所以 $S^{-1}R$ 是域.

(2). 即定理 3.5.3. □

例. 整数环的分式域是有理数域.

例. 域 $\mathbb{F}$ 的多项式环 $\mathbb{F}[x]$ 的分式域是域 $\mathbb{F}$ 的有理分式域

$$\mathbb{F}(x) = \{\, f(x)/g(x) \mid\ f(x), g(x) \in \mathbb{F}[x],\ g(x) \neq 0 \,\}\,.$$

从有理数域构造实数域

从有理数构造实数, 通常有 Dedekind 的分割法和 Cantor 的序列法. 这里简介序列法的要点.

现在从有理数开始. 记住：现在还没有实数, 只有有理数.

首先注意：有理数域 $\mathbb{Q}$ 上有 "正负性", 即有子集 $\mathbb{Q}^{(+)} \subseteq \mathbb{Q}$ 满足：

(P1) 对任 $a \in \mathbb{Q}$, 三者 $a \in \mathbb{Q}^{(+)}$, $a = 0$, $-a \in \mathbb{Q}^{(+)}$ 之一且仅一成立;

(P2) 对任 $a, b \in \mathbb{Q}^{(+)}$ 有 $a + b \in \mathbb{Q}^{(+)}$ 和 $ab \in \mathbb{Q}^{(+)}$.

只要有了这两条，就可以定义大小关系和绝对值. 更一般的论述如下.

3.5.5 定义. 设 $\mathbb{F}$ 是域，且有子集 $\mathbb{F}^{(+)} \subseteq \mathbb{F}$ 满足：

(P1) 对任 $a \in \mathbb{F}$, 三者 $a \in \mathbb{F}^{(+)}$, $a = 0$, $-a \in \mathbb{F}^{(+)}$ 之一且仅一成立;

(P2) 对任 $a, b \in \mathbb{F}^{(+)}$ 有 $a + b \in \mathbb{F}^{(+)}$ 和 $ab \in \mathbb{F}^{(+)}$;

就称 $\mathbb{F}$ 是 *有序域*; 若 $a \in \mathbb{F}^{(+)}$ 则称 a 是 $\mathbb{F}$ 的 *正元*; 若 $-a \in \mathbb{F}^{(+)}$ 则称 a 是 $\mathbb{F}$ 的 *负元*.

设 $\mathbb{F}$ 是有序域. 由 (P1), $\mathbb{F}$ 划分为不交并 $\mathbb{F} = \mathbb{F}^{(+)} \bigcup \{0\} \bigcup (-\mathbb{F}^{(+)})$, 其中 $-\mathbb{F}^{(+)} := \{-a \mid a \in \mathbb{F}^{(+)}\}$. 以下记 $\mathbb{F}^{+} = \mathbb{F}^{(+)} \bigcup \{0\}$. 那么 $\mathbb{F}^{+} \bigcap (-\mathbb{F}^{+}) = \{0\}$.

命题. *设 $\mathbb{F}$ 是有序域. 对任 $a, b \in \mathbb{F}$, 如果 $b - a \in \mathbb{F}^{+}$ 则记 $a \le b$. 则 "$\le$" 是 $\mathbb{F}$ 的全序关系.*

证. (1). 自反性： $a - a = 0 \in \mathbb{F}^{+}$, 即 $a \le a$.

反对称性:若 $a \le b$ 且 $b \le a$, 即 $b-a \in \mathbb{F}^{+}$ 且 $a-b \in \mathbb{F}^{+}$, 所以 $a-b \in \mathbb{F}^{+} \bigcap (-\mathbb{F}^{+}) = \{0\}$; 故 $a - b = 0$, 即 $a = b$.

传递性：若 $a \le b$ 且 $b \le c$, 即 $b - a \in \mathbb{F}^{+}$ 且 $c - b \in \mathbb{F}^{+}$, 由定义条件 (P2), 得 $c - a = (b - a) + (c - b) \in \mathbb{F}^{+}$; 故 $a \le c$. □

3.5.6 命题. *设 $\mathbb{F}$ 是有序域. 对任 $a \in \mathbb{F}$, 定义* $|a| = \begin{cases} a, & \text{若 } a \in \mathbb{F}^{+} \text{ (即 } a \ge 0\text{);} \\ -a, & \text{若 } -a \in \mathbb{F}^{(+)} \text{ (即 } a < 0\text{).} \end{cases}$

称 $|a|$ 为 a 的 绝对值. 则以下三条成立：

(V1) $|a| \ge 0$, $\forall\ a \in \mathbb{F}$, *且* $|a| = 0$ *当且仅当* $a = 0$;

(V2) (三角不等式) $|a + b| \le |a| + |b|$, $\forall\ a, b \in \mathbb{F}$;

(V3) $|ab| = |a| \cdot |b|$, $\forall\ a, b \in \mathbb{F}$.

证. 首先，按绝对值的定义有： $|-a| = |a|$.

对 (V1), 按绝对值即可验证.

对 (V2), 分别情况验证. 若 $a \ge 0$, $b \ge 0$, 则按绝对值定义， $|a| + |b| - |a + b| = a + b - (a + b) = 0 \in \mathbb{F}^{+}$, 所以 $|a + b| = |a| + |b|$; (V2) 中的等号成立当然 (V2) 成立.

若 $a \le 0$, $b \le 0$, 同上验证此时也是等号成立.

设 $a \ge 0$, $b \le 0$. 再分两种子情形. 子情形 1: $a + b \le 0$. 则因 $-a \le 0$, 由上面已证结论， $|b| = |(a + b) + (-a)| = |a + b| + |-a| = |a + b| + |a|$; 即 $|a + b| = |b| - |a|$; 所以 $|a| + |b| - |a + b| = |a| + |b| - (|b| - |a|) = 2|a| \in \mathbb{F}^{+}$; 得 $|a + b| \le |a| + |b|$.

子情形 2: $a + b \ge 0$. 可以类似地验证 (V2) 成立.

对 (V3), 如同对 (V2) 一样分情形逐一验证. □

3.5.7 注. 如果集合 A 到有序域 $\mathbb{F}$ 有二元函数 $d(a, a')$ 满足：

(D1) $d(a, a') \ge 0$, $\forall\ a, a' \in A$, 且仅当 $a = a'$ 时有 $d(a, a') = 0$;

(D2) $d(a, a') = d(a', a)$, $\forall\ a, a' \in A$;

(D3) $d(a, a') \le d(a, a'') + d(a'', a')$, $\forall\ a, a', a'' \in A$;

就称二元函数 d 是 A 的一个 *度量*, 称 (A,d) 是一个 *度量空间*.

从有序域 $\mathbb{F}$ 的绝对值函数可以定义一个度量 $d(a,a')=|a-a'|$ (证明作为习题 4), 称为有序域 $\mathbb{F}$ 的 *绝对值度量*.

现在开始从有理数构造实数. 记住：有理数域是有序域, 上面的一般理论对有理数域均成立. 下一个主角是无限序列及其极限. 无限序列 $a_1,a_2,\cdots$, 简称序列, 简记为 $\{a_n\}$.

定义. (1) 称一个有理数序列 $\{a_n\}$ 有极限 a(或说收敛于 a), 记作 $\lim\limits_{n\to\infty}a_n=a$ (或更简单地记作 $a_n\to a$), 如果对任正有理数 ε 存在正整数 N 使得对任 $n>N$ 有 $|a-a_n|<\varepsilon$.

(2) 称一个序列 $\{a_n\}$ 是无穷小序列如果 $\lim\limits_{n\to\infty}a_n=0$

(3) 称一个有理数序列 $\{a_n\}$ 是 Cauchy 序列如果对任正有理数 ε 存在正整数 N 使得对任 $m,n>N$ 有 $|a_m-a_n|<\varepsilon$.

第 1 步. 在全体有理数 Cauchy 序列的集合

$$\mathcal{R}=\left\{\text{有理数 Cauchy 序列 }\{a_n\}\right\}.$$

上定义关系：如果 "差序列" $\{a_n-b_n\}$ 是无穷小序列, 则记 $\{a_n\}\sim\{b_n\}$.

验证 "$\sim$" 是集合 $\mathcal{R}$ 上的等价关系如下. 自反性与对称性显然成立; 验证传递性时用到三角不等式：

$$|(a_n-c_n)|=|(a_n-b_n)+(b_n-c_n)|\le|(a_n-b_n)|+|(b_n-c_n)|\,.$$

记 $\{a_n\}$ 所在等价类为 $[a_n]$; 记商集为

$$R:=\mathcal{R}/\sim\ =\ \{\text{有理数 Cauchy 序列的等价类 }[a_n]\}\,.$$

以下我们将引用一些基本知识, 它们都可通过简单的 ε-N 推理予以证明：

- 一个有理序列如果收敛于有理数则它一定是 Cauchy 序列; 但有理数 Cauchy 序列在有理数范围不一定有极限.
- 如果 $\lim\limits_{n\to\infty}a_n=a$, 而 $\{a_n\}\sim\{b_n\}$, 则 $\lim\limits_{n\to\infty}b_n=a$; 特别, 若 $b_n\ne0$, $n=1,2,\cdots$, 则 $a_n/b_n\to1$.
- 若 $\{a_n\}$ 是 Cauchy 序列, 则它的任意子序列 $\{a_{i_n}\}$ 也是 Cauchy 序列, 且 $\{a_{i_n}\}\sim\{a_n\}$.
- 任何 Cauchy 序列 $\{a_n\}$ 是整体有界的, 即：存在有理数 $L<U$ 使得 $L<a_n<U$, $\forall\ n=1,2,\cdots$.

3.5.8 引理. *如果有理数 Cauchy 序列 $\{a_n\}\not\sim\{0\}$, 则存在正有理数 q 和正整数 n_0 使得以下之一且仅一成立：*

(1) *所有 $a_{n_0+i}>q,\ \ i=0,1,\cdots$;*

(2) *所有 $a_{n_0+i}<-q,\ \ i=0,1,\cdots$.*

定义. 若所有 $a_{n_0+i} > q$ 则称 $[a_n]$ 是正类，记作 $[a_n] > [0]$. 若所有 $a_{n_0+i} < -q$ 则称 $[a_n]$ 是负类，记作 $[a_n] < [0]$.

证. 由于 a_n 不收敛于 0, 故存在有理数 $\varepsilon_0 > 0$ 使得对任正整数 N 都存在 $n > N$ 使得 $|a_n| = |a_n - 0| \geq \varepsilon_0$.

由于 $\{a_n\}$ 是 Cauchy 序列，对于正有理数 $\varepsilon_0/2$ 存在正整数 N_0 使得对任 $m, n > N_0$ 都有 $|a_m - a_n| < \varepsilon_0/2$. 但由上段结论，对这个 N_0, 存在 $n_0 > N_0$ 使得 $|a_{n_0}| \geq \varepsilon_0$.

现在取 $q = \varepsilon_0/2$, 则 $a_{n_0} \geq 2q$ 或 $a_{n_0} \leq -2q$.

而对任 $n > n_0$ 都有 $|a_n - a_{n_0}| < \varepsilon_0/2 = q$, 即 $a_{n_0} - q < a_n < a_{n_0} + q$.

所以对任 $n > n_0$ 都有：

— 当 $a_{n_0} \geq 2q$ 时， $a_n > a_{n_0} - q \geq q$;

— 当 $a_{n_0} \leq -2q$ 时， $a_n < a_{n_0} + q \leq -q$. □

第 2 步. 在商集 R 上定义运算使之成为域：

$$[a_n] + [b_n] = [a_n + b_n]\ ; \tag{+}$$

$$[a_n] \cdot [b_n] = [a_n b_n]\ ; \tag{•}$$

需验证运算定义与代表元选取无关. 这里验证乘法定义合理：若 $\{a'_n\} \sim \{a_n\}$, $\{b'_n\} \sim \{b_n\}$, 则

$$\begin{aligned} |a'_n b'_n - a_n b_n| &= |a'_n b'_n - a'_n b_n + a'_n b_n - a_n b_n| \\ &\leq |a'_n b'_n - a'_n b_n| + |a'_n b_n - a_n b_n| \\ &= |a'_n| \cdot |b'_n - b_n| + |a'_n - a_n| \cdot |b_n|\ ; \end{aligned}$$

论证中用到 (V2),(V3) 两条. 那么易见 $a'_n b'_n - a_n b_n \to 0$. 所以 $\{a'_n b'_n\} \sim \{a_n b_n\}$.

容易验证加法满足结合律和交换律，零序列的等价类 $[0]$ (即所有无穷小序列的集合) 是零元，简记 $0 = [0]$; $[-a_n]$ 是 $[a_n]$ 的负元，即 $-[a_n] = [-a_n]$.

还易验证乘法满足结合律，满足对加法的分配律；序列 $1, 1, 1, \cdots$. 的等价类 $[1]$ 是单位元.

最后，设 $[a_n] \neq [0]$, 由引理 3.5.8, 存在有理数 $q > 0$ 和子序列 a_{i_n}, $n = 1, 2, \cdots$ 使得所有 a_{i_n} 同号且 $|a_{i_n}| > q$; 由于 $\{a_{i_n}\} \sim \{a_n\}$. 所以可取代表序列 $\{b_n\}$ 使得 $[b_n] = [a_n]$, 但每 b_n 同号且 $|b_n| > q$. 那么

$$|b_m^{-1} - b_n^{-1}| = \frac{|b_n - b_m|}{|b_n| \cdot |b_m|} < \frac{|b_n - b_m|}{q^2}\ ,$$

计算中用到 (V3); 所以 $b_1^{-1}, b_2^{-1}, \cdots$ 也是 Cauchy 序列. 显然 $[b_n^{-1}][b_n] = [b_n^{-1} b_n] = [1]$. 即 $[b_n^{-1}]$ 是 $[b_n] = [a_n]$ 的逆元.

结论. $(R, +, \cdot)$ 是一个域.

第 3 步. 验证 R 构成一个有序域.

按引理 3.5.8 后的定义, 记 $R^{(+)} = \{\,[a_n] \mid [a_n] \text{ 是正类}\}$. 按引理 3.5.8, 定义 3.5.5 中的 (P1) 成立. 再按 R 中的运算定义 (+) 和 (•), 可知 (P2) 成立. 所以 R 是一个有序域.

那么由命题 3.5.6 及注 3.5.7, R 中大小关系, 绝对值都可定义. 因此序列极限, Cauchy 序列等都可定义; 子集的稠密性也可定义.

第 4 步. 把 $\mathbb{Q}$ 嵌入 R, 即构造单射 $\mathbb{Q} \to R$ 使得运算和序关系都得到保持.

对任 $a \in \mathbb{Q}$, 常值序列 $a, a, \cdots$, 记作 $\{\underline{a}\}$, 是 Cauchy 序列, 为避免混淆记此常值序列等价类为 $[\underline{a}]$, 即 $[\underline{a}] \in R$. 映射 $\mathbb{Q} \to R$, $a \mapsto [\underline{a}]$, 显然是单射; 而且显然保持加法和乘法; 正有理数映射为正序列, 负有理数映射为负序列; 所以保持序关系.

把有理数 a 等同于常值序列 $\{\underline{a}\}$ 的等价类 $[\underline{a}]$, 以下认为 $\mathbb{Q} \subseteq R$.

3.5.9 定理. *记号如上. 则 $\mathbb{Q}$ 在 R 中稠密, 任何有理数 Cauchy 序列在 R 中有极限.*

证. 先证稠密性. 设 $[a_n] \in R$, 设 r 是任意正有理数. 要证明存在有理数 q 满足 $|[\underline{q}] - [a_n]| < [\underline{r}]$, 这里 $[\underline{q}]$ 是常值序列 $q, q, \cdots$ 的等价类, $[\underline{r}]$ 是同样含义. 由于 $a_1, a_2, \cdots$ 是有理 Cauchy 序列, 故存在正整数 N 使得

$$|a_m - a_n| < r\ , \qquad \forall\ m, n \geq N\ .$$

取 $q = a_N$, 考虑常值序列 $q, q, \cdots$ 的等价类 $[\underline{q}]$. 由上式, 差序列 $q - a_1,\ \cdots,\ q - a_N,\ \cdots$ 的绝对值序列

$$|q - a_1|,\ \cdots,\ |q - a_N|,\ |q - a_{N+1}|,\ \cdots$$

的从第 N 项 $|q - a_N|$ 开始的子序列都满足

$$|q - a_n| < r\ , \qquad \forall\ n \geq N\ ;$$

注意, 序列 $a_1, a_2, \cdots, a_N, a_{N+1}, \cdots$ 与其子序列 $a_N, a_{N+1}, \cdots$ 等价, 所以 $|[\underline{q}] - [a_n]| < r$.

再证明有理数 Cauchy 序列 $a_1, a_2, \cdots$ 在 R 中有极限. 每 a_i 是有理数, 在 R 中就是常值序列 $a_i, a_i, \cdots$ 所在等价类; 同上, 为避免混淆记此常值序列等价类为 $[\underline{a_i}]$; 所以有理数 Cauchy 序列 $a_1, a_2, \cdots$ 在 R 中就写为等价类序列 $[\underline{a_1}],\ [\underline{a_2}],\ \cdots$.

又, 在 R 中, 为避免混淆记序列 $a_1, a_2, \cdots$ 所在等价类为 $[a_1, a_2, \cdots]$. 对任正有理数 ε, 由于 $a_1, a_2, \cdots$ 是 Cauchy 序列, 存在正整数 N 使得

$$|a_m - a_n| < \varepsilon\ , \qquad \forall\ m, n \geq N\ . \tag{A}$$

那么在 R 中, 对任 $n > N$ 计算 $|[a_1, a_2, \cdots] - [\underline{a_i}]|$ 就是计算差序列的绝对值序列:

$$|a_1 - a_i|,\ |a_2 - a_i|,\ \cdots,\ |a_N - a_i|,\ |a_{N+1} - a_i|,\ \cdots$$

由 (A) 式, 这个序列第 N 项以后的子序列每项都 $< \varepsilon$, 所以作为序列等价类之差有

$$|[a_1, a_2, \cdots] - [\underline{a_i}]| < [\underline{\varepsilon}]\ .$$

按定义，得 $\lim\limits_{i\to\infty}[\underline{a_i}]=[a_1,a_2,\cdots]$. □

定义. (1). 若度量空间 (X,d) 的任何 Cauchy 序列有极限，就称 X 是 *完备空间*.
(2). 若有序域 $\mathbb{F}$ 关于绝对值度量是完备的，就称 $\mathbb{F}$ 是 *完备域*.

作为一般拓扑的基本知识，有

引理. *如果度量空间 (X,d) 的稠密子集 Y 的任何 Cauchy 序列在 X 中有极限，那么 X 是完备空间.*

证. 设 $x_1,x_2,\cdots$ 是 X 的 Cauchy 序列. 由 Y 的稠密性，对任 x_n 存在 $y_n\in Y$ 使得

$$d(y_n,x_n)<2^{-n}\,,\qquad n=1,2,\cdots\,. \tag{D}$$

对任有理数 $\varepsilon>0$, 有正整数 N_1 使得

$$2^{-n}<\varepsilon/3\,,\qquad \forall\, n>N_1\,;$$

由于 $x_1,x_2,\cdots$ 是 Cauchy 序列，存在正整数 N_2 使得

$$d(x_m,x_n)<\varepsilon/3\,,\qquad \forall\, n>N_2\,.$$

取 $N=\max(N_1,N_2)$, 那么对任 $m,n>N$ 有

$$\begin{aligned} d(y_m,y_n) &\le d(y_m,x_m)+d(x_m,x_n)+d(x_n,y_n)\\ &< 2^{-m}+\varepsilon/3+2^{-n}<\varepsilon/3+\varepsilon/3+\varepsilon/3=\varepsilon\,. \end{aligned}$$

所以 $y_1,y_2,\cdots$ 是 Cauchy 序列. 由条件，存在 $x_0\in X$ 使得 $\lim\limits_{n\to\infty}y_n=x_0$. 再由 (D) 式，即得 $\lim\limits_{n\to\infty}x_n=x_0$. □

于是从定理 3.5.9 马上有推论：

推论. *定理 3.5.9 中的 R 是完备域.* □

注. 这个 R 称为 $\mathbb{Q}$ 的关于绝对值 $|a|$ 的 *完备化*. 它就是实数域.
完备化也具有类似于定理 3.5.3 的泛性质.

习题 3.5

1. 设 P 是整环 R 的理想. 则差集 $S=R-P$ 是乘闭子集当且仅当 P 是素理想.

2. 取 $R=\mathbb{Z}$, p 为一个素数. 令 $S=\mathbb{Z}-p\mathbb{Z}$. 求 $S^{-1}\mathbb{Z}$.

3. 设 S 是整环 R 的乘闭子集. 如果 S 中的元都是 R 的可逆元，则 $S^{-1}R=R$.

4. 设 $\mathbb{F}$ 是一个有序域. 对任 $a,b\in\mathbb{F}$, 定义 $d(a,b)=|a-b|$. 证明： $d(a,b)$ 是 $\mathbb{F}$ 的一个度量.

5. $d = k+t_1\cdot 10^{-1}+t_2\cdot 10^{-2}+\cdots+t_n\cdot 10^{-n}$, 其中 $k\in\mathbb{Z}$ 而每 $t_i\in\{0,1,2,3,4,5,6,7,8,9\}$, 称为 n- 位十进小数, k 称为 d 的整数部分.

有理数序列 $d_1, d_2, \cdots, d_n, \cdots$, 称为十进小数序列如果任第 n 项 d_n 恰是 n- 位十进小数, 而且任 d_{n+1} (它是 $n+1$ 位十进小数) 的前 n 位与 d_n 完全相同, 即 $0\le d_{n+1}-d_n<10^{-n}$. (注：一个十进小数序列就是一个十进无限小数.)

记号同 3.5.9. 证明：

(1) 十进小数序列 $\{d_n\}$ 是 Cauchy 序列.

(2) 两个十进小数序列 $\{d_n\}\sim\{d'_n\}$ 当且仅当 $d_n=d'_n$, $n=1,2,\cdots$.

(3) 任一等价类 $\alpha\in R$ 含有序列 $\{a_n\}$ 满足 $a_1\le a_2\le\cdots$.

(4) 任一等价类 $\alpha\in R$ 含有唯一一个十进小数序列 (就是实数 α 的十进小数表示).

§3.6 整环的整除理论

概要: 整除相关概念；因子分解整环的性质；因子分解整环判断条件；主理想整环.

整数环 $\mathbb{Z}$, 和域 $\mathbb{F}$ 上的多项式环 $\mathbb{F}[x]$, 是能做因子分解的整环. 这里把它们的整除理论推广到一般整环. 所得结论是：在一定条件下, 因子分解定理成立.

本节始终设 R 是一个整环.

可逆元也称为 *单位 (unit)*. R 的可逆元乘群 $R^\times$ 以下述方式作用在集合 R 上：

$$R^\times\times R\longrightarrow R\,,\quad (u,r)\mapsto ur\,.$$

在此作用下的 $R^\times$- 可迁关系 $r\sim s$ 称为 *相伴关系*, R 被划分的轨道称为 *相伴类*.

例. 所有可逆元 $R^\times$ 是一个相伴类. $\{0\}$ 是一个相伴类.

对任 $0\ne a\in R$, a 所在的相伴类 $[a]=R^\times a=\{\,ua\mid u\in R^\times\,\}$.

设 $a,b,c\in R$. 如果 $a=bc$, 那么称 a 是 b 的 *倍元*, 称 b 是 a 的 *约元*; 也称 a 被 b 整除, 称 b 整除 a, 记作 $b\,|\,a$.

整除、相伴的有关性质. *在整环 R 中：*

(1) 整除关系 "$b|a$" 满足自反性和传递性. (但不满足对称性, 见下面 (4).)

(2) 如果 $f\,|\,\tilde f$, $g\,|\,\tilde g$, 则 $fg\,|\,\tilde f\tilde g$.

(3) 如果 $f|g$ 且 $f'\sim f$ 和 $g'\sim g$, 则 $f'|g'$.

(4) $f\sim g$ 当且仅当 $f|g$ 且 $g|f$.

证. 都按定义直接验证. □

注. 上述 (3) 说明整除关系是相伴类集合上的关系. 所以倍元、约元等等也都是关于相伴类的概念.

显然, 0 是任何元的倍元, 不是任何元的约元.

另一方面，一个可逆元仅以可逆元为约元，没有其它约元.

任何非零不可逆元 a 至少有两类约元：可逆元、与 a 相伴的元； a 的其它约元称为*真约元*.

3.6.1 定义. 设 $a \in R$ 是非零的不可逆元.

(1) 如果只要 $b|a$ 就必有 b 或者可逆或者与 a 相伴 (即 a 没有真约元), 就称 a 为 *不可约元 (irreducible element)*, 或称 *既约元*. 否则称 a 为 *可约元 (reducible element)*.

(2) 如果只要 $a|(bc)$ 就必有或者 $a|b$ 或者 $a|c$, 就称 a 为 *素元* (prime element).

引理. *素元必为不可约元.*

证. 设 $p \in R$ 是素元. 若 $p = bc$, 那么或者 $p|b$ 或者 $p|c$; 由上述性质， $p|b$ 时 $p \sim b$, 有 $u \in R^\times$ 使得 $p = bu = bc$, 消去 b 得 $c = u$ 是可逆元；同理 $p|c$ 时得 b 是可逆元. 所以 p 是不可约元. □

注. 不可约元不必为素元，见习题 1.

几乎所有整除概念可以用主理想概念表达.

3.6.2 命题. (1) $a \in R^\times \iff Ra = R$.

(2) $a \sim b \iff Ra = Rb$.

(3) $b \,|\, a \iff a \in Rb \iff Ra \subseteq Rb$.

(4) *b 是 a 的真约元* $\iff Ra \subsetneqq Rb \subsetneqq R$.

(5) *a 是不可约元* $\iff Ra$ *是 R 的极大的主理想.*

(6) *a 是素元* $\iff Ra$ *是 R 的非零素理想.*

证. 习题 □

推论. *主理想整环的非零素理想是极大理想.* □

以下讨论三类重要的整环：欧氏环、主理想整环、因子分解环.

前两类已在 §3.2 介绍过，而且已经知道： *欧氏环必为主理想整环*. 重要例子：整数环 $\mathbb{Z}$ ，域 $\mathbb{F}$ 上的多项式环 $\mathbb{F}[x]$ 都是欧氏环，故也都是主理想整环.

3.6.3 定义. 称 R 是 *因子分解整环* 如果 R 的任何非零的不可逆元 a 满足以下两条：

因子分解存在性. a 可以写成不可约元之积，即可写 $a = p_1 p_2 \cdots p_n$, 其中每个 p_i 都是不可约元.

因子分解唯一性: 如果还可写 $a = q_1 q_2 \cdots q_m$ 其中 q_i 都是不可约元，则 $m = n$, 且适当重标号后有 $q_i \sim p_i$, $i = 1, \cdots, n$.

此时我们称 $a = p_1 p_2 \cdots p_n$, 其中每 p_i 都是不可约元，为 a 的 *不可约分解*, 称 p_i 是 a 的不可约因子，称 n 为 *分解长度*.

3.6.4 引理. *设 R 是因子分解整环， a 是 R 的非零不可逆元， $a = p_1 p_2 \cdots p_n$ 是不可约分解. 则 a 的任何约元 b 相伴于一些不可约因子之积： $b \sim p_{i_1} \cdots p_{i_s}$; 特别是，在相伴意义下 a 只有有限个约元.*

证. 因为 b 是 a 的约元, 故 $a = bc$. 而 b, c 有不可约分解式 $b = q_1 \cdots q_s$, $c = q'_1 \cdots q'_{s'}$; 所以 $a = bc = q_1 \cdots q_s q'_1 \cdots q'_{s'}$ 也是 a 的不可约分解. 由因子分解唯一性, 存在 $p_{i_1}, \cdots, p_{i_s}$ 使得 $q_j \sim p_{i_j}$, $j = 1, \cdots, s$. 所以 $b = q_1 \cdots q_s \sim p_{i_1} \cdots p_{i_s}$. □

注. 对上述 a 的不可约分解 $a = p_1 p_2 \cdots p_n$ 做一技术处理: 不妨设 $p_1, \cdots, p_r$ 是分解式中出现的所有彼此不相伴的不可约因子; 把与 p_1 相伴的不可约因子表写为 p_1 与可逆元之积, 把与 p_2 相伴的不可约因子表写为 p_2 与可逆元之积, 等等. 就可以把分解式写成:

$$a = u p_1^{m_1} \cdots p_r^{m_r}, \quad u \in R^\times, \quad m_i > 0, \quad p_1, \cdots, p_r \text{ 是两两不相伴不可约元;}$$

称为 a 的 *标准分解式*. 那么上引理就是说: 对 a 的任意约元 b 存在整数 t_i 使得

$$b \ \sim \ p_1^{t_1} \cdots p_r^{t_r} \ , \qquad 0 \le t_i \le m_i \ , \quad i = 1, \cdots, r.$$

3.6.5 定理. *设 R 是因子分解整环. 则以下各条成立:*

(1) 因子链条件: *R 没有 无限长的真约元序列: $a_1,\ a_2,\ \cdots$, 其中任 a_i 是前项 a_{i-1} 的真约元.*

(2) 素元条件: *R 的不可约元必为素元;*

(3) 最大公因子条件: *R 的任意两个元素的最大公因子存在.*

证. (1). 假若存在无限长的真约元序列: $a_1,\ a_2,\ \cdots$. 首先可设 $a_1 \neq 0$, 否则去掉 a_1 仍然是无限长的真约元序列. 同理可设 a_1 不可逆. 那么 $a_1, a_2, \cdots$, 都是 a_1 的约元而且彼此不相伴; 于是相伴意义下 a 有无数个约元. 与引理 3.6.4 相矛盾.

(2). 设 p 是不可约元; 证明它是素元. 设 $p \,|\, ab$. 而 a, b 有不可约分解式 $a = p_1 \cdots p_s$, $b = p'_1 \cdots p'_{s'}$, 得到 ab 的不可约分解式 $ab = p_1 \cdots p_s p'_1 \cdots p'_{s'}$. 由引理 3.6.4, p 相伴于其中某个不可约因子; 若 $p \sim p_i$, 则 $p \,|\, a$; 若 $p \sim p'_i$, 则 $p \,|\, b$. 所以 p 是素元.

(3). 设 $a,\ b \in R$. 如果 $a = 0$, 则 $\gcd(a, b) \sim b$. 如果 $a \in R^\times$, 则 a 只以自己的相伴元为约元, 故 $\gcd(a, b) = 1$. 下设 a, b 都是非零不可约元. 那么由 3.6.4 后的注解, 有两两不相伴的不可约元 $p_1, \cdots, p_k$ 使得

$$\begin{aligned} a &= u p_1^{m_1} \cdots p_k^{m_k} \ , \qquad u \in R^\times, \quad m_i \ge 0, \quad i = 1, \cdots, k \ ; \\ b &= v p_1^{n_1} \cdots p_k^{n_k} \ , \qquad v \in R^\times, \quad n_i \ge 0, \quad i = 1, \cdots, k \ . \end{aligned}$$

其中 $m_i \ge 0$ 是因为我们这里取的 p_i 有可能不在 a 的分解式中出现而只在 b 的分解式中出现. 对 $n_i \ge 0$ 是同样的原因. 那么由 3.6.4,

$$d = p_1^{s_1} \cdots p_k^{s_k} \ , \qquad s_i = \min\{m_i, n_i\}, \quad i = 1, \cdots, k \ ,$$

是 a, b 的公因子; 而且对 a, b 的任公因子 c 有

$$c \ \sim \ p_1^{t_1} \cdots p_k^{t_k} \ , \qquad 0 \le t_i \le m_i \text{ 且 } 0 \le t_i \le n_i, \quad i = 1, \cdots, k \ ;$$

也就是 $0 \le t_i \le s_i$, $i = 1, \cdots, k$, 因而 $c|d$. 故 d 是 a, b 的最大公因子. □

作为判断整环是否为因子分解整环的充分条件则不需要三个条件.

3.6.6 定理. *如果整环 R 满足因子链条件和素元条件则 R 是因子分解整环.*

证. 先证明因子分解存在性. 如果存在非零不可逆元 a 其因子分解不存在, 则 a 可约 (否则 $a = a$ 就是不可约分解), 即 $a = a_1 a_1'$ 使得 a_1, a_1' 都是 a 的真约元 (即都不是可逆元), 而且 a_1, a_1' 中至少一个的因子分解不存在 (否则把 a_1 和 a_1' 的不可约分解合起来就得到了 a 的不可约分解). 不妨设 a_1' 的因子分解不存在.

那么 $a_1' = a_2 a_2'$ 其中 a_2, a_2' 都是不可逆元, 而且. a_2, a_2' 中至少一个的因子分解不存在. 不妨设 a_2' 的因子分解不存在.

以此递推, 得到真约元的无限序列 $a,\ a_1,\ a_2,\ \cdots$, 与条件矛盾.

再证明因子分解唯一性. 设 $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, 其中所有 p_i 所有 q_j 都是不可约元. 那么 $p_1 \,|\, q_1 q_2 \cdots q_m$. 而由条件, p_1 是素元, 故存在某 q_j 被 p_1 整除, 适当重编号后可设 $p_1 | q_1$. 由 q_1 的不可约性, $p_1 \sim q_1$, 即 $q_1 = u p_1$, $u \in R^\times$. 那么 $p_1 p_2 \cdots p_n = u p_1 q_2 \cdots q_m$, 消去 p_1 得: $p_2 p_2 \cdots p_n = q_2' q_3 \cdots q_m$, 其中 $q_2' = u q_2$ 仍为不可约元. 按对不可约分解的长度归纳, 得 $m - 1 = n - 1$, 即 $m = n$, 而且, 适当重编号, 有 $p_2 \sim q_2' \sim q_2$, $p_3 \sim q_3$, $\cdots$, $p_n \sim q_n$. □

3.6.7 推论. *主理想整环是因子分解整环.*

证. 设 R 是主理想整环. 只需证明 R 满足因子链条件和素元条件.

若因子链条件不满足, 则 R 有无限长真约元序列 $a_1,\ a_2,\ a_3,\ \cdots$; 于是

$$Ra_1 \subsetneqq Ra_2 \subsetneqq Ra_3 \subsetneqq \cdots$$

是理想的无限严格升链, 易见并集 $I = \bigcup_{i=1}^{\infty} Ra_i$ 是 R 的一个理想, 所以可以由一个元 a 生成: $I = Ra$; 那么存在指标 k 使得 $a \in Ra_k$. 于是对任何 $n \ge k$ 有

$$Ra_n \subseteq Ra \subseteq Ra_k \subseteq Ra_n\ ;$$

即 $Ra_n = Ra_k$. 与上述序列是严格升链相矛盾.

设 $p \in R$ 是不可约元, 那么 Rp 是 R 的极大主理想; 但是 R 的所有理想都是主理想, 所以 Rp 是 R 的极大理想, 因此也是 R 的素理想. 故 p 是 R 的素元. □

所以, 欧氏环是主理想整环; 主理想整环是因子分解整环.

但这两个断言的逆命题都不成立.

例. $\mathbb{Z}[x]$ 是因子分解整环, 但不是主理想整环.

证. 下节定理表明它是因子分解环. $\mathbb{Z}[x]$ 中由元 x 和 2 生成的理想 $I = \mathbb{Z}x + 2\mathbb{Z} = \{\, f(x) \in \mathbb{Z}[x] \mid f(x) \text{ 的常数项是偶数} \,\}$ 不是主理想; 反证如下: 若 $I = \Big(g(x)\Big) =$

$\{\, g(x)f(x) \mid f(x) \in \mathbb{Z}[x] \,\}$, 那么由 $2 \in I$ 知存在整多项式 $f(x)$ 使得 $g(x)f(x) = 2$, 故只能是 $g(x) = 2$, 但 $x \in I$, 故有整多项式 $h(x)$ 使得 $x = 2h(x)$; 但这是不可能的. □

例. 在整环 $\mathbb{Z}[\sqrt{-5}] = \{\, a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \,\}$ 中不可约分解存在但分解不唯一; 如 $(3 + \sqrt{-5})(3 - \sqrt{-5}) = 9 = 3 \cdot 3$. (习题 1.)

习题 3.6

1. 在整环 $R = \{\, a + b\sqrt{-5} \mid a, b \in \mathbb{Q} \,\}$ 中, 证明:

(1) 3 是不可约元, 但不是素元 $(3|(2 + \sqrt{-5})(2 - \sqrt{-5}))$.

(2) $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ 是两个不可约分解.

2. (1) 求 Gauss 整数环 $\mathbb{Z}[\mathbf{i}]$ 中的所有可逆元.

(2) 求 Gauss 整数环 $\mathbb{Z}[\mathbf{i}]$ 中的所有不可约元.

3. 证明命题 3.6.2.

4. 在整环 R 中, 称 b 为 $a_1, \cdots, a_n$ 的公倍子如果 b 是每个 a_i 的倍元; 称 m 为 $a_1, \cdots, a_n$ 的最小公倍子如果 m 是 $a_1, \cdots, a_n$ 的公倍子而且只要 b 是 $a_1, \cdots, a_n$ 的公倍子就有 $m|b$.

(1) 证明: 因子分解整环 R 中任意两个元素的最小公倍子存在.

(2) 进而证明: 因子分解整环 R 中任意 $n > 2$ 个元素的最小公倍子存在.

5. 举例说明因子分解整环的子环不必为因子分解整环.

6. 设 R 是主理想整环, $0 \neq a \in R$. 证明 R 只有有限个理想包含 a.

7. 设 R 和 $\delta : R - \{0\} \to \mathbb{Z}^+$ 是欧氏整环. 证明:

(1) $\delta(1) = \min\{\, \delta(a) \mid 0 \neq a \in R \,\}$;

(2) $u \in R$ 是可逆元当且仅当 $\delta(u) = \delta(1)$;

(3) 设 $v \in R$ 使得 $\delta(v) = \min\{\, \delta(a) \mid 0 \neq a \in R - R^\times \,\}$, 则 R/Rv 是域, 从而 v 是不可约元.

8. 如果整环 R 满足因子链条件和最大公因子条件则 R 是因子分解整环.

§3.7 整系数多项式环

概要: 因子分解整环上的多项式环是因子分解整环.

本节证明关于因子分解整环的一个重要定理.

3.7.1 定理. 因子分解整环 R 上的多项式环 $R[x]$ 是因子分解整环.

3.7.2 推论. 域 $\mathbb{F}$ 上的 n 元多项式环 $\mathbb{F}[x_1, \cdots, x_n]$ 是因子分解整环.

为便于理解证明过程, 以下证明: $\mathbb{Z}[x]$ 是因子分解整环. 上述一般定理的证明是完全一样的, 只需把证明中的 $\mathbb{Z}$ 换为因子分解整环 R, 把 $\mathbb{Q}$ 换为 R 的分式域 Q 即可.

定义. 如果 $f(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}[x]$, $\deg f(x)>0$, 的系数互素,即 $\gcd(a_0,a_1,\cdots,a_n)=1$, 称 $f(x)$ 为 本原多项式.

高斯引理. 两非常数整系数多项式之积是本原多项式当且仅当两多项式都是本原多项式.

证. 设 $f(x)=\sum_{i=0}^{n}a_ix^i,\ g(x)=\sum_{j=0}^{m}b_jx^j\in\mathbb{Z}[x]$, $\deg f(x),\deg g(x)>0$.

如果 $f(x)$, $g(x)$ 之一不是本原多项式, 如 $f(x)$ 不是本原多项式, 则存在素元 $p\in\mathbb{Z}$ 使得 $p\,|\,a_i$, $i=0,1,\cdots,n$; 那么 p 整除乘积多项式 $f(x)g(x)$ 的所有系数, 因而 $f(x)g(x)$ 不是本原多项式.

再设 $f(x)$, $g(x)$ 都是本原多项式. 假若乘积多项式 $f(x)g(x)$ 不是本原多项式, 则存在素元 $p\in\mathbb{Z}$ 使得 p 整除 $f(x)g(x)$ 的所有系数. 但 p 不整除所有 a_i. 设 a_s 是不被 p 整除的最小标号系数, 即 $p\,|\,a_i$, $i=0,1,\cdots,s-1$, 但 $p\nmid a_s$. 同理, 有 b_t 使得 $p\,|\,b_j$, $j=0,1,\cdots,t-1$, 但 $p\nmid b_t$. 那么乘积多项式 $f(x)g(x)=\sum_{k=0}^{m+n}x^k\sum_{i+j=k}$ 中的 x^{s+t} 的系数

$$a_0b_{s+t}+a_1b_{s+t-1}+\cdots+a_{s-1}b_{t+1}+a_sb_t+a_{s+1}b_{t-1}+\cdots+a_{s+t-1}b_1+a_{s+t}b_0\ ,$$

它被 p 整除, 它的表达式中除 a_sb_t 以外, 其他各项被 p 整除, 故该项 a_sb_t 被 p 整除; 但 p 是 $\mathbb{Z}$ 的素元, 所以或者 $p\mid a_s$ 或者 $p\mid b_t$; 这与 a_s 和 b_t 的选取矛盾. □

引理. (1) $\mathbb{Z}[x]$ 的可逆元乘群 $(\mathbb{Z}[x])^\times=\mathbb{Z}^\times=\{\pm1\}$.

(2) $\mathbb{Z}[x]$ 的本原多项式的相伴多项式还是本原多项式.

证. (1). 设 $f(x)g(x)=1$; 因为 $\mathbb{Z}[x]$ 是整环, 故

$$\deg f(x)+\deg g(x)=\deg\left(f(x)\cdot g(x)\right)=\deg 1=0\ ;$$

因此 $\deg f(x)=\deg g(x)=0$, 即 $f(x)$ 与 $g(x)$ 都是非零常数多项式. $\mathbb{Z}$ 中两非零元之积等于 1, 所以只能是 $f(x)\in\mathbb{Z}^\times=\{\pm1\}$.

(2). 如果 $f(x)=\sum_{i=0}^{n}a_ix^i$ 是本原多项式, 与 $f(x)$ 相伴的多项式是 $\varepsilon f(x)=\sum_{i=0}^{n}(\varepsilon a_i)x^i$ 其中 $\varepsilon\in(\mathbb{Z}[x])^\times=\{\pm1\}$; 而

$$\gcd(\varepsilon a_0,\varepsilon a_1,\cdots,\varepsilon a_n)=\gcd(a_0,a_1,\cdots,a_n)=1\ ;$$

即 $\varepsilon f(x)$ 是本原多项式. □

把 $\mathbb{Z}[x]$ 放到 $\mathbb{Q}[x]$ 中来考虑. $\mathbb{Z}[x]$ 的元简称 $\mathbb{Z}$- 多项式, $\mathbb{Q}[x]$ 的元简称 $\mathbb{Q}$- 多项式.

引理. 对任 $f(x)\in\mathbb{Q}[x]$, $\deg f(x)>0$, 存在本原 $\mathbb{Z}$- 多项式 $f^*(x)\in\mathbb{Z}[x]$ 和 $\frac{d}{c}\in\mathbb{Q}$ 使得 $f(x)=\frac{d}{c}\cdot f^*(x)$; 这种本原 $\mathbb{Z}$- 多项式 $f^*(x)$ 在相伴意义下唯一.

证. 存在性. 把 $f(x)$ 的各系数写成分母相同的分数:

$$f(x)=\sum_{i=0}^{n}\frac{d_i}{c}x^i\in\mathbb{Q}[x]=\frac{1}{c}\cdot\sum_{i=0}^{n}d_ix^i\ ;$$

再令 $d=\gcd(d_0,d_1,\cdots,d_n)$; 令 $d_i^*=d_i/d$, $i=0,1,\cdots,n$; 那么 $f^*(x):=\sum_{i=0}^n d_i^*x^i$ 是整系数多项式且各系数的最大公因子

$$\gcd(d_0^*,d_1^*,\cdots,d_n^*)=\gcd(d_0,d_1,\cdots,d_n)/d=1\ ;$$

即 $f^*(x)$ 是本原整系数多项式. 现在 $f(x)=\frac{d}{c}\,f^*(x)$ 符合要求.

唯一性. 如果还有 $f(x)=\frac{d'}{c'}\,f'(x)$ 其中 $0\neq c',d'\in\mathbb{Z}$, $f'(x)=\sum_{i=0}^n d_i'x^i$ 是本原 $\mathbb{Z}$- 多项式; 那么 $\frac{d}{c}\,f^*(x)=f(x)=\frac{d'}{c'}\,f'(x)$, 即

$$c'd\sum_{i=0}^n d_i^*x^i=c'd\,f^*(x)=cd'\,f'(x)=cd'\sum_{i=0}^n d_i'x^i$$

因为 $\gcd(d_0^*,d_1^*,\cdots,d_n^*)=1=\gcd(d_0',d_1',\cdots,d_n')$, 这个等式两边表示同一个整系数多项式, 从左边表达式来看 $c'd$ 是各系数的最大公因子, 从右边表达式来看 cd' 是各系数的最大公因子; 这两个最大公因子在 $\mathbb{Z}$ 中相伴, 即 $c'd=\varepsilon cd'$ 其中 $\varepsilon\in\mathbb{Z}^\times=\{\pm1\}$. 代入上式并从两边消去 cd', 得 $\varepsilon f^*(x)=f'(x)$. 即 $f'(x)$ 与 $f^*(x)$ 在 $\mathbb{Z}[x]$ 中相伴. □

对 $f(x)\in\mathbb{Z}[x]$, 如果 $f(x)$ 在 $\mathbb{Q}[x]$ 中可约则称 $f(x)$ 是 $\mathbb{Q}$- 可约; 如果 $f(x)$ 在 $\mathbb{Z}[x]$ 中可约则称 $f(x)$ 是 $\mathbb{Z}$- 可约.

引理. *设 $f(x)$, $g(x)\in\mathbb{Z}[x]$ 是本原多项式.*

(1) *$f(x)$ 是 $\mathbb{Z}$- 不可约当且仅当 $f(x)$ 是 $\mathbb{Q}$- 不可约.*

(2) *$f(x)$ 与 $g(x)$ 在 $\mathbb{Z}[x]$ 中相伴当且仅当 $f(x)$, $g(x)$ 在 $\mathbb{Q}[x]$ 中相伴.*

证. (1). 设 $f(x)$ 在 $\mathbb{Z}[x]$ 中可约, 即 $f(x)=g(x)h(x)$ 其中 $g(x)$ 和 $h(x)$ 都在 $\mathbb{Z}[x]$ 中不可逆. 若 $g(x)=c$ 是常数多项式, 则 $c\neq0$, $c\neq\pm1$; 这与 $f(x)$ 的所有系数互素相矛盾; 所以 $\deg g(x)>0$. 同理, $\deg h(x)>0$. $f(x)=g(x)h(x)$ 当然也是在 $\mathbb{Q}[x]$ 中的分解式, 即在 $\mathbb{Q}[x]$ 中可约.

反过来, 设在 $\mathbb{Q}[x]$ 中 $f(x)=g(x)h(x)$ 其中 $g(x)$, $h(x)\in\mathbb{Q}[x]$ 是非常数多项式. 由上述引理, 存在本原 $\mathbb{Z}$- 系数 $g^*(x),h^*(x)\in\mathbb{Z}[x]$ 和分数 $\frac{b}{a}\in\mathbb{Q}$ 使得 $f(x)=\frac{b}{a}\,g^*(x)h^*(x)$. 可以设分母分子 a, b 互素. 但 $f(x)$ 是 $\mathbb{Z}$- 系数, 所以 a 整除 $g^*(x)h^*(x)$ 的各系数. 由高斯引理, $g^*(x)h^*(x)$ 仍是本原 $\mathbb{Z}$- 系数多项式, 它的各系数最大公因子是 $\mathbb{Z}$ 的可逆元, 所以 $a=\varepsilon\in\mathbb{Z}^\times$. 那么 $f(x)=(\varepsilon b)\cdot g^*(x)\cdot h^*(x)$ 是在 $\mathbb{Z}[x]$ 中的分解.

(2). 如果 $f(x)$ 与 $g(x)$ 在 $\mathbb{Z}[x]$ 中相伴, 即 $f(x)=\varepsilon g(x)$, $\varepsilon\in(\mathbb{Z}[x])^\times=\mathbb{Z}^\times$; 此等式也表明它们在 $\mathbb{Q}[x]$ 中相伴, 因为 $(\mathbb{Z}[x])^\times=\mathbb{Z}^\times\subseteq\mathbb{Q}^\times=(\mathbb{Q}[x])^\times$.

反过来, 设 $f(x)$ 与 $g(x)$ 在 $\mathbb{Q}[x]$ 中相伴, 即有 $\frac{d}{c}\in\mathbb{Q}^\times$ 使得 $f(x)=\frac{d}{c}\,g(x)$, 并可设分母分子 c, d 互素. 那么 $\frac{d}{c}\,g(x)$ 是整系数多项式, 因而 c 整除 $g(x)$ 的所有系数, 但 $g(x)$ 的所有系数互素, 所以 $c\in\mathbb{Z}^\times$. 又 $f(x)$ 的所有系数互素, 得 $d\in\mathbb{Z}^\times$. 故 $f(x)=\varepsilon g(x)$ 其中 $\varepsilon\in\mathbb{Z}^\times=(\mathbb{Z}[x])^\times$, 即 $f(x)$ 与 $g(x)$ 在 $\mathbb{Z}[x]$ 中相伴. □

推论. *本原 $\mathbb{Z}$- 多项式可以分解为 $\mathbb{Q}$- 不可约本原 $\mathbb{Z}$- 多项式之积.*

证. 本原 $\mathbb{Z}$- 多项式 $f(x)$ 若 $\mathbb{Q}$- 不可约则 $\mathbb{Z}$- 不可约，分解已存在. 若 $f(x)$ 是 $\mathbb{Q}$- 可约，则 $\mathbb{Z}$- 可约： $f(x)=g(x)h(x)$, 由高斯引理， $g(x)$ 和 $h(x)$ 也都是本原多项式，次数均小于 $\deg f(x)$; 按对次数的归纳法， $g(x)$ 和 $h(x)$ 都可写成 $\mathbb{Q}$- 不可约本原 $\mathbb{Z}$- 多项式之积；于是 $f(x)$ 也写成了 $\mathbb{Q}$- 不可约本原 $\mathbb{Z}$- 多项式之积. □

定理. (1) $\mathbb{Z}[x]$ 中的不可约元只有两类： $\mathbb{Z}$ 中的不可约元 *(即素数)*, 或者是 $\mathbb{Q}$- 不可约的本原 $\mathbb{Z}$ 多项式.

(2) $\mathbb{Z}[x]$ 是因子分解环.

证. (1). 首先，由上述引理， $\mathbb{Q}$- 不可约的本原 $\mathbb{Z}$- 多项式是 $\mathbb{Z}[x]$ 中的不可约元；而 $\mathbb{Z}$ 的不可约元 (即素数)p 在 $\mathbb{Z}[x]$ 中不可约，因为：如果 $p=g(x)h(x)$ 则 $g(x)$, $h(x)$ 也得是常数多项式即是两个整数，故其中之一必为 $\mathbb{Z}$ 的可逆元.

现在设 $p(x)$ 是 $\mathbb{Z}[x]$ 的不可约元. 如果 $p(x)=p$ 是常数多项式，则 p 在 $\mathbb{Z}$ 中必不可约，因它在 $\mathbb{Z}$ 中的分解式也是在 $\mathbb{Z}[x]$ 中的分解式. 再设 $\deg p(x)>0$. 设 d 是 $p(x)$ 的所有系数的最大公因子，那么从各系数提取公因子 d, 得到 $p(x)=d\,p^*(x)$, 其中 $p^*(x)$ 就是本原 $\mathbb{Z}$- 多项式，如果 $d\notin\mathbb{Z}^\times$ 则 $d\notin(\mathbb{Z}[x])^\times$, 那么表达式 $p(x)=d\,p^*(x)$ 说明 $p(x)$ 在 $\mathbb{Z}[x]$ 中可约，矛盾. 所以 $d\in\mathbb{Z}^\times=(\mathbb{Z}[x])^\times$; 那么 $p(x)$ 与 $p^*(x)$ 在 $\mathbb{Z}[x]$ 中相伴，故 $p(x)$ 是本原 $\mathbb{Z}$- 多项式；但已假设 $p(x)$ 在 $\mathbb{Z}[x]$ 中不可约，由上述引理， $p(x)$ 在 $\mathbb{Q}[x]$ 中不可约. 即 $p(x)$ 是 $\mathbb{Q}$- 不可约的本原 $\mathbb{Z}$ 多项式.

(2). 设 $f(x)\in\mathbb{Z}[x]$ 是非零不可逆元，即 $f(x)\neq0$, $f(x)\notin(\mathbb{Z}[x])^\times=\mathbb{Z}^\times$.

<u>因子分解存在性</u>. 首先，提取 $f(x)$ 的各系数的最大公因子 d 得 $f(x)=d\,f^*(x)$ 其中 $f^*(x)$ 就是本原 $\mathbb{Z}$ 多项式. 在 $\mathbb{Z}$ 中分解 d 为不可约元之积 $d=p_1\cdots p_r$. 再由上述引理的推论，在 $\mathbb{Z}[x]$ 中分解 $f^*(x)$ 为 $\mathbb{Q}$- 不可约本原 $\mathbb{Z}$ 多项式之积 $f^*(x)=q_1(x)\cdots q_s(x)$. 由上面结论 (1), $f(x)=p_1\cdots p_rq_1(x)\cdots q_s(x)$ 就是 $\mathbb{Z}[x]$ 中的不可约分解.

<u>因子分解唯一性</u>. 设 $f(x)=p'_1\cdots p'_{r'}q'_1(x)\cdots q'_{s'}(x)$ 也是 $\mathbb{Z}[x]$ 中的不可约分解，其中 $p'_1,\ \cdots,\ p'_{r'}$ 是 $\mathbb{Z}$ 的不可约元而 $q'_1(x),\ \cdots,\ q'_{s'}(x)$ 是 $\mathbb{Q}$- 不可约本原 $\mathbb{Z}$ 多项式. 那么

$$p_1\cdots p_rq_1(x)\cdots q_s(x)=f(x)=p'_1\cdots p'_{r'}q'_1(x)\cdots q'_{s'}(x)\ . \tag{$*$}$$

由高斯引理， $q'_1(x)\cdots q'_{s'}(x)$ 与 $q_1(x)\cdots q_s(x)$ 是本原 $\mathbb{Z}$ 多项式；再由多项式写为分数与本原 $\mathbb{Z}$- 多项式之积的唯一性，存在 $\varepsilon\in(\mathbb{Z}[x])^\times=\mathbb{Z}^\times$ 使得

$$q_1(x)\cdots q_s(x)=\varepsilon q'_1(x)\cdots q'_{s'}(x)\ ; \tag{$*1$}$$

从而按照 $(*)$ 式还有

$$\varepsilon p_1\cdots p_r=p'_1\cdots p'_{r'}\ . \tag{$*2$}$$

因为 $\mathbb{Q}[x]$ 是因子分解整环，从 $(*1)$ 式，在 $\mathbb{Q}[x]$ 中得 $s=s'$ 且适当重编号后有

$$q_1(x)\sim\varepsilon q'_1(x)\sim q'_1(x),\quad q_2(x)\sim q'_2(x),\quad\cdots,\quad q_s(x)\sim q'_s(x)\ ;$$

那么根据上述引理，在 $\mathbb{Z}[x]$ 中也同样有相伴式

$$q_1(x) \sim q_1'(x), \quad q_2(x) \sim q_2'(x), \quad \cdots, \quad q_s(x) \sim q_s'(x) \ .$$

最后，因为 $\mathbb{Z}$ 是因子分解整环，从 $(*2)$ 式，在 $\mathbb{Z}$ 中得 $r = r'$ 且适当重编号后有

$$p_1 \sim \varepsilon p_1 \sim p_1', \quad p_2 \sim p_2', \quad \cdots, \quad p_r \sim p_r' \ . \qquad \square$$

例. 在 $\mathbb{Z}[x]$ 中，$6x^3 - 18x + 12 = 2 \cdot 3 \cdot (x-1)^2(x+2) = (-2)3(-x+1)(x-1)(x+2)$ 等都是不可约分解.

但在 $\mathbb{Q}[x]$ 中，$6x^3 - 18x + 12 = (x-1)^2(6x+12) = (2x-2)(3x-3)(x+2)$ 等都是不可约分解.

习题 3.7

1. 证明：在 $\mathbb{Z}_6[x]$ 中 $x^2 + [3]x + [2]x = (x + [2])(x + [1]) = (x - [1])(x - [2])$.

2. 如果 $\frac{d}{c} \in \mathbb{Q}$, 其中 c 与 d 是互素的整数，是 $\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ 的根，其中 $a_n \neq 0$, 证明： $c|a_n$ 且 $d|a_0$.

3. 设 $f(x) \in \mathbb{Z}[x]$, $\deg f(x) > 0$. 如果 $f(x)$ 在 $\mathbb{Q}[x]$ 中可约则 $f(x)$ 在 $\mathbb{Z}[x]$ 中可约.

4. (爱森斯坦判别法) 设 $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. 如果存在素数 p 使得：

(i) $p \nmid a_0$; (ii) $p \mid a_i$ 对 $i = 1, \cdots, n$; (iii) $p^2 \nmid a_0$;

证明： $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

5. 下列多项式在 $\mathbb{Q}[x]$ 中是否可约：

(1). $x^p + px + 1$ 其中 p 是一个素数. (提示：做代换 $x = y - 1$.)

(2). $x^5 + x^3 + 3x^2 - x + 1$. (提示：如果可约，则在 $\mathbb{Z}[x]$ 中可约且有二次因子 $x^5 + x^3 + 3x^2 - x + 1 = (x^2 + ax + 1)(x^3 + bx^2 + cx + 1)$.)

6. 设 p 是素数. 则 $x^{p-1} + \cdots + x + 1$ 在 $\mathbb{Q}[x]$ 中不可约. (提示：做代换 $x = y + 1$.)

7*. 仿照本节证明完成定理 3.7.1 的证明.