

第1章 环

1.1 分式域

定义 1.1 (分式域)

若交换整环 R 是域 F 的子环且 $\forall a \in F, \exists b, c \in R$, 使得

$$a = bc^{-1},$$

则称 F 为 R 的分式域.

定理 1.1

设 R 为交换整环, 则 R 的分式域一定存在.

注 关于 R 的条件可放宽为 R 是无零因子交换环, 即 R 中不必有么元.

证明 令 $R^* = R \setminus \{0\}$, 在集合 $R \times R^*$ 中定义加法与乘法, $\forall (a, b), (c, d) \in R \times R^*$,

$$(a, b) + (c, d) = (ad + bc, bd), \quad (1.1)$$

$$(a, b)(c, d) = (ac, bd). \quad (1.2)$$

易验证 $R \times R^*$ 对上述加法与乘法都是交换幺半群, 它们的零元素及么元分别为 $(0, 1), (1, 1)$. 在 $R \times R^*$ 中定义一个关系 “ \sim ”,

$$(a, b) \sim (c, d), \quad \text{若 } ad = bc.$$

先证明关系 \sim 是等价关系. 事实上, 由 $ab = ab$ 知 $(a, b) \sim (a, b)$. 又若 $(a, b) \sim (c, d)$, 即 $ad = cb$, 因而 $(c, d) \sim (a, b)$. 最后, 假设 $(a, b) \sim (c, d), (c, d) \sim (e, f)$, 则 $adf = bcf = bde$. 由 R 是交换整环, $d \neq 0$, 于是 $af = be$, 即 $(a, b) \sim (e, f)$.

其次证明关系 \sim 对于 $R \times R^*$ 中的乘法是同余关系, 设

$$(a, b) \sim (c, d), \quad (e, f) \sim (g, h).$$

于是由式 (??) 知

$$(a, b)(e, f) = (ae, bf), \quad (c, d)(g, h) = (cg, dh),$$

而由 R 是交换整环可得 $(ae)(dh) = adeh = bcfh = (bf)(cg)$, 即有

$$(a, b)(e, f) \sim (c, d)(g, h).$$

再次证明关系 \sim 对于 $R \times R^*$ 中的加法是同余关系. 设

$$(a, b) \sim (c, d), \quad (e, f) \sim (g, h),$$

则由式 (??) 知

$$(a, b) + (e, f) = (af + be, bf), \quad (c, d) + (g, h) = (ch + dg, dh).$$

这时由 R 是交换整环可得

$$(af + be)dh = adfh + bedh = bcfh + fgbd = (ch + dg)bf,$$

因而 $((a, b) + (e, f)) \sim ((c, d) + (g, h))$.

令 $F = R \times R^* / \sim$ 为商集合, 以 $\frac{a}{b}$ 表示 (a, b) 所在等价类. 于是由定理 ??, 在 F 中有加法与乘法运算如下:

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd}, \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

再由定理??知 F 对加法与乘法都是交换幺半群. 零元素与幺元素为 $\frac{0}{1}, \frac{1}{1}$, 记 $0 = \frac{0}{1}, 1 = \frac{1}{1}$. 对 $\forall d \in R$, 由于 $0 \cdot d = 0 \cdot 1$, 故有 $(0, 1)$ 与 $(0, d)$ 等价, 即 $\frac{0}{1} = \frac{0}{d}$. 又由 $1 \cdot d = 1 \cdot 1$ 知 $\frac{1}{1} = \frac{d}{d} = 1$.

由

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab - ab}{b^2} = \frac{0}{b^2} = 0$$

知 F 对加法为交换群.

又若 $\frac{a}{b} \neq 0$, 即 $a \neq 0$, 则 $(b, a) \in R \times R^*$, 即 $\frac{b}{a} \in F$. 这时

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = 1,$$

故 $F^* = F \setminus \{0\}$ 对乘法为交换群且 $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. 又由

$$\begin{aligned} \left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{f}{e} &= \frac{ad + bc}{bd} \cdot \frac{f}{e} = \frac{adf + bcf}{bde} \\ &= \frac{adef + bcef}{bdee} = \frac{af}{be} + \frac{cf}{de} \\ &= \frac{a}{b} \cdot \frac{f}{e} + \frac{c}{d} \cdot \frac{f}{e}. \end{aligned}$$

知 F 中加法与乘法间分配律成立, 故 F 为域.

记 $R_1 \triangleq \left\{\frac{a}{1} : a \in R\right\}$, 则

$$\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1}, \quad \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1},$$

故 R_1 是 F 的子环. 由于 $\frac{a}{1} = \frac{b}{1}$ 当且仅当 $a = b$, 故 $\frac{a}{1} \rightarrow a$ 是 R_1 到 R 上的一个良定义的映射, 不难验证其也是同构映射, 因此可将 R 作为 F 的子环. 而对 F 中任一元素 $\frac{a}{b}$ 有

$$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1},$$

故 F 是 R 的分式域.

□

定理 1.2

交换整环 R 的分式域 F 是以 R 为子环的最小域, 因而 R 的分式域唯一.

♥

注 关于 R 的条件可放宽为 R 是无零因子交换环, 即 R 中不必有幺元.

证明 设 F' 是域且以 R 为子环, 则 F' 中子集

$$F_1 = \{ab^{-1} \mid a, b \in R, b \neq 0\}$$

是 F' 的子域, 事实上, 对 $\forall ab^{-1}, cd^{-1} \in F_1$, 有

$$ab^{-1} + cd^{-1} = (ad + cd)(bd)^{-1}, \quad -(ab^{-1}) = (-a)b^{-1},$$

故 F_1 对加法为 F' 的子群. 又若 $ab^{-1}, cd^{-1} \in F_1 \setminus \{0\}$, 则

$$(ab^{-1})(cd^{-1})^{-1} = (ad)(bc)^{-1},$$

故 $F_1 \setminus \{0\}$ 对乘法为 $F' \setminus \{0\}$ 的子群, 因此 F_1 是 F' 的子域. 由定理??知

$$\frac{a}{b} \triangleq \{(c, d) \in R \times R \setminus \{0\} : ad = bc\}, \quad F = \left\{\frac{a}{b} : a \in R, b \in R \setminus \{0\}\right\}.$$

又 $\frac{a}{b} \rightarrow ab^{-1}$ 是 R 的分式域 F 到 F_1 上的同构, 故可将 F 与 F_1 等同, 因而 $F \subseteq F'$.

□

例题 1.1 设 \mathbf{P} 是任一数域, 设 $\mathbf{P}[x]$ 的分式域为 $\mathbf{P}(x)$, 则

$$\mathbf{P}(x) = \left\{\frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbf{P}[x], g(x) \neq 0\right\}.$$

证明

□

例题 1.2 设 m 是非零整数, 则 $m\mathbf{Z}$ 的分式域为 \mathbf{Q} .

证明

□

1.2 多项式环

定义 1.2

设 \tilde{R} 是一个交换幺环, R 是 \tilde{R} 的子环且 $1 \in R$. 又设 $u \in \tilde{R}$, \tilde{R} 中由 R 与 u 生成的子环, 即包含 R 与 u 的最小子环记为 $R[u]$. 容易看出

$$R[u] = \{a_0 + a_1u + \cdots + a_nu^n \mid a_i \in R, n \geq 0\},$$

也称 $R[u]$ 为 R 上添加 u 生成的子环.

♣

定义 1.3

如果在 R 中存在有限多个元素 a_0, a_1, \cdots, a_n 且 $a_n \neq 0$, 使得

$$a_0 + a_1u + \cdots + a_nu^n = 0,$$

那么称 u 为 R 上的代数元, 使上述关系成立的最小正整数 n 称为代数元 u 的次数, 记为 $\deg(u, R)$.

♣